INTERPLAY BETWEEN KNOW YOUR COSTUMER (KYC) AND DATA PRIVACY.

Arghya Pattanayak, Arpita Nayak, Manorama Moharana
Student, Student, Student
Law and Legal Studies
KIIT School of Law, Cuttack, India

ABSTRACT

The growing regulatory framework surrounding Know Your Customer compliance has immensely changed data governance practices in the banking industry. While KYC regulations are important in preventing money laundering, financing terrorism, and financial fraud, they also involve extensive collection, verification, and storage of sensitive personal information from customers. This paper examines the intricate balance between mandatory KYC requirements and new standards of data privacy, particularly with regard to evolving digital banking environments and extended privacy regimes such as the Digital Personal Data Protection Act, 2023. The research investigates how banks balance the need for extensive customer due diligence with the need to comply with the principles of data minimization, purpose limitation, and informed consent. Through a doctrinal and comparative analysis of regulatory standards, compliance guidelines, and judicial methodologies, the paper highlights persisting tensions, systemic weaknesses, and the need for integrated policy frameworks. Finally, the study calls for a robustly designed regulatory framework that shields financial integrity while preserving the fundamental right to informational privacy.

KEYWORDS

Know Your Customer (KYC) Compliance, Data Privacy, Digital Personal Data Protection Act 2023, Banking Regulation, Customer Due Diligence.

INTRODUCTION

Contemporary banking operates at the intersection of strict regulatory compliance and an increasingly rights-based data protection landscape. Know Your Customer requirements that began with the necessity of combating money laundering and maintaining financial integrity now involve the collection and processing of a wide array of clients' personal and sensitive information. In a time of expanding digital banking, coupled with increased fintech inclusions and automated verification methods, not only has the volume increased, but so too has the vulnerability of this data, thus raising significant issues regarding privacy, proportionality, and data security. Conversely, new data protection regulations emphasize principles such as purpose limitation, informed consent, data minimization, and accountability, which are often in conflict with wide-ranging KYC requirements. This article analyzes the emerging relationship and evaluates how banks fulfill the dual mandate of implementing robust due diligence while upholding new privacy regulations, highlighting the growing need for harmonized regulatory standards that protect financial systems while preserving personal rights.

Despite substantial research on anti-money laundering compliance and growing literature on standards of data protection, there is a significant gap in reviewing how banks effectively balance the conflicting requirements of KYC obligations and data privacy laws in a rapidly digitizing financial ecosystem. Existing studies have focused largely either on the legal provisions involving KYC or examined data privacy as an abstract concept, without attempting to seriously evaluate the operational, technological, and doctrinal conflicts arising from the interaction of both regimes. Furthermore, few studies examine the impact of India's evolving data protection landscape-particularly post-2023-on banking practices, risk assessment methodologies, and consumer rights. The result of this lack of integrated evaluation is the unresolved issues related to proportionality, accountability, data retention practices, and conformity of laws. This paper intends to fill this gap by undertaking a comprehensive review of the relationship between KYC compliance and data privacy, underlining areas where existing laws and practices are incoherent or insufficiently developed.

Evolution and Objectives of KYC Norms in the Banking Sector

The evolution of KYC norms in banking emerges from the global initiative of achieving transparency in financial transactions and combating illicit financial activities. From its initial purposes of preventing money laundering and fraud, KYC norms have grown to address broader challenges: terrorist financing, identity theft, and systemic stability. International bodies such as FATF have laid down universal standards that forced countries, including India, to adopt more stringent customer due diligence processes. In India, the evolution took a path from mere identification techniques to comprehensive, risk-based KYC systems under laws like the Prevention of Money Laundering Act (PMLA) and guidelines given by the Reserve Bank of India. Today’s KYC goals are more than about satisfying regulatory requirements; they aim at protecting banks from reputational and operational risks, enhancing customer verification, guaranteeing online transactions securely, and ensuring systemic stability through a financial system increasingly dominated by technology.

Regulatory Framework Governing KYC in India: RBI, PMLA, and Fintech Guidelines

1. Regulatory Framework under RBI

The RBI plays a key role in shaping India's KYC framework through comprehensive Master Directions that detail the requirements of customer identification, verification, and ongoing due diligence. These directions apply to all regulated entities, including banks, NBFCs, payment banks, and cooperative banks. RBI's KYC norms incorporate a risk-based approach under which financial institutions are required to categorize customers as low, medium, and high risk and apply due diligence measures commensurately. Over years, the RBI has aligned its KYC framework to global standards, allowing for simplified KYC for small accounts, video-based customer identification, and digital onboarding. It also prescribes strict norms on data retention, reporting obligations, identification of beneficial ownership, and periodic updates, making it the foundational regulatory pillar for KYC compliance in India.

2. Regulatory Framework under PMLA

PMLA, 2002, established the statutory backbone for KYC obligations by making customer due diligence a legal requirement and not a regulatory formality. Accordingly, all reporting entities, including banks,

financial institutions, and intermediaries, are obliged under PMLA and its Rules to undertake identification of their customers, maintain their transaction records for the periods prescribed, and report suspicious and high-value transactions to FIU-IND. PMLA links KYC directly with AML and CFT objectives, thus strengthening the legal enforceability of the KYC norms. Non-compliance under PMLA attracts severe penalties in the endeavor for greater accountability to make KYC integral to national financial security and commitments on AML globally.

3. Fintech and Digital KYC Guidelines

The rise of fintech triggered the need to introduce special digital KYC guidelines to balance innovation with regulatory safeguards. These guidelines, per the RBI circulars and the related regulatory framework, allow different digital onboarding methods [i]such as Aadhaar-based e-KYC, XML offline KYC, and V-CIP. Digital payment service providers, including fintech companies offering prepaid instruments and lending platforms, have to comply with these standards focusing on secure authentication, prevention of identity fraud, and customer data protection. Technical requirements prescribed by these guidelines include secure storage, end-to-end encryption, audit trails, and real-time verification mechanisms. Through the integration of technology and compliance, these norms strive to further the goals of financial inclusion and seamless digital engagement while ensuring the integrity and security of customer identity information.

Scope and Significance of the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, covers all sectors that deal in digital personal data, including the banking sector, which involves dealing with some of the most sensitive kinds of customer information. It provides a rights-based framework based on principles such as informed consent, purpose limitation, data minimization, and lawful processing, thereby redefining the way financial institutions collect, store, and use personal information. It establishes specific obligations for data fiduciaries like banks and fintech firms in relation to secure processing, breach notification, grievance redressal, and accountability. The Act fosters trust among customers and aligns India's digital economy with international privacy standards by implementing strict compliance requirements and penalties for disclosure of unauthorized data or their misuse. The importance of the Act within the ambit of the KYC is that it seeks a balance in data collection and guides institutions to balance regulatory requirements with the fundamental right to privacy in information.

Types of Personal and Sensitive Data Collected During KYC

1. **Basic Identification Data** – Name, date of birth, gender, and photograph.
2. **Government-Issued Identity Numbers** – Aadhaar number, PAN, passport number, voter ID, or driving licence details.
3. **Contact Information** – Residential address, email ID, and mobile number.
4. **Biometric Data** – Fingerprints, facial recognition data, or iris scans (especially in Aadhaar-based e-KYC or V-CIP).
5. **Financial Information** – Bank account details, income proofs, tax records, and credit history relevant for risk assessment.

6. **Proof of Address Documents** – Utility bills, rental agreements, or official correspondence.
7. **Beneficial Ownership Details** – Information on individuals controlling or owning legal entities.
8. **Sensitive Personal Data** – Any data revealing identity traits or authentication credentials, such as signature samples or encrypted identification tokens.
9. **Transaction and Behavioural Information** – Patterns used to assess customer risk profile under AML/KYC norms.
10. **Digital Metadata** – IP address, device information, and geo-location data during digital onboarding or verification.

Data Minimisation vs. Mandatory Data Collection: The Core Tension

The principle of data minimisation requires organisations to collect only that personal information which is strictly necessary for fulfilling a specific, lawful purpose. The said principle becomes all the more important in the banking sector, as financial institutions regularly deal with voluminous sensitive and personally identifiable data. Data minimisation aims at decreasing the risks of misuse, breaches, and unauthorised access by reducing the size and sensitivity of the data repositories. It also strengthens customer autonomy by barring excessive or intrusive data practices. Banks, under privacy-centric frameworks, are expected to justify every piece of data they collect by showing that no alternative, less intrusive way exists to achieve the intended purpose.

In practice, however, mandatory data collection under KYC and anti-money laundering regimes often contradicts such a philosophy of data minimisation. Banks are legally bound to collect extensive documentation for identification, risk assessment, determination of beneficial ownership, and monitoring suspicious activities. These legal requirements leave little room for minimizing data collection, since failure to collect the information called for can amount to regulatory non-compliance. Digital onboarding, biometric authentication, and enhanced due diligence make the volume of data needed for KYC grow even further. This actually creates an inherent tension: privacy laws urge institutions to limit collection, while financial regulations require them to collect more than ever before, and a delicate balance must be found to satisfy both regulatory imperatives and privacy safeguards.

Legal basis for processing customer data under KYC obligations

This is further supported by the basis of processing customer data under KYC obligations which has its grounds firmly established in statutory requirements imposed by AML/KYC (Anti–Money Laundering)/l(Know Your Customer)Laws that include identity verification, risk assessment, and monitoring on a continuous basis for the prevention of money laundering, terrorism financing, and financial fraud. Processing under data protection frameworks, such as the GDPR, would fall under Article 6(1)c GDPR(compliance with a legal obligation) and, in appropriate contexts, Article 6(1)e GDPR (task carried out in the public interest). However, because the requirements are legal in nature, organizations cannot seek consent from individuals, nor can they delete the customer's data upon request; rather, they have to retain it for determined periods.

This relationship represents a balance between the commitment to necessary compliance obligations and the principles of data protection. While KYC laws demand far-reaching data collection and verification, privacy

regulations call for data minimization, purpose limitation, transparency, and strong security measures. Some privacy rights, such as access or erasure, may be restricted to avoid impairing investigations or statutory retention obligations. The interplay, therefore, illustrates how an organization should concurrently meet regulatory expectations while taking care of customer data and not developing disproportionate or unlawful processing.

Consent, Autonomy and Purpose Limitation

Consent and individual autonomy are severely limited in the context of KYC processes, since customers are compelled by law to provide personal information for identity verification and anti-money laundering compliance. Purpose limitation is therefore necessary for privacy preservation, despite these mandatory requirements. Though the relevant KYC laws demand the collection and verification of personal data, the respective privacy regulations stringently limit the use of that data for compliance-related purposes, such as verification of identity, risk assessment, and reporting of suspicious activity.

Consent and Autonomy in KYC

Consent is not the main legal basis in KYC because customers are legally obliged to provide their information for AML/KYC compliance.It is a limited autonomy, since nobody can freely decline a data collection without refraining from financial or regulated services.The limitation imposed here reflects a tension that exists between free individual choice and compulsory compliance, which is one of the core areas where KYC and data privacy interact.Lack of consent for anything shows the need for strong privacy protections to protect people against limited free will.

Limitation of Purpose in KYC

KYC data collection and usage must strictly be for legally required purposes and within the lines of identification verification, risk assessment, and anti-money-laundering oversight.Privacy laws ban the use of KYC data for unrelated purposes such as marketing, profiling, or commercial exploitation.Limitation of purpose means that compulsory collection of data cannot result in overreach and, therefore forms a fundamental safeguard to privacy. This principle aims at balancing regulatory requirements with data protection, reinforcing the interplay between necessary compliance and the protection of customer rights.

Data storage and deletion requirements in bank

1. Requirements for Data Storage

- Banks are obliged to store KYC data securely, including customer identity documents, records of transactions, financial profiles, and risk assessments.
- Security measures should involve encryption, restricted access, audit logs, and secure servers that protect the information stored within from unauthorized access or any form of cyber threat.
- Data should be organized and structured in such a way that allows for efficient monitoring, reporting, and regulatory compliance, like suspicious activity reporting.
- Interplay with data privacy arises because, while banks must collect and store detailed personal data in order to perform compliance-related functions, the privacy laws require that unnecessary data storage be minimized or done with protection of customer information.

2. Data Retention Requirements

- KYC (Know Your Customer)and AML (Anti–Money Laundering)regulations require retaining information for 5–10 years after the end of the customer relationship or, in the case of a transaction, after its completion.
- Customers cannot demand deletion or erasure during this period, as retention of data is necessary for purposes of legal and regulatory compliance.
- Retention policies have to be aligned with regulatory requirements, as well as compliance frameworks, to make sure the data is kept no longer than legally required.
- while privacy principles advocate for storage limitation, KYC obligations call for long-term retention, meaning a careful balancing by banks.

3. Requirements for Data Erasure

- Once the mandatory retention period has elapsed, banks must delete or anonymize KYC data, provided there are no continuing legal obligations, investigations, or disputes.
- Proper deletion requires structured deletion schedules, data lifecycle management, and audit documentation for compliance.
- This ensures that privacy laws take effect again so that customers' personal data can be removed or anonymized and avoid being misused or over-retained.

Cyber security challenges in digital KYC and E-KYC

The upsurge of digital KYC (dKYC) and electronic KYC (e-KYC) systems has significantly facilitated customer on boarding and verification processes, while it also introduces unique cybersecurity challenges. Banks and financial institutions collect sensitive personal information, including government-issued IDs, biometric data, financial details, and transaction histories which are stored digitally and transmitted through digital channels. This opens up points of vulnerability such as data breaches, phishing attacks, ransomware, identity theft, and unauthorized access. Poor encryption, insecure storage, or weak access controls could compromise customer data with losses not only financially but also in terms of reputation and attracting regulatory penalties under privacy laws. Technical difficulties in integrating multiple verification platforms while keeping end-to-end security raise an additional risk layer.

The interplay between KYC obligations and data privacy becomes particularly evident in digital systems. On one hand the KYC regulations prescribe the collection, storage, and verification of extensive personal data, while on the other hand, privacy laws like GDPR or locally implemented data-protection frameworks demand severe safeguards, minimal retention, and strict purpose limitation. E-KYC systems must be designed with robust cybersecurity measures including multi-factor authentication, encrypted data transfers, and continuous monitoring, in order to protect customer data. Secondly, compliance frameworks should guarantee that no more data is collected than legally required and that it will not be used for any other purpose than verification or any regulatory purpose, including secondary or commercial use. This proves the twofold responsibility of banks: they have to fulfill regulatory obligations related to KYC and ensure privacy and security in the digital environment.

Role of Technology : AI- based verification & biometrics

1. Role of AI-Based Verification in KYC

AI-based verification is one of the cornerstones of modern-day KYC processes, which enables automated identity checks, document verification, and transaction monitoring. AI algorithms can easily validate government-issued IDs, passports, and utility bills much faster by detecting forgery, inconsistencies, or manipulated images in those. Also, AI can analyze behavioral patterns, transaction history, and risk scores for spotting suspicious activity and helping to enhance AML compliance.

Advantages:

- Accelerates the onboarding process and minimizes manual errors.
- It enables real-time risk assessment and fraud detection.
- Supports scalability for large customer bases, especially in digital banking and fintech.

Privacy Risks:

- AI, very often requires massive amounts of personal data, sensitive and financial information.
- Algorithms may profile or score customers beyond strictly required KYC purposes, raising purpose limitation concerns.
- Automated decision-making may lead to biased outcomes or risk scoring that could potentially infringe on data-subject rights under privacy laws such as GDPR.

2. Role of Biometrics in KYC

Biometric technologies, including facial recognition, fingerprint scanning, iris recognition, and voice verification add a robust layer of security to identity verification. They reduce impersonation and identity fraud by making sure the person presenting the document is the legitimate owner. Biometrics also make it easier to perform remote or digital on boarding, which is important in mobile banking and fintech platforms.

Advantages:

- It provides high accuracy in verifying the identity of a customer.
- It prevents duplication and impersonation in customer databases.
- Enhance convenience for the customer in digital on boarding.

Privacy Risks:

- Biometric data is classed as highly sensitive personal information under most data protection frameworks.
- Hacking, unauthorized access, or storage breaches result in irreversible identity theft because biometric traits cannot be changed like passwords.
- Unnecessary or excessive collection of biometric information runs the risk of violating data minimization and purpose limitation principles.

Comparative Analysis: EU GDPR, US Regulations, and Indian Framework

The relative geography of data protection fabrics across the European Union(EU), the United States(US), and India reflects unnaturally different nonsupervisory doctrines shaped by distinct socio-legal surrounds. The EU's General Data Protection Regulation(GDPR) represents the most comprehensive and harmonized

data protection governance, predicated in the idea of sequestration as a abecedarian right under the Charter of Fundamental Rights of the European Union. Its principles of legality, fairness, translucency, purpose limitation, data minimization, and responsibility produce a livery, rights- centric structure with strict scores for data regulators and processors, including extraterritorial connection. In discrepancy, the United States adopts a sectoral, request- driven approach driven largely by consumer protection and assiduity-specific bills similar as the Health Insurance Portability and Responsibility Act(HIPAA), Gramm – Leach – Bliley Act(GLBA), and the Children's Online sequestration Protection Act(COPPA). With no single civil sequestration law, the US frame relies heavily on state legislation most specially the California Consumer sequestration Act(CCPA) and its emendations which give limited, consumer- acquainted rights compared to the EU's robust individual protections. India's evolving frame, presently anchored in the Digital Personal Data Protection Act, 2023(DPDPA), represents a mongrel model that blends rudiments of the GDPR with considerations of public security, executive convenience, and digital governance precedences. While the DPDPA introduces concurrence- grounded processing, data fiduciary duties, and rights of data headliners, it also grants broad immunity to the State, raising enterprises about proportionality and oversight. relative analysis reveals that while GDPR sets a global gold standard for rights- grounded data protection, the US prioritizes invention and profitable interests, and India seeks to balance sequestration rights with experimental and nonsupervisory imperatives. This divergence underscores the need for lesser adjustment to insurecross-border data flows, legal certainty for businesses, and more effective protection of individual sequestration in an decreasingly connected digital ecosystem.

Judicial Interpretation of Privacy Rights in Financial Data Processing

Judicial interpretation of privacy rights in the context of financial data processing has evolved significantly as courts across jurisdictions have grappled with the balance between individual autonomy and regulatory or commercial interests. In India, the Supreme Court's landmark decision in *Justice K.S. Puttaswamy v. Union of India (2017)* affirmed privacy as a fundamental right under Article 21, laying the constitutional foundation for safeguarding sensitive financial information. The Court recognized informational privacy as a core facet of personal liberty, emphasising that data collection and processing must satisfy tests of legality, necessity, and proportionality. This principle was further applied in *K.S. Puttaswamy v. Union of India, (2019)* where the Court scrutinised the Aadhaar Act's mandates concerning the collection of biometric and financial identifiers. Although Aadhaar was upheld for welfare purposes, the Court invalidated Section 57, holding that private entities cannot demand Aadhaar-based authentication, marking a crucial restraint on financial data misuse. Internationally, the European Court of Justice, in *Schrems v. Data Protection Commissioner* (*2015*), invalidated the EU–US Safe Harbour framework, ruling that financial data transferred to the United States lacked adequate protection from state surveillance. This judgment reinforced the principle that cross-border financial data flows must ensure equivalent privacy safeguards. In the United States, the Supreme Court's decision in *Carpenter v. United States,(2018)* expanded constitutional protections to include digital records held by third parties, holding that accessing such data without a warrant violates the Fourth Amendment. While Carpenter focused on location data, its reasoning has profound implications for financial records, as it rejects the rigid third-party doctrine and acknowledges heightened

expectations of privacy in digitally stored information. Collectively, these rulings demonstrate a converging judicial recognition that financial data, due to its sensitivity and potential for profiling, requires robust constitutional and statutory protections, ensuring that regulatory schemes and technological innovations do not erode individual privacy rights.

Liability and Accountability: Banks as Data Fiduciaries or Data Controllers

The question of liability and responsibility in fiscal data governance has gained renewed significance as banks decreasingly operate as both custodians of sensitive particular information and major players in digital fiscal ecosystems. Under contemporary data protection administrations, banks may assume the part of " data fiduciaries " or " data regulators, " each designation carrying distinct legal counteraccusations . In authorities told by the EU GDPR, banks serve as data regulators when they determine the purposes and means of recycling fiscal data, thereby bearing primary responsibility for compliance with principles similar as legality, purpose limitation, data minimization, and responsibility. This includes scores to apply strong security measures, conduct Data Protection Impact Assessments(DPIAs), and insure translucency toward data subjects. Again, India's Digital Personal Data Protection Act, 2023(DPDPA) conceptualizes banks as data fiduciaries, emphasizing a heightened duty of care, fairness, and fidelity toward data headliners. As data fiduciaries, banks must secure informed concurrence, insure accurate processing, notify breaches, and help abuse, while significant data fiduciaries face fresh scores similar as appointing Data Protection Officers and witnessing independent checkups. Despite these statutory fabrics, the practical challenges are substantial banks constantly partake data with third- party fintech mates, credit information companies, and nonsupervisory bodies, raising complex issues of common controllership and vicarious liability. Judicial trends decreasingly emphasize that responsibility can not be adulterated simply because processing is algorithmic or outsourced. Regulatory penalties fornon-compliance — similar as GDPR's heavy executive forfeitures or the DPDPA's steep financial warrants — support the anticipation that banks maintain robust internal governance, threat operation practices, and inspection mechanisms. Eventually, whether classified as data regulators or data fiduciaries, banks enthrall a position of heightened trust, and their liability frame must reflect the perceptivity of fiscal data, the asymmetry of power between institutions and individualities, and the need for transparent, rights- centric data handling practices in the digital fiscal geography

Impact of Data Breaches and KYC Leaks on Consumer Trust

The impact of data breaches and Know Your client(KYC) leaks on consumer trust in the fiscal sector is profound, far- reaching, and frequently unrecoverable. KYC data comprising Aadhaar figures, visage details, biometric identifiers, fiscal histories, and sensitive demographic information — forms the core of an existent's digital identity. When similar data is exposed through breaches, it creates a deep sense of vulnerability and undermines public confidence in fiscal institutions that are fairly obliged to guard this information. Frequent incidents of unauthorized access, phishing attacks, ransomware intrusions, and internal mismanagement support consumer comprehensions that banks and fintech platforms are ill-equipped to cover their data. The corrosion of trust is n't simply cerebral; it has palpable behavioral consequences. Consumers come reluctant to use digital banking channels, detention online deals, or avoid

linking accounts with third- party fiscal apps, thereby negatively affecting fiscal addition and digital invention sweats. In India, large- scale KYC leaks have boosted debates on the acceptability of institutional safeguards and raised questions about responsibility under the Digital Personal Data Protection Act, 2023. Internationally, studies in GDPR authorities show that breach announcements, though obligatory, frequently fail to restore consumer confidence unless accompanied by transparent remediation and provable systemic advancements. likewise, the reputational damage for fiscal realities is substantial institutions that witness major breaches suffer stock devaluation, increased client churn, and heightened nonsupervisory scrutiny, including heavy penalties for shy security practices. For consumers, the detriment extends beyond immediate fiscal loss to long- term pitfalls similar as identity theft, unauthorized account access, profiling, and surveillance. Eventually, the patient rise in data breaches and KYC leaks highlights a structural trust deficiency that can only be eased through stronger nonsupervisory enforcement, robust cybersecurity practices, transparent communication, and a provable commitment by fiscal institutions to uphold the sequestration and security of consumer data as a core fiduciary responsibility.

Need for Harmonised Policy Frameworks and Regulatory Convergence

The growing complexity of global data flows and the adding interdependence of fiscal ecosystems emphasize the critical need for harmonised policy fabrics and nonsupervisory confluence in data protection and fiscal governance. Divergent public norms similar as the GDPR in the European Union, sectoral sequestration rules in the United States, and India's Digital Personal Data Protection Act, 2023 — produce fractured compliance geographies that burden transnational fiscal institutions and fintech platforms. These inconsistencies lead to nonsupervisory arbitrage, uneven consumer protections, and challenges in administering responsibility across borders. As fiscal deals routinely involvecross-jurisdictional processing, the absence of harmonised rules heightens pitfalls associated with data breaches, identity theft, and unauthorized surveillance, while also impeding the smooth inflow of capital and digital fiscal services. Harmonisation does n't indicate uniformity but rather the development of interoperable norms, combined delineations of crucial generalities similar as concurrence, data fiduciaries regulators, sensitive particular data, and common principles of translucency, purpose limitation, and proportionality. Regulatory confluence can empower countries to coordinate cybersecurity morals, establish harmonious breach-announcement conditions, and streamline mechanisms forcross-border examinations. transnational cooperation through bodies like the G20, OECD, and Financial Action Task Force(FATF) becomes essential for creating model guidelines that insure data protection without hindering invention or profitable growth. For developing countries, confluence allows them to borrow global stylish practices while acclimatizing rules to domestic socio- profitable surrounds. also, harmonised programs enhance consumer trust by guaranteeing that their fiscal data receives similar protection anyhow of where it's reused. Eventually, a coherent and coincident nonsupervisory ecosystem reduces compliance burdens, strengthens institutional responsibility, and supports flexible digital finance. In an period where data is the backbone of fiscal operations, harmonised fabrics are n't simply desirable but necessary for icing fairness, security, and stability in the global fiscal armature.

CONCLUSION

At the heart of modern banking governance, KYC compliance and data privacy are in constant interplay-a delicate balance between imperatives of national security and individual rights. Indeed, as this paper illustrates, KYC obligations demand that financial institutions collect a wide range of personal and sensitive information for identity verification, risk assessment, and anti-money laundering functions; this is inherently in tension with foundational privacy principles such as consent, purpose limitation, and data minimisation. Driven by the advent of digital onboarding, AI-based verification, biometric authentication, and various fintech integrations, the scale and sensitivity of collected data have grown, further amplifying the operational and ethical complexities facing banks.

The enforcement of the Digital Personal Data Protection Act, 2023, and its accompanying Data Privacy Rules, 2025, has changed the regulatory landscape in no small measure. The 2025 Rules introduce compulsory DPIAs for high-risk processing like biometrics and AI-based KYC, strict breach-notification timelines, purpose-specific retention schedules, algorithmic accountability norms, and more rights accorded to data principals regarding the right to grievance redressal and transparency related to automated decision-making. For banks, these Rules classify them as Significant Data Fiduciaries with increased duties of care, including periodic audits, appointment of Data Protection Officers, encryption, and pseudonymization standards, and compulsory proportionality assessments before collecting any additional KYC-related data.

Against this backdrop, the banking sector has to strike a balance between the dual, and sometimes competing, imperatives of compliance with regulatory requirements and preservation of privacy. If KYC laws require extensive data collection to preserve financial integrity, the 2025 Data Privacy Rules ensure that such collection is not inordinate, exploitative, or prone to misuse. The emergence of a harmony between these regimes necessarily implies that banks would have to adopt systems based on privacy-by-design, minimize data collection wherever legally permissible, and enhance cybersecurity infrastructure and total transparency regarding data practices. Ultimately, what will be required is a robust integrated regulatory framework, underpinned by technological safeguards, judicial oversight, and institutional accountability, to protect both the integrity of the financial system and the informational autonomy of individuals in India's rapidly digitizing economy.

REFERENCES

Prevention of Money Laundering Act, 2002, No. 15 of 2003, INDIA CODE.

Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE.

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18 of 2016, INDIA CODE.

General Data Protection Regulation, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

Reserve Bank of India, *Master Direction – Know Your Customer (KYC) Direction, 2016* (updated 2024), RBI/DBR/2015–16/18, https://www.rbi.org.in.

Reserve Bank of India, *Video-Based Customer Identification (V-CIP) Guidelines*, RBI Circular (various updates), https://www.rbi.org.in.

Financial Action Task Force (FATF), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (2023), https://fatf-gafi.org.

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

K. **S. Puttaswamy v. Union of India (Aadhaar-5J)**, (2019) 1 SCC 1.

Schrems v. Data Protection Commissioner, Case C-362/14, 2015 E.C.R. I-nyr (CJEU).

Carpenter v. United States, 585 U.S. ___ (2018).

Reserve Bank of India, www.rbi.org.in.

UIDAI – Aadhaar, https://uidai.gov.in.

L. Tannan, *Tannan's Banking Law and Practice in India* (LexisNexis, 2022).

Udit Sharma, *Interplay Between Know Your Customer (KYC) Norms and Data Protection Laws in India*, 12 **Int'l J. Legal Sci. & Innovation** 45 (2020).