# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

# DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

**ISSN: 2582-6433**

# EDITORIALTEAM

## EDITORS

### Dr. Samrat Datta

*Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board*

### *Dr. Namita Jain*

*Head & Associate Professor*
*School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.*

*Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019*

**ISSN: 2582-6433**

## Mrs.S.Kalpana

Assistant professor of Law

*Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.*

## Avinash Kumar

*Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.*

ISSN: 2582-6433

# ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

# "A POST-LIBERALISATION ANALYSIS OF INDIA'S DIGITAL BANKING WITH REFERENCE TO DATA PROTECTION AND CYBERSECURITY"

AUTHORED BY - K.M.NANDITHA
Assistant Professor
ISBR Law College

CO-AUTHOR: - ASWATH REDDY
Assistant Professor
Patel Law College

## Abstract

India's journey to being a global leader in the digital banking space, is a result of the structural transformation that followed India's 1991 economic liberalisation reforms that were aimed at changing the kind of banking system that existed in India at the time (i.e. conventional banking) into a technologically up-to-date integrated digital financial system. In the past three decades, there has been an explosion of electronic banking (both consumer and business) and digital public infrastructure has grown exponentially through initiatives such as Core Banking Solutions (CBS) internet and mobile banking, Aadhaar and the Unified Payments Interface (UPI). This has enabled unprecedented financial inclusion, linking millions of people to the formal financial system through a more efficient and seamless way to conduct transactions and access financial services. In addition, government initiatives such as Digital India, along with the Pradhan Mantri Jan Dhan Yojana (PMJDY) strengthened India's digital public infrastructure and enabled the rapid expansion of cashless transactions and engagements with consumers.

Despite these remarkable advances, the digital banking ecosystem faces layered threats that endanger the safety, robustness and integrity of the financial system in India. The shift of sensitive personal and financial information into digital ecosystems has exposed customers and institutions to increasingly-sophisticated cyber threats, including phishing, identity theft, ransomware, synthetic identity fraud, malware exploitation, man-in-the-middle attacks, automated credential stuffing and AI-enhanced cyberattacks. Institutional failures to protect

ISSN: 2582-6433

against large-scale data breaches, unauthorized transactions and systemic security breaches have revealed that weak links in the chain in cybersecurity preparedness, regulatory oversight, institutional coordination and consumer knowledge from a particular perspective, among the socio-economically marginalized sections of society.

The present article provides an exhaustive examination of the normative framework for electronic banking in India, particularly focusing on data protection and cybersecurity in view of the growing risks posed by the digital environment. It begins with the constitutional protection and the recognition of privacy as a fundamental right under Article 21 in Justice K.S. Puttaswamy (Retd.) v. Union of India and explores legislative enactments like the Reserve Bank of India Act, 1934, Banking Regulation Act, 1949, Information Technology Act, 2000, Payment and Settlement Systems Act, 2007, Consumer Protection Act, 2019 and the Digital Personal Data Protection Act, 2023. The paper assesses regulatory guidelines issued by the Reserve Bank of India (RBI), operational frameworks developed by the National Payments Corporation of India (NPCI) and judicial determinations regarding institutional liability for the digital mediums of transactions.

India has an extensive legal and policy architecture to support the digital banking sector. Despite this, persistent enforcement gaps including limited capacity in cyber forensics, fragmented regulatory processes, outdated technological infrastructure for several banks and fast-evolving cyber threats continue to present significant obstacles. The article contends that harmonised governance frameworks, mandated compliance with cybersecurity, strong institutional capacity, resilient technology and broad-based consumer awareness are key components of India's digital future. The article ultimately concludes that the sustainability of India's digital banking development depends on embedding cybersecurity and data protection within the broader, overarching framework of financial governance which, in turn, will sustain systemic stability, protect consumer confidence and bolster India's global leadership in ethical and inclusive digital finance.

*Keywords: E-Banking, LPG, Data Protection, Cybersecurity, Financial Technology Regulation*

ISSN: 2582-6433

## Introduction

The banking landscape of India has experienced a transformative shift; moving away from informal indigenous financial systems, to a sophisticated technology-enabled ecosystem that accommodates one of the world's largest and most rapidly expanding digital payment systems. This shift was profoundly influenced by the economic liberalisation reforms of 1991, which represented a sea change to the principles of Liberalisation, Privatisation and Globalisation (LPG).[1] The reforms removed a number of inflexible regulatory structures, encouraged competition from private banks and foreign banks, increased autonomy of operations and encouraged technological innovation for the effective delivery of a public good to a society that was becoming rapidly modernised. The transition from experience-based, document-heavy banking systems to automated, electronic interfaces marked the beginning of electronic banking revolution in India.[2]

One of the most revolutionary outcomes of LPG was the institutionalisation of electronic banking, which fundamentally altered the delivery of financial services. Core Banking Solutions was a solution that did away with the geographical fragmentation in the past, allowing real-time processing of transactions across branch networks. The set of ATMs that proliferated in the 1990s and the introduction of internet banking and mobile banking in the early 2000s was the final step in increasing the accessibility of banking, enabling the consumer to conduct transactions at any time and any place.[3]

The digital revolution underwent a major watershed moment with the launch of the Unified Payments Interface (UPI) in 2016, an interoperable and real-time payments system that greatly increased the scope and speed of digital payments in India. The UPI system allows users to transfer funds almost instantaneously using only a simple identifier. It was poised to position India as a leader in the global digital payments space, while also helping boost financial inclusion in urban and rural areas alike.

Public policy undertakings contributed significantly to the expansion of the digital banking ecosystem. The Digital India program aimed to embed technology across governance and

[1] R. H. Patil, Evolution of the Indian Financial System and Liberalisation Reforms, 47 ECON. & POL. WKLY. 69 (2012).
[2] S. K. Mitra, Digital Banking in India: Theoretical and Empirical Perspectives, 55 J. FIN. ECON. POL'Y 145 (2022).
[3] N. Uppal, E-Banking in India: Challenges and Opportunities, 4 ASIA PAC. J. RES. 121 (2013).

ISSN: 2582-6433

public service delivery and the Pradhan Mantri Jan Dhan Yojana (PMJDY) established an almost universal banking architecture by providing zero-balance accounts to millions of previously unbanked citizens. The incorporation of Aadhaar-based biometric authentication, compounded by increasing smartphone penetration and the emergence of fintech intermediaries, augmented a tremendous digital infrastructure capable of processing high volumes of secure and inclusive financial transactions.[4]

However, the significant growth of digital banking has also generated new systemic vulnerabilities. The expanding digitisation of financial information places consumers and institutions under an increasingly diverse and nefarious array of cyber threats, including phishing, identity theft, ransomware attacks, data breaches, social engineering scams, automated credential stuffing and AI-enabled fraud. Many of these threats arise from human behavioural weaknesses, technological vulnerabilities or regulatory shortcomings, all of which substantially increase the risk to financial security and personal privacy. Sociocultural differences in digital literacy also increase these vulnerabilities, as certain groups can be more vulnerable to fraud and exploitation.

The fast-paced evolution of digital financial ecosystems calls for a legal framework that promotes innovation while providing appropriate consumer protection, data privacy and institutional accountability. The Indian legal system response has been multi-faceted, including constitutional jurisprudence, statutory laws, regulatory guidelines and judicial action. The enforcement of the right to privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India[5] offers a constitutional bedrock for the establishment of data protection standards for digital banking.[6] Statutory law, namely the Reserve Bank of India Act, 1934, the Banking Regulation Act, 1949, the Information Technology Act, 2000 and more recently the Digital Personal Data Protection Act, 2023, together will govern digital transactions, cybersecurity obligations, consumer protection obligations and data privacy issues in respect of the financial sector.

[4]Aadhaar Authentication Framework: Technical Overview 2020, UIDAI, (Nov. 07, 2025, 10:47 AM), https://uidai.gov.in/en/component/search/?searchword=Aadhaar%20Authentication%20Framework&searchphrase=all&limit=20

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

[6] U. Baxi, The Constitutional Right to Privacy and Its Implications for Digital Governance, 61 J. INDIAN L. INST. 75 (2019).

ISSN: 2582-6433

Regulatory circulars, master directions and cybersecurity frameworks from the Reserve Bank of India (RBI) all play an important role in operationalizing statutory mandates. They set out parameters for secure authentication, fraud monitoring, reporting requirements, tokenisation, encryption and grievance handling protocols for electronic financial service providers. Judgments by courts have also concretized liability for unauthorized usages, interpreted regulatory requirements and reaffirmed the responsibilities of banks to safeguard consumers.[7]

The gaps, however, remain. Fragmentation of regulation, discrepancies in enforcement, technological limitations of banks, inadequate cyber forensic capability and low levels of consumer awareness hamper the digital finance ecosystem's ability to safeguard protection. The continuous escalation of the sophistication of cyber threats many of which are evolving faster than institutional responses will require an integrated, future-focused governance structure that intertwines technological resilience, consistent compliance, coherent regulation and enhanced institutional capacity.

This article provides an in-depth review of these dynamics through the historical development of digital banking, the implications of liberalisation, the intricate cybersecurity challenges arising from digitisation and the legal regime for electronic banking in India. The analysis identifies significant gaps and suggests necessary reforms to ensure that India's digital financial journey will be inclusive, secure and robust. In the end, the sustainability and credibility of India's digital banking ecosystem is tied to integrating adequate legal, institutional and technological protections as necessary foundations of governance for the digital age.

## Historical Background of E-Banking in India

The history of banking in India has always been multi-faceted, an evolution of inquiry and financial accommodation that is deeply intertwined with India's own history. In the earliest years of financial transactions in India, informal methods, rooted in the community through schroffs, mahajans, seths, chettis and moneylenders, controlled the credit environment. These informal systems relied on trust, family and community reputation and local knowledge.[8] While formally unregulated and decentralized, they nonetheless played a crucial role in meeting urgent credit and deposit needs in the local economy. However, their disadvantages

[7] RBI v. Jayantilal N. Mistry, (2016) 3 SCC 525 (India).
[8] K.N. Ramesh, TRADITIONAL BANKING SYSTEMS IN INDIA: A HISTORICAL APPRAISAL 58–62 (Orient BlackSwan 2020).

ISSN: 2582-6433

unregulated, non-standardized, unreliable resolution of conflicts and potential for exploitation massively necessitated the establishment of defined, institution-based banking.[9]

The British colonial administration established a formal banking structure, notably in the establishment of the Presidency Banks of Bengal (1806), which preceded Bombay (1840) and Madras (1843) Banks.[10] While the earliest glimmers of formalized commercial banking, the Presidency Banks met the interests of the colonial trade and administration, with an urban focus which eliminated services to the majority of Indians. Despite national recognition connected with the formation of the Imperial Bank of India in 1921, the Presidency Banks had further eliminated public face and more sustained operations to the public.[11]

Post-independence in 1947, the Indian government attempted to steer banking towards national developmental objectives. The nationalisation of a majority of private banks in 1969 and again in 1980 was a significant turning point in India's banking and financial history.[12] The nationalisation program catered to the need of rural credit, equalising regional disparities in authority over banking and decisively moving from private motives for profit, towards goals of socio-economic development. Government facilitation of banks contributed to the dramatic expansion of bank branches and the distribution of formal financial service provision. By the 1980s, however, public sector banks experienced structural inefficiencies with respect to manual institutional treatments, bureaucratic resistance to change, presence of non-performing assets (NPAs) and lack of infrastructure.

The architecture of 1991's economic crisis produced a systemic shift administratively under the auspices of the LPG reforms. The LPG reforms represented a historical rupture with the period of state-dominated financial sectors, purporting opening banking sector activity to private entrants, permitting foreign investments, altering the regulatory conditions of banking and increasing competition. The recommendations of the Narasimham Committee provided a roadmap for modern banking reforms, advocating prudential norms, technology innovation,

[9] M. Lakshmi Kant Rao, EVOLUTION OF BANKING INSTITUTIONS IN INDIA 45–49 (Himalaya Publishing 2018).
[10] B.R. Sharma, BANKING IN BRITISH INDIA: INSTITUTIONAL EVOLUTION AND POLICY IMPACT 88–92 (Cambridge Univ. Press 2017).
[11] R. Kulkarni, The Presidency Banks in Colonial India: A Historical Review, 52 ECON. & POL. WKLY. 45, 47–49 (2017).
[12] Narasimham Committee I, Report of the Committee on Banking Sector Reforms, GOI, 12–15,1991.

ISSN: 2582-6433

reinforced regulation and efficiency in the market.[13]

One of the most significant impacts of LPG was technological modernisation. Once Automated Teller Machines (ATMs) were made available to customers in the early 1990s, they enjoyed a level of convenience unique to the period in banking. Customers could access cash and essential services at their convenience, 24/7. Technological modernisation accelerated in the late 90s and early 2000s, when banks began to implement Core Banking Solutions. CBS connected branch networks and provided real-time transaction processing. CBS broke down geographical barriers, created a standard experience across networks and facilitated the early stages of internet and mobile banking.[14]

Also, during this time, the development of electronic funds transfer systems like Electronic Clearing Service (ECS), Real-Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT) hugely reduced reliance on physical documents and allowed supplemental and faster settlement cycles.[15] Each of these systems represented in the initial stages the systems involved in electronic transaction frameworks within India and opened the door to more developed electronic payments systems.

The swift establishment of internet and mobile telephony, in turn, led to the next stage of evolving digital banking. Banks were adopting internet banking, a platform that enabled customers to handle myriads of banking transactions online and moving away from bank-centred banking. Mobile banking on mobile applications followed, offered accessibility to younger age groups, remote areas and users or customers, who utilized digital payments for the first time.[16]

The launch of UPI in 2016 was remarkable. UPI, which was developed by the National Payments Corporation of India (NPCI), allows fund transfers to be sent instantly and interoperable using simple identifiers, such as the mobile number or virtual payment address.

[13] R. Sridharan, Banking Sector Reforms in India: An Empirical Assessment, 38 INDIAN ECON. J. 115, 118–20 (1990).
[14] S.K. Gupta & R. Mittal, CORE BANKING SOLUTIONS: EVALUATION OF TECHNOLOGY ADOPTION IN BANKS 88–92 (PHI Learning 2015).
[15] C.S. Mohan & R. Manoharan, ELECTRONIC BANKING AND INFORMATION TECHNOLOGY IN INDIA 121–24 (Kunal Books 2018).
[16] Rajesh Kumar, MOBILE BANKING: EVOLUTION AND IMPACT ON FINANCIAL INCLUSION IN INDIA 67–72 (Routledge 2021).

ISSN: 2582-6433

The low-cost system and user-friendly architecture empowered users and democratized digital payments to a degree that even highly developed economies could not replicate in volume. UPI is now a global standard and benchmark in inclusive and secure digital payments.[17]

The government initiatives have operationalized significant strengths in the ecosystem. The Digital India initiative has accelerated the adoption of digital governance-related initiatives, delivered government services electronically and strengthened internet penetration. The PMJDY incorporated millions of previously unbanked persons within the formal financial space. Aadhaar-enabled biometric authentication ensured secure identity-based digital access.[18] Collectively, these efforts have established a large-scale digital public infrastructure that supports one of the largest digital financial ecosystems seen anywhere globally.

India's journey from informal moneylending practices to a technology-driven e-banking architecture illustrated a unique coupling of indigenous financial practices, institutional reform and public innovation. The historical development created an evolutionary baseline that continues to inform the incremental move towards modern digital banking systems with a design emphasis on efficiency, inclusion and technology resiliency.

## Impact of Liberalisation, Privatisation and Globalisation on E-Banking

The LPG reforms of 1991 ushered in a revolutionary paradigm shift in the banking space in India from a bureaucratic, centrally regulated system to a competitive, technology-enabled and globally reformulated banking system. The LPG reforms dismantled layers of bureaucratic state control, paved the way for greater participation of private entities, exposed banking aspects of operations to the best practices globally and created a milieu for technological, innovative banking. All these shifts in factorization of banking operations facilitated the emergence of India's electronic banking era and a consequential dynamic digital financial ecosystem.[19]

[17] Saurabh Agarwal & Vivek Mittal, UPI and the Transformation of Digital Payments in India, 57 ECON. & POL. WKLY. 42, 44–47 (2022).
[18] Department of Financial Services, Pradhan Mantri Jan-Dhan Yojana: Progress Report 2017, GOI, 8–12 (Nov. 16, 2025, 03:04 PM), https://pmjdy.gov.in.
[19] V. Raghavan, INDIA'S FINANCIAL SECTOR REFORMS: A HISTORICAL AND ANALYTICAL OVERVIEW 112–16 (Cambridge Univ. Press 2020).

ISSN: 2582-6433

### 1. Liberalisation

Liberalisation led to the relaxation of earlier restrictive regulatory frameworks, providing banks with increased functional freedom, for instance, in aspects such as determining their interest rates, opening new branches, diversifying their products and delivering services. This additional freedom put pressure on banks to enhance their efficiency and introduce modern technology to maintain competitiveness. The pressure to respond to customer needs eventually led to substantial investments in IT and automation. Consequently, the banking sector was quickly outfitted with ATMs, adopted Core Banking Solutions and began offering internet and mobile banking services. The liberalisation of banking also led to the development of IT-based risk management schemes and speeded the adoption of electronic fund transfer services (i.e., RTGS, NEFT, ECS) that provided the technological platform, to provide expanded e-banking services across banks in India.[20]

### 2. Privatization

Private banks also entered the Indian financial landscape as a result of the privatisation aspect of the LPG reforms. FICCI, HDFC and Axis brought global experience, modern infrastructure and an innovative and aggressive mindset that changed banking for Indian consumers. 24/7 access to customer service, user-friendly internet and mobile banking apps, SMS banking and OTP-based security and authentication were introduced as standard services. Private banks have brought instrumentation for detecting fraud and processes for monitoring in real time. The existence of nimble private banks pressured public sector banks into modernisation, upgrading legacy systems, digitizing internal processes and improving service levels.[21] Overall, privatisation has facilitated an intensification of customer-focused innovation and the pace of digital transformation within the banking sector.

### 3. Globalisation

Globalisation has connected India's banking systems to global financial markets, regulatory frameworks and technology standards. As Indian banks became more engaged with global trade and capital flows, they began to receive actual exposure to international standards of risk assessment, capital adequacy, governance and cybersecurity. Becoming internationally exposed also facilitated the adoption of the newest encryption tools in banking, secure

[20] S. Vardhan, IT-Driven Risk Management in Post-Liberalisation Indian Banks, 12 J. FIN. RISK MGMT. 144, 147–50 (2017).
[21] R. Chawla, INDIAN BANKING SECTOR REFORMS: A COMPREHENSIVE ANALYSIS 214–20 (Sage Publications 2021).

ISSN: 2582-6433

authentication systems and advanced cybersecurity protocols. In addition, banks began adopting technologies such as artificial intelligence, machine learning, biometrics, cloud computing and blockchain, improving the digital banking platforms' sophistication. Globalisation expanded the operational space for Indian banks, modernising India's digital finance ecosystem.[22]

The momentum generated by LPG reforms was self-reinforced by audacious government actions for financial inclusion and digital empowerment. The JAM Trinity Jan Dhan Yojana, Aadhaar and Mobile connectivity enabled a powerful ecosystem of direct benefit transfer and digital identification. The Digital India programme accelerated the spread of internet connectivity while also pushing for digital governance and access to online financial services. Similar to the JAM Trinity, the PMJDY cemented millions of unbanked individuals, into the formal banking system to enable digital finance on a broad scale. Aadhaar-enabled Payment Systems (AePS) provided a biometric authentication system that enabled secure financial services to even remote and rural areas. Together, these efforts pushed digital finance and e-banking to the forefront and became embedded in the daily lives of citizens in India.

UPI which was among the many post-LPG innovations, is possibly the most disruptive. Launched in 2016, UPI changed the game for digital payments in India by allowing instant, low-cost, interoperable payments using simple identifiers like mobile numbers and virtual payment addresses. It was cost-effective, simple to use and appealed to all strata of the public which led to mass adoption, rapidly increasing digital transactions. It created an entire ecosystem by linking banks, consumers, fintech players and merchants. UPI was not only a gamechanger for digital payments in India but also made the country a global leader in efficient and inclusive digital finance and other countries are seeking to replicate the Indian model.

Although LPG-enabled digital advances have truly transformed convenience and innovation (more so than a decade ago, at least), it has also expanded the threat environment. The pace of the digital infrastructure's growth widened the vulnerability surface with respect to banking systems. Increased connectivity and reliance on third-party fintech providers exposed banks to supply-chain risks and more frequent incidents of cyber insecurity. Phishing attacks, ransomware intrusion, malware compromise, identity theft and AI-enabled fraud increased,

[22] P.K. Jain & M. Kanojia, Globalisation and Cybersecurity Practices in the Indian Banking Sector, 13 INT'L J. FIN. STUD. 54, 57–60 (2021).

ISSN: 2582-6433

showcasing the elevated security risks. Large scale data breaches and sophisticated cyberattacks emerged as a frequent phenomenon that called for strong cybersecurity policy, high-level digital forensics and increased regulatory oversight. So, while LPG was the impetus behind the increased growth for digital banking, it also necessitated an even greater need for comprehensive cyber resilience and everywhere, strong legal frameworks. However, LPG reforms ignited India's digital banking revolution through creating innovation, competition, technological modernisation and integration with the global financial system. But LPG reforms also introduced complex cybersecurity risks, regulatory hurdles and systemic vulnerabilities that require continuous responsibilities to the law, technology and institutions. The digital momentum created through LPG brought about advanced e-banking systems and with them the challenges of protecting data and securing cyberspace became a little more complicated.

## Data Protection and Cybersecurity Challenges in E-Banking

India's journey from physical banking to digital banking since the post-LPG era and the rise of digital payment platforms like UPI has changed the very nature of how financial transactions are made, leaving us more exposed than ever to vulnerabilities. Cybercriminals are targeting digital banking systems, seeking to exploit behavioural patterns, institutional weaknesses, technological flaws and system disruptions. Each of the following challenges represents serious risks to India's e-banking ecosystem.

### 1. Phishing and Social Engineering Attacks

Phishing is, by far, the most prevalent digital threat affecting Indian banking customers. Attackers impersonate a bank or financial institutions through email, text message, website and voice calls and trick customers into sharing sensitive information like login credentials, OTP or card details. Phishing attacks rely on a form of psychological manipulation, leaving it largely ineffective against technological measures alone.[23] India has some of the highest rates of phishing attacks in the world scams frequently target UPI customers, senior citizens and rural customers. The 2016 Union Bank of India breach with a fraudulent phishing transfer attempt of USD 171 million illustrates the scale and sophistication of these attacks.[24]

[23] R.K. Singh & Ruchika Gupta, Cyber Frauds in Indian Banking Sector: Trends, Issues and Challenges, 54 INDIAN J. PUB. ADMIN. 295, 301–03 (2018).
[24] Suhasini Haidar & Manojit Saha, Hacked: How $171 Mn Stolen from Union Bank Was Recovered, THE HINDU, Apr. 16, 2017, at 1.

ISSN: 2582-6433

### 2. Malware and Ransomware Intrusions

Malicious software trojans, spyware and keyloggers threatens consumers and banks alike. Malicious actors will use malicious software (malware) to harvest login credentials, disrupt transactions and gain unauthorized access to digital systems.[25] The number of ransomware attacks is increasing, with attackers demanding ransom to restore banking data after encryption takes place. Ransomware attacks have stopped operations at several Indian banks, compromised customer information and resulted in large-scale forensic cleanup.[26] Some of the most recent attacks have started using what are referred to as double-extortion attacks; a tactic where the attacker steals data before encrypting systems and threatens to make the data public unless paid.

### 3. Man-in-the-Middle (MITM) Attacks

Man-in-the-middle (MITM) attacks happen when a hacker intercepts the interaction between a bank and the customer, typically via unprotected public Wi-Fi networks or hacked routers. The attacker can then, without the user's knowledge, approve a digital transaction or access sensitive financial information, which compromises its confidentiality. Considering that mobile banking apps and QR-based payments are becoming increasingly common, we are seeing an increase in MITM attacks, making stronger encryption and session-management protocols necessary.[27]

### 4. Distributed Denial-of-Service (DDoS) Attacks

More banks and digital payment services are experiencing DDoS attacks, where hackers flood servers with an overwhelming amount of traffic in an effort to shut down services. DDoS attacks often occur during high traffic periods salary days, festive seasons or periods of intensive UPI activity resulting in outages and eroded consumer confidence. Additionally, DDoS attacks have targeted some of the major banks in India, payment gateways and fintech aggregators, providing further evidence for the need for resilient server architecture and real-time defence systems.[28]

[25] M. Sharma, Cybersecurity in the Indian Banking Sector: Challenges and Responses, 12 J. BANKING & INS. L. 45, 49–52 (2021).
[26] CERT-In, Annual Report 2020, Indian Computer Emergency Response Team, Ministry of Electronics & Information Technology, Government of India (2021).
[27] S. Bhattacharya & R. Singh, Cybersecurity Risks in Indian Digital Payments, 14 INT'L J. INFO. SEC. & SYS. 33, 38–40 (2022).
[28] S. Pandey & A. Chatterjee, Cyberattacks on Indian Digital Payment Infrastructure: A Study of Patterns and Mitigation Strategies, 9 J. CYBER POL'Y 57, 63–65 (2022).

ISSN: 2582-6433

### 5. Identity Theft, Account Takeovers and Credential Stuffing

Stolen credentials, often incidence of data breach, are then used by cybercriminals to illicitly access accounts - this is referred to as account takeover (ATO). The size of India's digital footprint makes users in India particularly vulnerable to account takeover because credential combinations are easily automated and reused from an attacker's side following a simple credential stuffing attack - e.g. if a credential is stolen from an account that is used on multiple platforms, that stolen credentials can simply be put into other platforms. If consumers reuse passwords, credential stuffing will always work and multifactor authentication and behavioural analytics will always be needed to combat fraud.

### 6. AI-Powered and Automation-Based Attacks

The rise of AI-enabled cybercrime is a new frontier. Cyber criminals are now using AI to create adaptive hacking scripts, develop hyper-realistic phishing attempts, evade detection mechanisms and automate fraud attempts. AI is also being used to create synthetic identities a blend of stolen and artificial data which can be used to open fraudulent digital banking accounts. As AI technology continues to develop, its criminal applications become increasingly complex, heightening the need for AI-enabled defensive solutions.[29]

### 7. Large-Scale Data Breaches

One of the most damaging threats to India's digital banking space is the risk of data breaches. Breaches of financial data can be compromised for identity fraud, credit manipulation or sold on the dark web to malicious actors. Multiple banks and payment operators in India have endured data breaches, compromising lakhs of customer financial records. Problems such as insufficient encryption-legacy systems, third party risks and misconfigured servers have contributed to such breaches.[30] Data breaches also exacerbate the risk of social engineering, which can be further exacerbated with the use of the exposed records to target scams.

### 8. Legacy Infrastructure and Technological Obsolescence

Numerous public sector banks continue to maintain legacy Core Banking Solutions or encryption methods that were established several decades ago. Outdated encryption methods lack the capabilities to address contemporary cyber challenges, are incapable of real-time

[29] D. Maurer & T. DeMarco, AI-Driven Cyberattacks and the Future of Financial Crime Prevention, 18 J. FIN. CRIME 245, 252–55 (2021).
[30] PwC India, CYBERSECURITY IN FINANCIAL SERVICES: AN ASSESSMENT OF DATA BREACH TRENDS IN INDIA 8–14 (Price Waterhouse Coopers India 2022).

ISSN: 2582-6433

monitoring and may have undocumented vulnerabilities. Transitioning legacy systems to current technology can be heavy on the budget, extremely complicated and fairly slow often depending on the bureaucracy making it a matter of pressing urgency.[31]

### 9. Third-Party and Fintech-Related Risks

The growth of fintech bank partnerships has increased the attack surface area. Third-party vendors frequently function under lower security standards than banks, which adds risk to the supply chain. The data given to fintech apps, payment processors, KYC service providers and cloud service providers is vulnerable to exposure by vendor security controls (e.g., strong passwords, encryption), as they all have access to that data. Therefore, third-party risk management is one of the most important aspects of the governance of cybersecurity.[32]

### 10. Regulatory and Institutional Challenges

Inconsistent monitoring and enforcement of regulations occurs due to their fragmentation across multiple regulatory authorities - RBI, MeitY, CERT-In, NPCI, CCPA. Moreover, there is a shortage of trained professionals and cyber forensic experts, gaps in cross-border cooperation and long (and anecdotally, slow) investigative processes that are curtailing effective resolutions of cybercrimes. Finally, widespread (or pervasive) lapses in consumer digital literacy expand these risks - leaving many digital users' vulnerable exposure to everyday scams.[33]

As a result, India's e-banking cybersecurity domain is becoming more multifaceted and dangerous. Phishing, malware, man-in-the-middle attacks (MITM), denial-of-service (DDoS) attacks, identity theft, automation/cognitive threats, AI-driven attacks, data breaches, weak legacy systems and third-party risks combine in ever-evolving patterns requiring diverse, always-on, coordinated pre-emptive defenses. As a result, addressing these threats requires not just technical enhancements but systemic institutional reform and extensive improvement in digital literacy to strengthen India's digital financial frontier.

[31] Vivek Agarwal, BANKING TECHNOLOGY AND CYBERSECURITY: CHALLENGES FOR INDIA'S PUBLIC SECTOR BANKS 87–92 (Oxford Univ. Press 2021).
[32] Somasekhar Sundaresan, FINTECH LAW AND POLICY IN INDIA 133–38 (Eastern Book Co. 2022).
[33] N.S. Nappinai, TECHNOLOGY LAWS DECODED 412–18 (2d ed., LexisNexis 2022).

ISSN: 2582-6433

## Legal Framework

The statutory instruments together create the legal structure regulating e-banking in India, dictating certain aspects related to cybersecurity, data protection and consumer protection. The legal framework governing electronic banking in India is a multi-faceted structure consisting of legal guarantees, regulatory legal provisions, national policies and regulatory guidelines. Collectively, these layers support the concept of disallowing wrongdoing that arises from the convergence of technological innovations that deliver consumer benefits alongside the benefits of consumer protection, cybersecurity and institutional accountability. E-banking is increasingly consolidating its position in India's socio-economic environment and the law will continue to evolve to address challenges arising from new vulnerabilities associated with data protections, digital frauds and technology risk.

### 1. Constitutional Framework

The constitutional basis of India's digital banking regulation is paramount. In the case of Justice K.S. Puttaswamy (Retd.) v. Union of India, the Apex Court recognized the right to privacy as a fundamental right under Article 21, which requires all aspects of processing personal and financial data to satisfy the requirements of legality, necessity, proportionality and informed consent.[34] These requirements of personal and financial data processing create layers of accountability and obligations for banks, neobanks and fintech companies that routinely collect and process some of people's most sensitive financial information.[35] Further, Articles 14, 19 and 32 add additional layers of rights for digital consumers with guarantees of equality, freedom of trade and profession and access to constitutional remedies.[36] Any subsequent cases after Puttaswamy clarify that banks cannot delegate solely the burden of the loss from an unauthorized transaction to consumers, if the bank is negligent; nonetheless, consumers must still take reasonable care to report fraud.[37]

### 2. Reserve Bank of India Act, 1934

The Reserve Bank of India Act, 1934 constitutes the foundational law that regulates digital banking in India. Financial institutions are obliged to provide information necessary for the

[34] Supra note 5.
[35] Justice B.N. Srikrishna, DATA PROTECTION IN INDIA: A CONSTITUTIONAL & LEGAL ROADMAP 33–38 (Indian Law Institute 2020).
[36] H.M. Seervai, CONSTITUTIONAL LAW OF INDIA 1253–64 (4th ed., Universal Law Publishing 2013).
[37] Suhas Pai v. ICICI Bank, 2022 SCC OnLine NCDRC, p. 112 (India); (holding that banks must demonstrate absence of negligence to deny compensation for unauthorized electronic withdrawals).

ISSN: 2582-6433

RBI's oversight function, which is important in particular to monitor large electronic transactions.[38] Act empowers the RBI to give directions to financial institutions that are compulsory, therefore providing the statutory framework for regulations regarding cybersecurity, fraud prevention and electronic banking security procedures.[39] In addition, act allows the RBI to create regulations that are important to a framework for technology discipline, risk management and secure payments.[40] All these provisions enable the RBI to create Master Directions on various topics, such as tokenisation, KYC, card security, cyber incident reporting and the security of digital payments.[41]

### 3. Banking Regulation Act, 1949

The Banking Regulation Act, 1949 supports the RBI Act through grant of regulatory powers over banking activity, including the engagement of digital technologies. The RBI is now empowered to engage these regulatory powers over digital lending models and app-based credit systems as it covers consumer lending practices.[42] It also provides the RBI with the power to issue compulsory directions to banks under operational risk directives covering operational risk, incident management, fraud and cybersecurity preparedness.[43] The statutory powers support an expectation that financial institutions must maintain sufficiently secure digital interfaces and processes, multi-factor authentication, electronic verification of KYC compliance and protecting consumer interests in online banking environments.[44]

### 4. Information Technology Act, 2000

The IT Act, 2000 is the primary legal framework in India that provides for digital authentication, cybercrimes and recognition of electronic records. The act grants legal recognition to electronic records, allowing for paperless transactions such as, online banking statements, electronic contracts and communications associated with internet banking.[45] It also gives legal recognition to electronic signatures which provide a mechanism for online banking to utilise OTP-based authentication or Aadhaar enabled e-signatures.[46] The provision also

[38] Reserve Bank of India Act, 1934, § 45J
[39] Id. § 45L.
[40] Id. § 58.
[41] B. Vaidyanathan, TECHNOLOGY AND BANKING REGULATION IN INDIA 112–15 (Oxford Univ. Press 2020).
[42] Banking Regulation Act, 1949, § 21.
[43] Id. § 35A.
[44] Reserve Bank of India, Guidelines on Digital Lending (2022); RBI, Master Direction on KYC (2023).
[45] Information Technology Act, 2000, § 4(2).
[46] Id. § 5.

ISSN: 2582-6433

provides for cyber liabilities in the form of civil liability for unauthorised access including the criminal liability for hacking.[47] Further, digital banking fraud is addressed under this act for identity theft and online impersonation, which are frequently associated with phishing and UPI-based frauds.[48] Section 72 creates liability for breach of confidentiality and Section 70B establishes CERT-In and compels banks and payment intermediaries to report cybersecurity incidents. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, was notified under Section 43A and mandates banks to establish privacy policies, obtain informed consent, safeguard sensitive financial information and compensate customers for the negligence of the bank in the appropriate protection of the data.[49]

### 5. Payment and Settlement Systems Act, 2007

The act establishes statutory governance for the digital payment framework that exists in India, including RTGS, NEFT, IMPS and UPI.[50] The act requires authorization by the RBI for a payment system to operate, thereby ensuring that payment systems are digitally secure and meet compliance requirements.[51] IT also authorizes the RBI to issue binding instructions, which allows it to mandate interoperability, encryption standards, incident reporting and fraud monitoring.[52] Further, provision provides for the finality of settlement, meaning the digital transaction is hereby final and irrevocable once it has been completed.[53] The act emphasis penalties against operators of the payment system, increasing accountability across the fintech ecosystem, i.e., payment aggregators and digital wallet providers and their compliance with regulations, should their notifications or disclosures violate any legislative provisions.[54] These same provisions are essential elements of the RBI's deeper initiatives including Digital Payment Security Framework, Tokenisation and Compensation Frameworks for failed transactions.

### 6. Digital Personal Data Protection Act, 2023

The DPDP Act, 2023 establishes a comprehensive data governance framework that outlines

[47] Id. §§ 43, 66.
[48] Id. §§ 66C–66D.
[49] Pavan Duggal, CYBER LAW IN INDIA 54–61 (5th ed., Oxford Univ. Press 2021).
[50] S.R. Subramanya, PAYMENT SYSTEMS LAW IN INDIA 131–38 (2d ed., LexisNexis 2022).
[51] Payment and Settlement Systems Act, 2007, § 4.
[52] Id. § 10.
[53] Id. § 18.
[54] Id. § 23.

ISSN: 2582-6433

the manner in which banks and financial intermediaries store, collect and process consumer financial data. The act limits the processing of personal data to cases where consent is both specific, informed and explicit; thereby setting a high bar for lawful processing under a digital banking regime.[55] Further, builds upon this by imposing obligations upon data fiduciaries (banks) to take appropriate measures regarding data minimization, accuracy, limited storage, as well as maintaining adequate security safeguards, such as encryption or access limitations.[56] Additionally, increase consumers' autonomy by granting them rights to access, rectify, delete or obtain redress for their financial data.[57] Also, requires compulsory reporting of a breach to affected consumers and the Data Protection Board, hence ensuring transparency when personal data wells outside of the financial ecosystem due to breach or cyber-harmful events.[58] Together, these measures significantly improve privacy protections for consumers in India's e-banking landscape.[59]

### 7. Consumer Protection Act, 2019

The CPA 2019 builds upon customers' rights for consumers accessing online digital financial services. The language used captures the essence of banking in the definition of service, providing explicit reference and permitting customers to file complaints relating to deficiencies resulting from unsuccessful online transactions, unauthorized debits/deductions or any other service failure.[60] In addition, it is directly applicable to unfair trade practices associated with fintech advertisements, exploitative digital lending, undisclosed charges and deliberately misleading customer interfaces.[61] Finally, the Act permits the Central Consumer Protection Authority (CCPA) to identify systemic issues related to the use of digital financial platforms, while also ensuring consumer-centricity in a potentially unregulated electronic financial environment.[62]

### 8. Consumer Protection (E-Commerce) Rules, 2020

The rules broaden the scope of fairness and transparency mandates for fintech platforms, digital

[55] Digital Personal Data Protection Act, 2023, § 4.
[56] Id. § 8.
[57] Id. §§ 12–15.
[58] Id. § 20.
[59] Apar Gupta, DATA PROTECTION LAW IN INDIA: A COMMENTARY ON THE DPDP ACT 89–104 (Oxford Univ. Press 2024).
[60] Consumer Protection Act, 2019, § 2(42).
[61] Id. § 2(47).
[62] Avtar Singh, LAW OF CONSUMER PROTECTION 271–79 (Eastern Book Co. 2022).

ISSN: 2582-6433

payment applications, neo-banks and online lending interfaces.[63] E-Commerce Rules requires that relevant information, including fees and charges for services offered to the consumer, refund policies and terms and conditions for electronic transactions, is made clear and transparent to the consumer. This is particularly relevant for users of digital banking who will be made aware of UPI limits, internet banking charges, online EMI and dispute resolution policies.[64] Further it prohibits unfair trade practices, which include algorithms that engage in unfair trade practices, misleading representations and unauthorized sharing of data and requiring transparency concerning advertisements for digital loans.[65] Furthermore, the rule establishes that all e-commerce financial service providers must appoint a grievance officer and produce their contact details on their website and acknowledge and/or respond to complaints within a prescribed time frame. This adds further procedural accountability of digital financial service providers concerning all e-commerce consumers across India's digital financial service ecosystem.[66]

### 9. Bharatiya Nyaya Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023

The BNS, 2023 modernizes the criminal law so it can more effectively address the commission of cyber-enabled financial offences. The act broaden the nature of cheating, fraud, identity-based offences and impersonation to clearly include methods of committing these acts using electronic devices and online transaction platforms.[67] To these provisions, it adds value to prohibiting phishing, UPI fraud, SIM-swap attacks, vishing calls, OTP theft and fund diversion by social engineering.[68] In relation to this, the BSA, 2023 updates evidentiary law for the digital age. For example, it electronic records, including digital transaction logs, metadata, core banking entries, CCTV footage and electronic statements, as formal admissible evidence.[69] The act also removes hurdles for secondary admissibility of electronic evidence and introduces presumptions of the electronic records.[70] These new and amended provisions will build India's capacity to investigate and prosecute multi-layered complex cyber frauds that involve digital modes of banking.

[63] Paramjit S. Jaswal & Nishtha Jaswal, CONSUMER PROTECTION LAW: CASES AND MATERIALS 348–57 (N.M. Tripathi 2022).
[64] Consumer Protection (E-Commerce) Rules, 2020, r. 5.
[65] Id. r. 6.
[66] Id. r. 7.
[67] Bharatiya Nyaya Sanhita, 2023, §§ 316–320.
[68] K.N. Chandrasekharan Pillai, CRIMINAL LAW: COMMENTARY ON BHARATIYA NYAYA SANHITA 412–25 (Eastern Book Co. 2024).
[69] Bharatiya Sakshya Adhiniyam, 2023, § 61.
[70] Id. §§ 63, 65.

ISSN: 2582-6433

### 10. Negotiable Instruments Act, 1881 and Bankers' Books Evidence Act, 1891

The NI Act, 1881 incorporates technological advances within its broadening definition of cheques.[71] As modified, now also includes electronic cheques, as well as cheque images, thus allowing effective digital clearance via the Cheque Truncation System (CTS)[72] and extends the existing protection to banks collecting cheques in good faith, where the amendment to the Act provided for the collection of cheques processed electronically under CTS environments.[73] The entire scheme of the amended Act supports secure and technologically advanced cheque-based financial transactions. Alongside this, the Bankers' Books Evidence Act, 1891 has also enhanced the evidential value for digital transactions - by expanding the definition of "banker's books" to also include electronic ledgers, printouts, computer generated records or server-based data.[74] In addition, the act permits certified digital records to be treated as primary evidence; thus, enabling courts to robustly accept online statements, electronic logs and digital audit trails of activity or in disputes involving unauthorized transactions, cyber fraud or e-banking irregularities.[75]

### National Policies Supporting the Legal Ecosystem

National policy frameworks provide additional mechanisms to statutory mandates by advancing digital capacity and infrastructure and improving cybersecurity preparedness.[76] The National Cyber Security Policy (2013) promotes resilience, cybersecurity awareness and collaboration between government and private organizations. Similarly, the National Digital Communications Policy (2018) is committed to bolstering communications infrastructure that underpins digital banking. Likewise, the National Strategy for Financial Inclusion, 2019-2024 seeks to ensure universal access to digital financial services, particularly for rural populations. Finally, within this ecosystem, national payments policies evolve and allow for secure, interoperable functionality for India's high-volume digital payment systems.[77]

### Regulatory Guidelines

The Reserve Bank of India holds the principal regulatory responsibility for overseeing

[71] Avtar Singh, NEGOTIABLE INSTRUMENTS 137–42 (Eastern Book Co. 2019).
[72] Negotiable Instruments Act, 1881, § 6 (as amended).
[73] Id. § 131.
[74] Bankers' Books Evidence Act, 1891, § 2(3).
[75] Id. § 4; M.K. Sharma, LAW OF EVIDENCE: COMMENTARY ON BANKERS' BOOKS EVIDENCE ACT 212–18 (Universal Law Publishing 2020).
[76] Ramesh Bangia, INFORMATION TECHNOLOGY AND CYBERLAW 412–17 (Khanna Publishers 2021).
[77] Reserve Bank of India, Payment and Settlement Systems in India: Vision Document 2025.

ISSN: 2582-6433

electronic banking processes. The Reserve Bank of India has issued master directions and circulars that prescribe the factors to be followed, such as two-factor authentication, tokenisation of card data, fraud monitoring mechanisms, cybersecurity incident reporting, strong KYC norms and ongoing risk assessments.[78] The regulatory oversight of electronic banks is supplemented by the National Payments Corporation of India (NPCI), which manages systems such as UPI, IMPS, RuPay and AEPS, ensuring adherence to uniform technical and security standards.[79]

**Consumer Rights and Regulatory Protections**

The rights of consumers represent a significant aspect of the digital banking ecosystem within India. The Reserve Bank of India's Charter of Customer Rights enshrines important tenets, including the consumer's right to be treated fairly, access to clear disclosures, equitable access to digital services and physical banking services and timely grievance redress.[80] Legislation affords specific protections against unauthorized transactions and limits liability provided the consumer has reported the transaction in a timely manner and with reasonable care.[81] Privacy protections, based upon both statutory and constitutional principles, involve the processing of personal data with consent and secure processing via encryption, access controls and standardized data management practices.[82]

Grievance portals, such as the Integrated Ombudsman Scheme, have been established to provide structured pathways for consumers to raise complaints about failed transactions, deficiencies in service, unauthorized debits and delays.[83] While these protections are available, there remain substantial gaps with respect to consumer awareness, digital literacy and institutional compliance in an equitable manner - particularly at smaller regional banks with limited capabilities in cyberterrorism-related issues.[84]

Given a firm legal and regulatory framework, there are different levels of enforcement.

[78] Reserve Bank of India, Master Direction on Digital Payment Security Controls (2021); RBI, Master Direction – Know Your Customer (KYC) (updated 2023).
[79] National Payments Corporation of India, UPI Procedural Guidelines (2022); NPCI, IMPS & AEPS System Standards (2021).
[80] Reserve Bank of India, Charter of Customer Rights (2014).
[81] Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions (2017).
[82] Supra note 34; Digital Personal Data Protection Act, 2023, §§ 4, 8.
[83] Reserve Bank of India, Integrated Ombudsman Scheme (2021).
[84] NITI Aayog, Digital Banking and Financial Inclusion: Assessment Report 41–47 (2022).

ISSN: 2582-6433

Oversight has evolved into a patchwork of federal, state and local jurisdictions by multiple entities; and, the cybersecurity forensic capacities are often non-existent. Enabling functions of third-party service providers have operational challenges that enhance the risk of computer-enabled fraud. As cyber threats are moving quickly, consumer education has not kept up which is increasing their susceptibility to fraud and will have a downward effect on the speed at which they receive grievance redress.

## Suggestions and Future Direction

India's regulation of digital banking, while comprehensive, is often disjointed and reactive to new issues, indicating the need for reform that is both urgent and follows a forward-looking approach.

One of the first recommendations would be to create an umbrella authority focused on the regulatory aspects of cyber-finance to be responsible for regulation on banking, fintech and data protection purposes. This rule-making umbrella would help to streamline the rule-making process, reduce jurisdictional overlap both among the RBI, Ministry of Electronics & IT and as well as sector-specific regulators and allow for consistent administration of cyber and data protection. Developing some degree of harmonisation would lead to diminished regulatory arbitrage and provide more transparency in compliance requirements for businesses operating at this intersection of finance and technology.

Mandatory, fully enforceable compliance regulation for cybersecurity is also necessary. This should encompass controls with multiple layers of security such as: end-to-end encryption, multi-factor authentication, identity and access management, network micro-segmentation and continual security monitoring. The regulation should also require the use of AI-based threat detection systems, if feasible, that would proactively block breaches, rather than just waiting for some breach to fully materialize. Further, standardisation of tokenization of sensitive payment data and mandated electronic disclosures of serious issues should also be considered. Lastly, enforcement measures must allow for penalties to be meaningful, in order to promote responsible operation of compliance obligations.

It is important to strengthen institutional capacities. This entails developing frontline cyber forensic capabilities in enforcement agencies, creating inter-agency collaboration frameworks to facilitate real-time intelligence sharing and developing robust mechanisms for the efficient

ISSN: 2582-6433

investigation of cross-border cyber-crime and the sharing of evidence. Investment in skilled human resourcing, technology and training is the essential foundation for maintaining regulatory effectiveness against sophisticated attackers.

Also, there is a need for consumer education across a broader environment to enhance digital literacy, fraud awareness and financial safety practices. There is also the need for consumer education that specifically targets rural and vulnerable users at greatest risk of exploitation. The Government, financial institutions and the civil society should work together to deliver awareness campaigns in multiple languages, accessible public engagement programs, paired with simplified and user-friendly information about living and working safely in the digital economy.

As evidenced, the regulatory framework must also be a facilitator of the safety and effectiveness of the use of technology and innovation, for instance, using blockchain technologies that allow for secure and transparent transaction ledgers; “smart” AI models for fraud detection; and cloud infrastructure solutions that are compliant with data privacy standards. Ultimately, however, the innovations are to support the safest, largest solution space, while remaining compliant with regulations, all serving to enhance the overall stability of financial institutions.

Avoiding regulatory inaction means ensuring that the merits of the technolgy-level risk are understood, society is prepared to accept and manage the associated risk; including an active enforcement regime through Canadian action, where appropriate. We need to amend the Information Technology Act to create explicit offense provisions for AI-enabled fraud, synthetic identities and smart contracts disputes. In decentralized digital finance, jurisdictional challenges require international cooperation and treaty implementation. Establishing clear statutory requirements requiring organizations to notify the public of a known data breach and statutory frameworks to articulate the responsibility of actors in complex cyber incidents would close existing gaps.

Thus, it is only through this will we create a digital banking ecosystem that is robust and balances the needs of innovation with consumer powers whilst maintaining a high level of systemic security. Being proactive in regulatory design and fortifying institutional preparedness through prevention, recovery and resilience mechanisms would go a long way in

ISSN: 2582-6433

securing India's digital financial future in fast evolving technology change.

## Conclusion

The post-liberalisation digital banking revolution in India will go down as one of the biggest transformations in the financial history of the country, enhancing accessibility, efficiency and economic inclusion in an unprecedented manner. Significant advances in technology, notably Core Banking Solutions, internet and mobile banking, alongside the rapid growth of the UPI, has positioned India as the foremost country in the world in terms of digital payments and financial innovation. However, with the technological transformation that has enabled financial services, it has also generated new complexities and vulnerabilities that now peril the integrity, stability and trust in the digital banking ecosystem.[85]

The legal framework for e-banking, which is case studied in the context of the constitutional provisions and further strengthened by legislative statutes lays a better foundation. Judiciary developments, particularly in the form of the Apex Court articulating the right to privacy under Article 21 in the Puttaswamy verdict, advance and reinforce the necessity of data protection and procedural fairness in digital financial services. The RBI Master Directions, NPCI guidelines and regulatory circulars give effect to these legislative mandates to shape the operations of e-banking platforms.

Despite this legal framework being relatively mature, enforcement gaps continue to exist, undermining its effectiveness. Fragmented regulatory oversight, complex institutional jurisdictions, narrow cyber forensic capabilities and variations in compliance by banks and fintech intermediaries create barriers for timely and coordinated action to address cyber threats. Cyberattacks continue to grow in sophistication from AI-enabled fraud to synthetic identity. The current regime does not provide ongoing, real-time protection from these threats. Meanwhile, lower levels of digital literacy and awareness in large portions of the population leads to more vulnerabilities, while attackers leverage behavioural weaknesses rather than technological shortcomings.

In order to baseline this evolving challenge, India's digital banking ecosystem should transition from a reactive, institutional standpoint to a coordinated, systemic and forward-thinking basis.

[85] R. Kannan, *Digital Banking in India: Technology, Transformation and Trends* 287–301 (Oxford Univ. Press 2021).

ISSN: 2582-6433

A unified cyber-finance regulatory body can coordinate oversight of banking, fintech, data privacy and payments systems. Reinforcing statutory cybersecurity obligations - such as Zero Trust architecture, mandatorily using multi-factor authentication, standardized tokenisation approaches, uniform breach reporting requirements could help boost the resilience of individual institutions. Increased investments into cyber forensic capabilities, inter-agency intelligence sharing and investigative capabilities will strengthen enforcement.

Consumer empowerment through long-term national digital educational efforts, multilingual campaigns focused on cyber safety and simple, transparent grievance redressal portals will be equally important. Legal reforms must continue to evolve, along with technology, to address gaps related to AI-driven fraud, cross-border digital crime and emerging avenues for fintech innovation to ensure holistic regulatory coverage.

Ultimately, the continued evolution of India's digital banking landscape is contingent not solely on the technology but also on establishing cybersecurity and data protection provisions as foundational elements of its financial architecture. A rights-based, legally coherent, technological and adaptive framework will be necessary to protect consumer interests, ensure financial stability to maintain India's status as a global leader in the area of inclusive digital finance.[86] In this regard, India's legal and regulatory evolution will need to remain adaptable, anticipatory and technologically capable of ensuring that digital banking remains an avenue for inclusive growth and no source of systemic risk.

[86] R. Kannan, DIGITAL BANKING IN INDIA: TECHNOLOGY, TRANSFORMATION AND TRENDS 287–301 (Oxford Univ. Press 2021).