INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CYBERSECURITY AND DATA PRIVACY IN THE INDIAN FINANCIAL SECTOR: A MULTI-CASE ANALYSIS OF BREACHES AND LEGAL FRAMEWORKS

AUTHORED BY - AMOGH SHUKLA
(B.A.LL.B.)
Law Student at Amity University, Noida, Uttar Pradesh.

Abstract

The financial sector is one of the leading targets of advanced cyber attacks as India is rapidly moving towards digitisation. This paper reviews some critical incidents that happened in the State Bank of India (SBI), Aadhaar, MobiKwik, and Juspay. This study shows the vulnerabilities at the system level of India's digital ecosystem by examining these incidents in light of the Information Technology Act (2000), the Digital Personal Data Protection Act (2023), and judicial precedents. The study finds that although legal frameworks are developing, there are still many issues to address for financial stability and consumer trust, such as corporate accountability, transparency of reporting breaches, and strong encryption.

1. Introduction

The shift towards a "Digital India" has transformed the financial landscape by making it more inclusive, but it has also created a bigger target for cyber criminals. Financial institutions, the holders of highly confidential personal data, are under mounting pressure to be innovative whilst being secure. This paper assesses the nexus between technology, law and corporate responsibility on the basis of four historic case studies and a study of Indian privacy jurisprudence.

2. Case Studies of Major Financial Data Breaches

2.1 State Bank of India (SBI): The Vulnerability of Centralization

In 2019, an unprotected server in SBI's Mumbai data center exposed the personal information of millions of customers. The breach revealed account balances and masked account numbers due to a fundamental lack of password protection and encryption protocols.

ISSN: 2582-6433

- **Legal Implications:** Under **Section 43A of the IT Act (2000)**, corporate entities are liable for negligence if they fail to implement "reasonable security practices." The SBI incident exemplifies a failure to meet the standards set by the **IT Rules (2011)** and RBI's cybersecurity frameworks.
- **Key Lesson:** Centralized storage systems represent single points of failure. The incident underscores the necessity of decentralized security and mandatory breach notification.

2.2 The Aadhaar Ecosystem: Systemic Flaws and Third-Party Risks

Unlike isolated hacks, Aadhaar's data exposure often stems from systemic vulnerabilities, such as insecure government portals and unauthorized third-party access points.

- **Legal Analysis:** In *Puttaswamy (Aadhaar-5J) v. Union of India*, the Supreme Court emphasized that data collection must pass the tests of legality, necessity, and proportionality. Despite the **Aadhaar Act (2016)**, the involvement of numerous private and public stakeholders complicates the enforcement of uniform security standards.

2.3 MobiKwik: The Crisis of Corporate Transparency

The 2021 MobiKwik breach, allegedly affecting 100 million users, highlighted a significant gap in corporate accountability. Despite evidence of data appearing on the dark web, the firm initially denied the breach.

- **Policy Conflict:** This denial highlights the conflict between a firm's reputational interests and the user's right to know. The **Digital Personal Data Protection Act (2023)** now addresses this by mandating breach notifications to the Data Protection Board and affected individuals.

2.4 Juspay: Third-Party Intermediary Risks

The 2020 Juspay breach exposed 100 million records. While the company utilized encryption for sensitive card details, the leak of email addresses and phone numbers demonstrated that encryption is only one component of a holistic defense strategy.

- **The Intermediary Dilemma:** As a payment gateway, Juspay sits between merchants and banks. This multi-layered structure makes assigning liability difficult, necessitating clear contractual obligations regarding data security.

ISSN: 2582-6433

3. The Judicial Landscape: Key Precedents

Indian courts have been instrumental in defining the boundaries of digital privacy. The following table summarizes the foundational cases that govern data protection today:

Case Law	Legal Principle Established
K.S. Puttaswamy (2017)	Established Privacy as a Fundamental Right under Article 21.
Canara Bank v. Collector (2005)	Upheld privacy of financial and banking records.
Shreya Singhal v. UOI (2015)	Clarified intermediary liability and digital freedom of expression.
Karmanya Singh Sareen (2017)	Highlighted the necessity of informed consent in data sharing (WhatsApp case).
Avnish Bajaj v. State (2008)	Discussed corporate and individual liability for online offenses (Bazee.com case).

4. Discussion: Regulatory Gaps and Challenges

The analysis of these cases reveals three recurring themes:

1. **Enforcement Deficit:** While the **RBI** and **CERT-In** provide guidelines, the lack of public enforcement actions following major breaches weakens the deterrent effect of the law.
2. **The Transparency Gap:** Organizations often prioritize reputation over disclosure, preventing users from taking mitigative steps like changing passwords or monitoring for identity theft.
3. **Technological Obsolescence:** As seen in the SBI and Juspay cases, "reasonable security" is a moving target. What was secure five years ago is now insufficient.

5. Conclusion

The evolution from the Information Technology Act (2000) to the Digital Personal Data Protection Act (2023) marks a shift toward a more robust data sovereign regime in India. However, the case studies of SBI, Aadhaar, MobiKwik, and Juspay serve as a reminder that legislation is only as effective as its implementation. Financial institutions must move beyond compliance based security to a "security by design" culture. Strengthening corporate accountability, mandating transparency, and adopting advanced encryption are essential steps to safeguarding India's digital future.

ISSN: 2582-6433

References

1. The Information Technology Act, 2000 (Act 21 of 2000), s. 43A.
2. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3.
3. Reserve Bank of India, "Master Direction on Information Technology Framework for Banks" (RBI, 2016).
4. The Digital Personal Data Protection Act, 2023 (India).
5. Justice K.S. Puttaswamy (Aadhaar5J.) v. Union of India, (2019) 1 SCC 1.
6. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (India).
7. The Information Technology Act, 2000 (Act 21 of 2000), s. 43A.
8. The Information Technology Act, 2000 (Act 21 of 2000), s. 43A.
9. Peter Carey, Data Protection: A Practical Guide 103 (Oxford University Press, Oxford, 2018).
10. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
11. Justice K.S. Puttaswamy (Aadhaar5J.) v. Union of India, (2019) 1 SCC 1.
12. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
13. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
14. District Registrar and Collector v. Canara Bank, (2005) 1 SCC 496.
15. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
16. Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
17. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
18. Google India Pvt. Ltd. v. Visaka Industries, (2020) 4 SCC 162.
19. MySpace Inc. v. Super Cassettes Industries Ltd., 2017 SCC OnLine Del 12108.
20. Avnish Bajaj v. State (NCT of Delhi), 150 (2008) DLT 769
21. Christian Louboutin SAS v. Nakul Bajaj, 2018 SCC OnLine Del 12215.
22. Karmanya Singh Sareen v. Union of India, 2017 SCC OnLine Del 10860
23. X v. Hospital Z, (1998) 8 SCC 296.
24. Selvi v. State of Karnataka, (2010) 7 SCC 263.