

CHAPTER 9

Cyber Security and Artificial Intelligence in Financial Systems: Confronting AI-Driven Threats to India's Digital Infrastructure

Rajakulasekharan V and Kaushik Sundararajan S

in *Law in Transition: Rights, Sovereignty and Regulation in a Changing World*, edited by Siddharth Saxena and Bhagyashree Agarwal (VidhiAagaz 2026), pp. 97–107

DOI <https://doi.org/10.63108/VAB.LIT.1.9>



CITATIONS

BLUEBOOK (21ST ED.)

Rajakulasekharan V & Kaushik Sundararajan S, *Cyber Security and Artificial Intelligence in Financial Systems: Confronting AI-Driven Threats to India's Digital Infrastructure*, in *LAW IN TRANSITION: RIGHTS, SOVEREIGNTY AND REGULATION IN A CHANGING WORLD* 97 (Siddharth Saxena & Bhagyashree Agarwal eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Rajakulasekharan V and Kaushik Sundararajan S, 'Cyber Security and Artificial Intelligence in Financial Systems: Confronting AI-Driven Threats to India's Digital Infrastructure' in Siddharth Saxena and Bhagyashree Agarwal (eds), *Law in Transition: Rights, Sovereignty and Regulation in a Changing World* (VidhiAagaz 2026) 97.

CHICAGO (17TH ED.)

Rajakulasekharan, V, and Kaushik Sundararajan S. "Cyber Security and Artificial Intelligence in Financial Systems: Confronting AI-Driven Threats to India's Digital Infrastructure." In *Law in Transition: Rights, Sovereignty and Regulation in a Changing World*, edited by Siddharth Saxena and Bhagyashree Agarwal, 97–107. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LIT.1.9>.

APA (7TH ED.)

Rajakulasekharan, V., & Sundararajan, K. S. (2026). Cyber security and artificial intelligence in financial systems: Confronting AI-driven threats to India's digital infrastructure. In S. Saxena & B. Agarwal (Eds.), *Law in transition: Rights, sovereignty and regulation in a changing world* (pp. 97–107). VidhiAagaz. <https://doi.org/10.63108/VAB.LIT.1.9>

SOURCE

<https://doi.org/10.63108/VAB.LIT.1.9>

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CHAPTER 9

Cyber Security and Artificial Intelligence in Financial Systems: Confronting AI-Driven Threats to India's Digital Infrastructure

RAJAKULASEKHARAN V* AND KAUSHIK SUNDARARAJAN S**

The rapid integration of artificial intelligence (AI) into the financial systems, particularly in banking and payment infrastructure, has significantly intensified cybersecurity risks. While the existing legal framework provides a regulatory structure, it fails to address the AI driven risks. While the Digital Personal Data Protection Act, 2023 regulates data processing obligations and the Information Technology Act, 2000 provides a framework governing cyber offences, both the statutes operate within a technologically narrow paradigm which fails to take into account adversarial AI attacks, automated fraud, and algorithmic manipulation within financial ecosystems.¹ This gap in the law creates ambiguity in assigning liability, where responsibility for AI-driven cyber incidents causing financial loss is unclear and often diffused across developers, financial institutions, and intermediaries without clear standards.²

The paper seeks to investigate this contradiction through statutory interpretation, regulatory practices, and judicial precedents, particularly in the case of Shreya Singhal v. Union of India, where the Supreme Court of India underscored the necessity of precision in regulating technologically mediated conduct.³ It further examines how the regulatory approach of the Reserve Bank of India addresses cybersecurity risks in financial systems but fails to incorporate AI-specific accountability mechanisms, resulting in fragmented and ineffective governance. The paper adopts a doctrinal methodology that combines statutory interpretation, policy review, and comparative analysis to show that existing liability doctrines lack the essential structure to deal with autonomous AI driven cyber harms.

The analysis establishes that cybersecurity failures in financial systems arise not only from technological vulnerabilities but also from statutory design limitations, necessitating a risk-based, AI-specific regulatory framework aligning liability, institutional accountability, and adaptive governance.

Keywords: Algorithmic accountability, Digital Financial Infrastructure, AI Driven cyber threats, Cybersecurity regulation, Cyber risk attribution

* Student at Tamil Nadu National Law University, Tiruchirappalli, Tamil Nadu, India.

** Student at Tamil Nadu National Law University, Tiruchirappalli, Tamil Nadu, India.

¹ Rajat Bhandari, *AI and Cybersecurity: Opportunities, Challenges, and Governance*, SSRN ELEC. J., at 5–7 (2025).

² Kapoor, *Adversarial Machine Learning Attacks in Cybersecurity Systems*, SSRN ELEC. J., at 8–10 (2023).

³ Shreya Singhal v. Union of India, (2015) 5 SCC 1, ¶¶ 87–90.

1 INTRODUCTION

The incorporation of Artificial intelligence on financial systems has changed the very nature of cybersecurity risks by embedding autonomous and data-driven decision-making within the banking and payment infrastructure. Apart from conventional cyber threats which are premised on unidentifiable unauthorised access or manipulation, AI driven cyber-attacks act through adaptive learning processes that obscure causation, intent, and execution. This transformation of cyber-attacks on banking systems challenges the foundational assumptions of existing legal framework which still rely on traceable human conduct and attribution.⁴ The rapidly changing Indian financial system and digital economy are governed by statutory frameworks such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, which regulate cyber offences and data processing obligations.

However, the legal framework of both these acts is anchored in certain sections such as Sections 43 and 66 of the Information Technology Act, which deal with unauthorised access and computer related offences,⁵ and sections 5 and 8 of the Digital Personal Data Protection Act, which impose limitations regarding lawful data processing and purpose limitation.⁶ These provisions operate within a narrow technological framework and have a static conception of risk, dealing with identifiable concerns and misconduct without accounting for autonomous decision-making systems which are capable of producing unpredictable outcomes.⁷ These statutes do not account for adversarial machine learning or autonomous AI behaviour.

The stance taken by the court and the judicial reasoning in India has also emphasised the necessity of proportion and precision in technologically mediated content. In the case of *Anuradha Bhasin v. Union of India*, the Supreme Court underscored the importance of narrowly tailored regulatory responses.⁸ Similarly the constitutional recognition of privacy of information in the case of *Justice K.S. Puttaswamy v. Union of India*, highlighted the evolving interface between technology and legal accountability.⁹

This paper seeks to analyse how the AI driven cyber within the financial systems in India generate a regulatory contradiction where the legal framework has ambiguity on who is liable in the case of technologically advanced harms. It adopts a doctrinal methodology

⁴ Ian J. Goodfellow, Jonathon Shlens & Christian Szegedy, *Explaining and Harnessing Adversarial Examples*, arXiv:1412.6572, at 3–5 (2014).

⁵ Information Technology Act, 2000, §§ 43, 66.

⁶ Digital Personal Data Protection Act, 2023, §§ 5, 8.

⁷ Nicolas Papernot, Patrick McDaniel, Somesh Jha, Matt Fredrikson, Z. Berkay Celik & Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, arXiv:1511.07528, at 8–10 (2015).

⁸ *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637, ¶¶ 70–75.

⁹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶¶ 180–183.

combining statutory and regulatory analysis to show that the existing legal framework dealing with technological crimes in the financial system is conceptually ill equipped to assign liability in such a context.¹⁰ The analysis additionally considers regulatory regimes in India, particularly those relating to cybersecurity institutions, to demonstrate how regulatory mechanisms remain fragmented and are inadequate for dealing with AI risks.¹¹

1.1 Literature Review

The existing body of literature examining the intersection of Artificial Intelligence (AI) and cyber security within the financial systems reveals significant analytical fragmentation, especially in addressing structural inadequacies and accountability gaps. Tapesh Meghwal, in his article “*Emerging Challenges in Regulating Artificial Intelligence Under Cyber Security Laws in India*,” analyses the limitations of Indian cyber security laws in dealing with AI driven attacks on financial systems, highlighting the issues of algorithmic opacity and the lack of liability attribution mechanisms, yet the analysis remains limited as it does not extend to sector-specific financial vulnerabilities. Similarly Ian Goodfellow in his work “*Explaining and Harnessing Adversarial Examples*,” demonstrates the susceptibility of AI systems to adversarial manipulation, establishing the unpredictability and instability of algorithmic outputs, yet the work remains highly confined to technical analysis without engaging with legal accountability framework.

The article titled “The Limitations of Deep Learning in Adversarial Settings,” a work done by Nicolas Papernot, further develops the argument stated in Ian’s article by formalising adversarial threat models, but does not engage with the translation of these technological vulnerabilities into questions of legal responsibility. Dr. Richa Singhal and Priyanka Bargujar in their work “Emerging Financial Scams In The Indian Banking Sector: Challenges And RBI’s Preventive Framework,” evaluate RBI’s preventive framework but overlooks implementation challenges. The article titled “Impact of Cyber-Attacks on Banking Institutions in India: A Study of Safety Mechanisms and Preventive Measures,” authored by Adarsh Mundhra analyses cyber threats within the banking sector by highlighting vulnerabilities, however the study lacks empirical validation to substantiate the effectiveness of the proposed reforms.

¹⁰ Tapesh Meghwal, *Emerging Challenges in Regulating Artificial Intelligence Under Cyber Security Laws in India*, SSRN ELEC. J. (Sept. 4, 2024), at 5–7.

¹¹ Reserve Bank of India, *Cyber Security Framework in Banks*, <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0> (last visited Apr. 14, 2026).

1.2 Objectives of the Study

- 1) To critically evaluate how the cybersecurity and data protection laws in India are inadequate in addressing AI driven threats within the financial system.
- 2) To analyse the attribution deficit in existing legal framework in assigning liability for AI driven cyber incidents within the financial systems.
- 3) To construct a risk-calibrated and AI-specific legal framework aimed at addressing gaps in cybersecurity governance and liability attribution within financial systems.

2 AI DRIVEN CYBER THREATS AND THE TRANSFORMATION OF LEGAL RISK

The application of artificial intelligence to financial systems has fundamentally changed cybersecurity risk by introducing autonomous decision-making into banking and payment systems. In contrast to the traditional cyber threats based on human identifiable intervention, AI-driven threats are developed by self-learning algorithms and do not require direct management by humans. This change calls into question the traditional thinking on traceability and the foreseeable behaviour of systems, which has been the basis of cybersecurity regulations.¹²

This means that traditional approaches to the cyber risk assessment lose their effectiveness as the system's behaviour changes without prior software programming.¹³ The opacity of more complex AI systems hinders the capability to trace the thinking that went into the generation of these algorithms. Complex neural networks are often used as 'black-box' systems without easy-to-understand internal logic that can be easily interpreted by regulators and financial institutions. Without meaningful interpretability, it is difficult to comprehend the behaviour of algorithms when it comes to fraud detection, automated credit assessment and payment authentication. While the Delhi High Court in *Avnish Bajaj v. State (NCT of Delhi)*¹⁴ acknowledged the importance of traceability for assigning the responsibility of intermediaries, the concept of AI systems does a complete undermining of the factual assumptions that lie behind traceability.

Adversarial manipulation is another example of the way AI is changing cyber risk from its traditional perimeter defence approach. The hazards of AI-based systems are even more enhanced in financial systems through adversarial manipulation that exploits system vulnerabilities but does not cross the external security boundaries.¹⁵ Adversarial attacks exploit

¹² Goodfellow, Shlens & Szegedy, *supra* note 4, at 3–4.

¹³ Papernot, McDaniel, Jha, Fredrikson, Celik & Swami, *supra* note 7, at 9.

¹⁴ *Avnish Bajaj v. State (NCT of Delhi)*, 150 (2008) DLT 769, ¶¶ 20–24.

¹⁵ *What Is Adversarial Machine Learning?*, IBM, <https://www.ibm.com/think/topics/adversarial-machine-learning> (last visited Apr. 15, 2026).

vulnerabilities in a system by tweaking input parameters in a way that affects the output of the model without violating any security perimeters outside of the system, and thus can uncover risks not traditionally identified by cybersecurity against an external adversary.¹⁶ This intersection of autonomy, adaptability, and opacity shows that AI not only introduces new forms of cyber risk but also transforms how legal responsibility is assessed. These characteristics fundamentally undermine predictability, traceability and transparency.

3 FAILURE OF EXISTING LEGAL FRAMEWORK

India's current statutory framework which governs cybersecurity was enacted to regulate cyber offences and personal data protection instead of autonomous behaviour of AI systems. Consequently, the present regime also addresses human-directed cyber misconduct but remains silent on the regulation of AI model behaviour after deployment. This omission represents not only a technical limitation but a statutory one as contemporary AI financial systems continue to evolve through model adaptation while operating outside a dedicated legal framework governing their post training conduct.¹⁷

3.1 The Information Technology Act 2000

In India, the Information Technology Act 2000 is the primary law under which digital governance inside the country currently is governed. The IT Act primarily focuses on unauthorised criminal access, data theft and other related cyber offences through provisions such as sections 43 and 66 of the Act. However these provisions are only for unauthorised human conduct and not for autonomous algorithmic behaviour. The act neither defines AI systems nor prescribes legal obligations governing model deployment, algorithmic modification or post deployment supervision. Consequently, when harm arises from algorithmic model behaviour instead of human intervention, the statutory framework does not provide any mechanism for regulating the legality of that behaviour itself.

3.2 The Digital Personal Data Protection Act, 2023: The Illusion of AI Accountability

Unlike the IT Act, the Digital Personal Data Protection Act, 2023 governs the collection, processing, and retention of personal data. Its regulatory architecture is therefore data centric rather than model-centric, leaving the behaviour of trained AI systems largely outside

¹⁶ *Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors*, BANK FOR INT'L SETTLEMENTS, <https://www.bis.org/bcbs/publ/d431.htm> (last visited Apr. 15, 2026).

¹⁷ Dwiti Gambhir & Raghu Raja Mehra, *AI Liability and Accountability: A Review*, INT'L J. SCI. & RSCH. 846, 849–50 (2025).

its statutory scope.¹⁸ There are three main ways that DPDP legislation currently does not work in an AI context. The first is that consent (Section 6 of the act) does not work well for deep learning because once data has been applied to an AI model's weights, the subsequent withdrawal of that consent would not necessarily be able to propagate through the AI pipeline in an effective manner since the model has already learnt from that data. The second reason is that the legitimate use exemptions of the act (Section 7) are too broad and could allow for public sector entities to use high risk AI to provide social benefits/surveillance without proportionality safeguards.¹⁹

Finally, while the DPDP is a law that regulates digital personal data, it does not define how AI creates or derives inference, and thus the type of inference, such as embedding or profiling metrics, can at times be even more invasive than the data. The absence of any statutory obligation relating to model retraining, inference deletion or post-training accountability illustrates that the Act governs personal data rather than AI behaviour.

Although the DPDP Act does contain a provision regarding withdrawal of consent (Section 6), the overall application of the law would also require the capacity to erase or suspend the processing of the concerned personal data. This becomes untenable under circumstances where personal data has already been embedded within the weight parameters of a trained AI model. Upon completion of training of an AI model, it is typically impossible to extricate or expunge the trained representations from the model, except through model retraining or specialized machine unlearning techniques.

3.3 The Failure of Technological Neutrality

The conventional ability of the Indian law to withstand technological evolution by maintaining a stance of technological neutrality now becomes far more weakened in situations where technology, after deployment, continues to evolve under its own steam. An AI program differs from typical software in the manner that it keeps altering its own working and operational behaviour through learning – a paradigm for which technological neutrality in statutory drafting was never designed.

While the Bharatiya Sakshya Adhinyam, 2023 provides the procedural preconditions required to permit the admissibility of an electronic record as evidence, it offers no mechanism to address issues regarding the explainability, reliability, and algorithmic bias of an AI output. Thus, while evidentiary admissibility is regulated in a procedurally orthodox manner, an autonomous AI output goes unscrutinized at a substantive reliability and evidentiary admission standard.

¹⁸ Arshpreet Singh & Shailja Thakur, *Data Protection and AI Under the Digital Personal Data Protection Act, 2023: An Indian Perspective*, 13 INT'L J. CREATIVE RSCH. THOUGHTS 115, 115 (2025).

¹⁹ *Id.* at 120.

4 LIABILITY BREAKDOWN IN AI-DRIVEN CYBER INCIDENTS

4.1 Legal Failure to Liability Indeterminacy

The primary legal challenge with autonomous AI goes beyond uncertainty about legal liability, however, and is the fragmentation of responsibility: under current liability concepts, liability is only possible if a legal entity is identified that decided on the harmful action for which liability should be claimed and that acted as the source of the harm, but the use of autonomous AI makes such a straightforward linkage of liability to an entity impossible post-deployment. The post-deployment liability analysis with autonomous AI does not only have uncertainties regarding legal liability, but also the question of whether liability can be attributed at all: under existing liability concepts, the question of liability can only be answered when a legal entity can be identified that made the decisions for the harmful action for which the liability is claimed, and that is the source of the harm, but the use of autonomous AI makes such an easy attribution of the liability neutral after implementation. It is not just the strain of doctrine that has been produced but the breakdown of structure in the capacity of law to distribute responsibility.²⁰

AI systems are based on a distributed architecture with developers, deployers (including financial institutions), and intermediaries. This multi-actor ecosystem divides the causal chain, and it is challenging to assign harm to one party that is identifiable. As observed in the literature, AI-induced harm can be caused by the interplay of various components of a system, instead of a particular human action, undermining the conventional liability models.²¹ This fragmentation produces what this paper characterises as an attribution deficit which is a structural inability within the existing legal doctrine to assign responsibility, given that harmful effects are generated by a multiplicity of human and algorithmic interactions, rather than one legally liable party.

4.2 Doctrinal Inadequacy: Negligence and Foreseeability

Duty of care, breach of duty, causation and reasonably foreseeable harm are all necessary to prove negligence liability. Each of these elements is complicated by the AI systems, as their behaviour could be different once they have been deployed. While developers may make reasonable design efforts, adaptive learning can also produce outputs, which were not intended or reasonably foreseeable.²² It is not negligence doctrine's fault, but rather the nature

²⁰ Sunil Kalagi et al., *Legal Liabilities of Artificial Intelligence: An Overview*, 12 SDG J. L. & SUSTAINABLE DEV. e3861, at 3–4 (2024).

²¹ *Id.* at 3–4.

²² *Id.*

of the factual assumptions on which negligence doctrine is grounded that are fundamentally changed by autonomous AI, such that the doctrine becomes less and less useful.

4.3 Strict Liability and the Problem of Distributed Control

The concept of strict liability that is commonly used with hazardous activities also does not work well with AI-driven situations. Strict liability assumes that a person has full control of an inherently hazardous activity which is no longer true in the case of autonomous AI, as the control of the operation is now fragmented among the developers, financial institutions, cloud service providers and ever evolving computational processes.²³ Algorithms are developed, implemented by financial institutions, and autonomously adapted by systems based on data inputs. This decentralization of authority makes strict liability conceptually fragile since there is no party that can be considered as having absolute power over the system.²⁴

4.4 Product Liability and the Dynamism of AI

The failure of product liability frameworks is further caused by their attention to static products. Artificial intelligence systems, in turn, are dynamic and in a state of constant evolution. A defect-free system at the time of deployment can later create undesirable results, as a result of adaptive learning.²⁵ Thus, the current doctrine has no systematic approach to dealing with defects that occur after the system is supplied, as a result of the post-deployment learning process, rather than pre-deployment design.²⁶

4.5 Indian Case Study: Algorithmic Trading and the NSE Co-Location Scandal

The NSE co-location case is an Indian case that exemplifies the complexity of liability in automated systems. In this scandal, some high-frequency trading (HFT) companies supposedly had priority access to the co-location servers of the National Stock Exchange, allowing them to execute algorithmic trades more quickly.²⁷

Though the case mainly concerned the question of market manipulation and violation of regulations, it also raised more structural-related questions concerning AI-driven systems. Algorithms made use of rapid-moving trading systems with little human input, and the benefit was integrated into the technological infrastructure, as opposed to deliberate action by humans.²⁸

²³ Gerhard Wagner, *Liability for Artificial Intelligence: A Proposal of the European Parliament*, 35 J. EUR. TORT L. 1, 15–17 (2020).

²⁴ *Id.* at 15–17.

²⁵ *Id.* at 12–14.

²⁶ *Id.*

²⁷ *In re* Nat'l Stock Exch. Co-Location Facility, O.P. No. 1 of 2019 (Sec. & Exch. Bd. of India Apr. 30, 2019).

²⁸ *Id.*

In terms of liability, there were a number of issues that arose:

- Attribution ambiguity: Did the liability lie with the exchange, brokers or the algorithm designers?
- Technological obscurity: The operation of trading algorithms was such that it was challenging to determine how benefit could be converted into injury.
- Systemic interaction: The consequences of the market were the result of the interaction of several automated systems but not an individual act.

This case exemplifies that in partially automated settings, the question of liability diffuses and disputes. These challenges will only tend to increase as financial systems implement AI-based decision-making, causing more uncertainty in accountability.²⁹

4.6 Liability Vacuum

The net impact of these doctrinal restrictions is the development of a vacuum of liability. Notwithstanding, the emerging attribution gap undermines both compensatory justice and deterrence as responsibility will not be attributed with the legal clarity desired because they are based on the assumption of sole human responsibility. What is emerging from autonomous AI is not just doctrinal defects, but a structural issue in the liability framework that assumes that we exercise our will alone.³⁰

5 REGULATORY FRAGMENTATION AND INSTITUTIONAL GAPS

5.1 Liability Vacuum to Governance Failure

With the development of AI-based financial systems it throws light not only on the doctrinal deficits but also the institutional constraints in the architecture of cybersecurity governance. The regulation of autonomous AI cannot happen in isolation, but needs to have co-regulation involving cybersecurity governance, financial regulation and data governance. In India, currently these functions are dispersed in different institutions that operate autonomously under their respective acts. At present, regulation is a scattered affair with specialized institutions like the RBI or authorities under the Digital Personal Data Protection Act, 2023. Both regulators would likely use their respective statutory remits towards creating detailed norms that regulate autonomous AI, but not financial infrastructure.³¹

²⁹ *Id.*

³⁰ Kalagi et al., *supra* note 20, at 12–14.

³¹ *Id.* at 6–9.

5.2 Findings of the Current Regulatory Frameworks

The Reserve Bank of India (RBI) is the key regulator of the financial system; the bank is more concerned with the classic risks, like credit and liquidity. The regulatory framework of AI has not yet addressed AI-specific risks, including algorithmic opaqueness and autonomous decision making.³² Similarly, the Digital Personal Data Protection Act, 2023 provides an exhaustive treatment of all legal and administrative duties concerning the processing of the personal data. Nevertheless, as an institutional matter, it only focuses on data governance, not on AI governance. While the legislation sets forth standards of permissible use, unlawful use and data fiduciary duties, it doesn't lay out systems of oversight pertaining to the updating and re-use of models and algorithmic performance assessment in the workplace. Cybersecurity laws and data protection rules will continue to remain segregated as the two converge more and more into the finance industry's fabric.³³

5.3 Institutional Gaps and Divided Oversight

The primary institutional flaw is not the existence of no regulation, but rather the absence of regulatory co-ordination. Responsibility for cyber security, financial regulation and privacy protection continues to be contained within separate regulatory silos which prevent any single regulator or body from monitoring the full lifecycle of AI. Such departmentalisation of control results in varied regulatory expectations on AI developments with substantial gaps in institutional oversight.³⁴

5.4 Structural Need to Coordinate Regulation

Regulatory fragmentation should be understood, then, as the structural consequence of these institution specific mandates, rather than as the absence of regulation. While India's financial and data protection regulators have strong individual supervisory powers, neither framework sets universal benchmarks that a regime for AI may need to track through the full system. This institutional break with the individual framework suggests we need coordinated regulation more than further statutory obligations. In this way institutional deficiencies lay the basis for the coordinated AI-specific regulation discussed in Part 6.

The regulatory lacuna explored herein, therefore, has not resulted in the total unavailability of data security or cybersecurity regulations, but a divorcing of these regulatory areas that leaves no one body with the ability to regulate AI systems during the whole system cycle. This separation provides a fundamental regulatory flaw in the context of this study.

³² Singh & Thakur, *supra* note 18, at 120–21.

³³ *Id.*

³⁴ *Id.*

6 CONCLUSION AND RECOMMENDATIONS

The analysis undertaken in this paper therefore shows that the legal challenges posed by AI-driven cyber threats in financial institutions extend far beyond technological innovation and reveals a structural disconnection between India's existing legal architecture and operational realities of AI. Collectively from the preceding parts we can infer that the current statutory, doctrinal and institutional framework continues to regulate human directed cyber activity while leaving AI model behaviour largely outside effective legal governance. These findings together demonstrate that the regulatory challenges are neither because of the absence of cybersecurity law nor the absence of data protection law, instead it is because of the absence of a coherent legal architecture which is capable of governing autonomous AI throughout its operational lifecycle.

The above section further elucidates that Indian legal architecture falls short not just in drafting of law but in the entire conception of the concept of liability. Doctrines that continue to rely on the notion of knowable actors, predictable behavior and knowable causal linkages fail miserably within the context of decision making taking place on adaptive AI systems that are networked within financial infrastructure. The argument, thus, warrants an overarching, AI-specific governance model with three overlapping principles at its core: required algorithm explainability within high-risk AI systems, full-lifecycle accountability beyond model deployment, and coordinated institutional regulation under existing cybersecurity, financial regulation, and data protection paradigms. The argument is not for a vast new body of law but for a body of law to adapt itself to the realities of autonomous AI to deal with today's problems.

Ultimately the paper demonstrates that challenges posed by AI driven cybersecurity are not because of the absence of cybersecurity regulation but based on the continued application of legal principles designed for human-directed conduct to autonomous computational systems. If India's statutory framework does not evolve beyond regulating cyber offences, personal data and financial supervision as separate regulatory domains, accountability within AI driven financial systems will remain fragmented and uncertain legally.

* * *