Analyzing Legal Frameworks for Artificial Intelligence in Fintech: A Comparative Study Across India, European Union and United States

A Thesis submitted to the

UPES

For the Award of

Doctor of Philosophy

in

Law

By

Bharanitharan K

September 2025

Supervisor

Dr. Gagandeep Kaur

Department of Law

School of Law (SOL)

UPES

Dehradun- 248007: Uttarakhand, India

Analyzing Legal Frameworks for Artificial Intelligence in Fintech: A Comparative Study Across India, European Union and United States

A Thesis submitted to the

UPES

For the Award of

Doctor of Philosophy

in

Law

By

Bharanitharan K

(SAP ID: 500113635)

September 2025

Supervisor

Dr. Gagandeep Kaur

Senior Associate Professor

School of Law

UPES

Department of Law

School of Law (SOL)

UPES

Dehradun - 248007: Uttarakhand, INDIA

DECLARATION

I **Bharanitharan K** hereby declare that the thesis entitled Analyzing Legal Frameworks for Artificial Intelligence in Fintech: A Comparative Study Across India, European Union and United States has been prepared by me based on original research under the guidance of Dr. Gagandeep Kaur, Senior Associate Professor of School of Law, UPES, Dehradun. I further declare that No part of this thesis has formed the basis for the award of any degree or fellowship previously.

Bharanitharan K

Bharanitharan K (Sap ID: 500113635)
School of Law,
UPES
Dehradun 248007: Uttarakhand

UPES
UNIVERSITY OF TOMORROW

Great Place To Work. Certified MAR 2022 - MAR 2023 INDIA

CERTIFICATE

This is to certify that Mr. Bharanitharan K has prepared the thesis entitled **"Analyzing Legal Frameworks for Artificial Intelligence in FinTech: A Comparative Study Across India, European Union and United States"** for the award of **Ph.D. degree** from the UPES, under my guidance. He has carried out work at the Department of School of Law, UPES.

G Kaur 22 August, 2025

SUPERVISOR
Dr. Gagandeep Kaur
Senior Associate Professor,
School of Law,
UPES,
Dehradun-248007, Uttarakhand
DATE: 22 August 2025

ABSTRACT

This thesis offers a comparative, doctrinal and analytical study of how artificial intelligence is reshaping the financial technology and how India, the European Union, and the United States are responding it through law and policy. The thesis analyzes the transformation of financial services from conventional digitization to advanced AI integration that now powers the payments, credit, trading, insurance, fraud control and compliance. On basis of these advancements and integration of AI in Fintech, the thesis maps a concrete risk landscape that includes the synthetic identity and deepfake fraud, model opacity and bias in lending and underwriting, market manipulation, smart contract exploits, conflicts over cross border data movement and unclear liability within the layered AI supply chains. Addressing these risks requires embedding of transparency, accountability, human supervision and structured model governance within the high-impact financial systems. The legal analysis surveys India's current mix of statutes and supervisory tools, including the Digital Personal Data Protection Act 2023, the Payment and Settlement Systems Act 2007, the Information Technology Act 2000, Reserve Bank of India directions, and sandbox mechanisms that enable controlled experimentation. It then examines the European Union's integrated, risk based architecture that combines GDPR 2016, the AI Act 2024, MiCA 2023, and DORA 2022, which collectively set detailed duties for data governance, documentation, and resilience. The United States presents a federated approach that blends with the federal consumer finance and market conduct rules with the state privacy laws and also policy instruments such as the AI Bill of Rights, and thus leading to robust enforcement mechanisms but a lack of coherent harmonization. The thesis comparison finds a shared foundations in privacy, market integrity and consumer protection, while the techniques are divergent. The European Union privileges advance documentation, conformity assessment and explicit obligations for the high risk systems. The United States relies more on agency enforcement and guidance. Whereas the India emphasizes inclusion, competition and supervisory pragmatism but lacks standardized obligations for model risk management and explainability. The thesis translates these insights into a reform agenda for India that includes a dedicated risk tiered statute for AI in finance. It also calls for mandatory impact assessments for high-risk models supported by proper logging and independent audits. It further emphasizes the need for a clarified liability in relation to automated decisions and code-based

agreements. In addition the thesis further proposes reforms to strengthen the cybercrime legislation, enhance the consumer protection mechanisms, impose a stricter requirements for data security with timely breach notification and broaden the use of regulatory sandboxes supported by robust supervisory oversight. It closes with a program for cross border interoperability focused on common incident reporting, portable model documentation and cooperation through the G20 summit and the Financial Stability Board, with the aim of limiting regulatory arbitrage while preserving innovation, fairness, and systemic resilience.

Keywords: Artificial Intelligence, FinTech, Data Protection, Regulatory Sandbox, Consumer Protection, Cross-Border Regulation, Comparative Legal Frameworks.

ACKNOWLEDGEMENT

I am deeply indebted to my Supervisor, **Dr. Gagandeep Kaur**, whose insightful guidance, unwavering encouragement and patient mentorship have been the foundation of this work. Her constant support has steered me through every stage of the thesis with clarity and confidence. I extend my sincere appreciation to **Prof. (Dr.) Abhishek Sinha, Dean, School of Law, UPES**, whose dynamic leadership and scholarly encouragement have greatly enriched the intellectual environment that nurtured this research. I am equally grateful to **Prof. (Dr.) Shikha Dimri, Associate Dean (R&D), School of Law, UPES**, for her inspiring vision, distinguished leadership and consistent motivation, which have been a driving force behind my pursuit of academic excellence.

A special acknowledgement is also due to **Mr. Rajeev Attri, Librarian, UPES**, for his unwavering support and timely assistance in accessing critical academic resources, which significantly enhanced the quality of my research. I remain sincerely thankful to the **Ph.D. Program staff, the Library staff, and the IT staff** of UPES for their professionalism, responsiveness and dedicated assistance at every stage of this journey. Their efforts behind the scenes have been invaluable in ensuring the seamless progress of my research. Finally, I owe an eternal debt of gratitude to **my family** for their steadfast love, patience and belief in me. Their encouragement provided the emotional strength that sustained me through this demanding yet rewarding academic journey.

I am also profoundly grateful to the UPES (formerly known as University of Petroleum and Energy Studies) for extending generous institutional support throughout my doctoral journey. The monthly stipend of ₹30,000 enabled me to carry out my research on campus with focus and stability, while the annual contingency grant of ₹30,000 facilitated my active participation in various international conferences. Without this invaluable assistance, the successful completion of this research would have been immensely difficult.

TABLE OF CONTENTS

DECLARATION.....II

CERTIFICATE.....III

ABSTRACT.....IV

ACKNOWLEDGEMENT.....VI

LIST OF TABLES.....XIV

LIST OF FIGURES.....XV

LIST OF ABBREVIATIONS.....XVI

LIST OF CASES.....XIX

LIST OF STATUES.....XXI

CHAPTER 1.....1

INTRODUCTION.....1

1.1 Introduction.....1

1.1.1 Fintech and AI Integration in the Financial Sector.....1

1.1.2 The Role of Banks in the Era of Fintech Innovations.....1

1.1.3 AI's Pervasive Influence Across Industries.....2

1.1.4 The Impact of IoT in Fintech.....3

1.1.5 The Convergence of AI and Fintech.....3

1.1.6 Legal and Regulatory Framework for FinTech in India.....4

1.1.7 Emerging Challenges in AI and Fintech.....4

1.1.8 Privacy Concerns in AI-Driven Fintech.....6

1.1.9 Regulatory Challenges in the Age of AI and Blockchain.....7

1.2 Scope of The Study.....8

1.2.1 Jurisdictional Scope.....8

1.2.2 Technological Scope.....8

1.2.3 Legal and Regulatory Scope.....8

1.2.4 Comparative Aspect.....8

1.2.5 Limitations.....8

1.3 Statement of Problem.....9

1.4 Literature Review.....12

1.5 Research Gap.....31

1.6 Research Objectives.....31

1.7 Research Questions.....32

1.8 Hypothesis.....32

1.9 Research Methodology.....32

CHAPTER 2.....34

FINTECH: HISTORICAL EVOLUTION, DEFINITION AND APPLICATION..34

2.1 Introduction to Financial Technology (Fintech).....34

2.1.1 Meaning of Fintech.....34

2.1.2 Technological Advancements in the Financial Sector.....35

2.2 Historical Evolution of Fintech.....36

2.2.1 Early Forms of Fintech: Transition from Paper-Based Systems to Digitalization.....37

2.2.2 Key Milestones in Fintech Development.....38

2.3 Key Components and Technologies Driving Fintech.....41

2.3.1 Mobile Banking.....41

2.3.2 Cryptocurrencies and Blockchain in Fintech.....42

2.3.3 Payment Gateways and Digital Wallets in Fintech.....45

2.3.4 Smart Contracts in Fintech.....46

2.3.5 Peer-to-Peer Lending and Crowdfunding Platforms in Fintech.....47

2.3.6 Insurtech (Insurance Technology) in Fintech.....48

2.4 Fintech Applications in the Financial Industry.....50

2.4.1 Retail Banking and Customer Interactions.....50

2.4.2 Investment Management and Robo-Advisors in Fintech.....52

2.4.3 Payments and Money Transfers in Fintech.....53

2.4.4 Lending and Credit in Fintech.....55

2.4.5 Insurance and Risk Management in Fintech.....56

2.4.6 Wealth Management and Personal Finance in Fintech.....57

2.5 Impact of Fintech on Traditional Financial Institutions.....58

2.5.1 Disruption to Traditional Banking and Financial Services by Fintech...59

2.5.2 Fintech's Role in Financial Inclusion and Reaching Underserved Populations.....60

2.5.3 Challenges and Risks Fintech Presents to Traditional Financial Models.....61

2.6 Current Trends and Innovations in Fintech.....63

2.6.1 Artificial Intelligence and Machine Learning in Fintech.....63

2.6.2 Blockchain and Smart Contracts in Financial Services.....65

2.6.3 Regulatory Technology (RegTech) and Compliance Solutions.....66

2.6.4 Open Banking and API-Based Ecosystems.....67

2.7 Conclusion.....68

CHAPTER 3.....70

ARTIFICIAL INTELLIGENCE: EVOLUTION, NATURE AND EMERGING DIMENSIONS.....70

3.1 Introduction to Artificial Intelligence (AI).....70

3.1.1 Meaning of Artificial Intelligence (AI).....70

3.1.2 Overview of AI's Impact on Various Industries, with a Focus on Fintech.....71

3.2 Evolution of AI in Financial Services.....72

3.2.1 Early Developments in AI: Historical Background.....72

3.2.2 Key Milestones in AI Adoption within Fintech.....73

3.3 The Nature of AI: Capabilities And Limitations.....80

3.3.1 Types of AI: Narrow AI, General AI and Superintelligence.....80

3.3.2 Capabilities of AI in Decision-Making and Data Processing.....82

3.3.3 Limitations of AI in Financial Applications.....83

3.3.4 AI's Impact on Employment in the Financial Industry.....85

3.4 The Future of AI in Fintech.....86

3.4.1 Predictions for AI's Role in Financial Services.....86

3.5 Conclusion.....87

CHAPTER 4.....88

LEGAL CHALLENGES AND ISSUES WITH INTEGRATION OF AI IN FINTECH.....88

4.1 Introduction to Legal Issues in AI And Fintech.....88

4.1.1 Overview of AI's Growing Role in Financial Services and Legal Framework.....88

4.2 Legal Challenges in AI-Driven Financial Systems.....91

4.2.1 AI-Powered Fraud: The Rise of Synthetic Identities.....91

4.2.2 Algorithmic Manipulations in High-Frequency Trading.....92

4.2.3 Deepfake Frauds and Financial Deception.....92

4.2.4 Smart Contract Exploits in Blockchain Systems.....93

4.2.5 AI-Enhanced Phishing Attacks.....94

4.2.6 Sentiment Manipulation Using AI Tools.....96

4.2.7 IoT-Driven Cybercrimes in Fintech.....96

4.2.8 The "Black Box" Problem in AI Decision-Making.....97

4.2.9 Algorithmic Bias and Fairness in AI-Driven Financial Decisions.....98

4.3 Regulatory Challenges in AI-Fintech Integration.....102

4.3.1 Compliance with Existing Laws: AI Disruption of Current Financial Regulations such as AML and KYC Protocols.....103

4.3.2 Governing AI in Cross-Border Financial Transactions: Addressing Jurisdictional Issues.....104

4.3.3 Liability and Accountability in AI Decision-Making: Legal Dilemmas in Financial Systems.....106

4.4 Intellectual Property (IP) Concerns with AI in Fintech.....107

4.4.1 Ownership of AI-Generated Content: Intellectual Property Issues.....107

4.4.2 Patent Law and AI Algorithms: Legal Implications for Patenting AI Innovations in Fintech.....108

4.5 Contractual Issues And AI-Enabled Financial Agreements.....109

4.5.1 Smart Contracts and Legal Enforceability: Legal Issues Around Blockchain-Based Smart Contracts.....110

4.5.2 Automated Financial Agreements: Challenges Related to AI Execution, Consent and Enforceability.....111

4.6 Ethical Considerations in AI-Driven Finance.....113

4.6.1 Ethics and AI Governance: Balancing Legal Frameworks with Ethical Considerations.....113

4.6.2 Ethical AI Frameworks in Fintech: Analysis of Existing Guidelines and Influence on Future Legal Frameworks.....115

4.7 Case Studies of AI Legal Issues in Fintech.....117

4.8 Conclusion.....125

CHAPTER 5.....126

INDIAN LEGAL FRAMEWORK ON ARTIFICIAL INTELLIGENCE IN FINTECH.....126

5.1 Introduction.....126

5.1.1 Overview of the Indian Legal Landscape Regarding AI in Fintech.....127

5.2 Key Institutions Governing AI in Fintech.....129

5.3 Current Laws Applicable to AI In Fintech.....131

5.3.1 Overview of Relevant Legal Frameworks.....132

5.3.2 Digital Personal Data Protection Act 2023.....138

5.3.3 Indian Contract Act 1872 – Smart Contracts & AI-Driven Transactions.....143

5.3.4 Payment & Settlement Systems Act 2007 – AI in Payment Systems.....145

5.4 Recent Developments in AI & Fintech Regulation.....146

5.4.1 Introduction of New Policies: National Strategy on Artificial Intelligence……147

5.4.2 Sandboxes & Pilot Projects for Fintech Regulation in India.....148

5.5 Challenges in the Indian Legal Framework for AI in Fintech.....149

5.6 Case Analysis on Legal Issues with AI in Indian Fintech.....155

5.6.1 Legal Responses to AI-Related Issues in Indian Fintech.....157

5.6.2 Insights from Regulatory Challenges in AI-Driven Indian Fintech.....158

5.7 Analysis of Indian Legislation.....160

5.7.1 Analysis of Current Legal Framework for AI in Indian Fintech….....160

5.8 Conclusion.....161

CHAPTER 6.....163

COMPARATIVE REGULATORY ANALYSIS: EU, US & INDIA.....163

6.1 Introduction.....163

6.1.1 Brief Overview of EU, US & India Frameworks for AI in Fintech.....163

6.1.2 Importance of Comparative Analysis.....164

6.2 Global AI-Fintech Landscape: Economic & Technological Context.....165

6.2.1 Comparative Dashboard of AI-Enabled Fintech.....165

6.2.2 Technological Context – AI-in-Fintech Indicators.....167

6.3 Cross-Border Intricacies of AI-Enabled Fintech.....168

6.3.1 Territorial Reach & Extraterritorial Statutes.....168

6.3.2 Data Localisation, Adequacy & Interoperability.....169

6.3.3 Licensing, Passporting & Supervisory Cooperation.....169

6.3.4 Conflict-of-Law & Dispute Resolution.....170

6.3.5 Synthesis: Divergent Paths to Convergence.....170

6.4 Regulatory Overview in the European Union.....170

6.4.1 GDPR, MiCA & AI Act 2024.....171

6.4.2 Focus Areas: Data & Consumer Protection, Financial Stability.....206

6.4.3 AI in Fintech: Gaps & Challenges in the EU.....207

6.5 Regulatory Overview in the US.....209

6.5.1 Key Federal Legislation Governing AI & Fintech.....209

6.5.2 State-Level Variations & Their Impact.....210

6.5.3 Focus Areas: Innovation, Consumer Protection, AML.....213

6.5.4 U.S. AI Bill of Rights (Blueprint 2022).....214

6.5.5 AI in Fintech: Gaps & Challenges in the US.....218

6.6 Regulatory Overview in India.....220

6.6.1 Key Legislation Governing AI & Fintech in India.....220

6.6.2 Focus Areas: Financial Inclusion, Consumer Protection, Data Privacy.....225

6.6.3 AI in Fintech: Gaps & Challenges in India.....226

6.7 Key Similarities: EU, US & India.....228

6.7.1 Data Protection & Consumer Privacy.....229

6.7.2 Financial Stability & Risk Mitigation.....230

6.8 Key Differences: EU, US & India.....232

6.8.1 Approach to Innovation & Regulation.....232

6.8.2 Jurisdictional Challenges.....234

6.9 Lessons for India From EU & US Approaches.....236

6.9.1 Adopting Regulatory Best Practices.....236

6.9.2 Enhancing India's Framework via International Examples.....237

6.10 Conclusion.....239

CHAPTER 7.....240

CONCLUSION & RECOMMENDATIONS.....240

7.1 Conclusion.....240

7.1.1 Summary of Findings.....245

7.2 Recommendations.....246

Recommendation 1: AI in Financial Technology Regulation Act 2025.....248

Recommendation 2: Blockchain-Smart Contract Compliance Framework..294

Recommendation 3: IT Act 2000 (Amended 2008): AI-Specific Cybercrime Provisions.....297

Recommendation 4: Amend RBI Act 1934: AI-Driven Financial Systems....305

Recommendation 5: Amend Consumer Protection Act 2019.....307

Recommendation 6: International Harmonization.....310

Recommendation 7: AI Transparency & Accountability.....313

Recommendation 8: Strengthening Data Privacy & Protection.....314

Recommendation 9: Encouraging Innovation.....315

7.2.1 Future Research Directions.....316

Bibliography.....317

List of Publication.....355

LIST OF TABLES

Table 2.1	Summarizes key stages in the early fintech evolution	37
Table 2.2	Summarizes the key milestones of Fintech	49
Table 6.1	Comparative table of key fintech and digital-payments metrics (2024) across the European Union, United States, and India.	166
Table 6.2	AI adoption in fintech – EU, US & India (2024-25).	167
Table 6.3	Cross-border AI-fintech rules & their practical impact – EU, US & India.	169
Table 6.4	Key Similarities in Regulatory Approaches: EU, US and India	229
Table 6.5	AI Regulation Aspect: EU and US Approaches	236

LIST OF FIGURES

Figure 2.1	Number of FinTech's Worldwide from 2018 to 2024, by region	40
Figure 2.2	Unified Payment Interface (UPI) usage across India in third quarted of 2024, by platform	52
Figure 2.3	Key Technologies Shaping the Payments Industry in 2024	54
Figure 3.1	Trends Impacting Banking in 2023	71
Figure 4.1	Number of Cyber Attacks from 2016-2023	95
Figure 4.2	AI Related Issues Worldwide	99
Figure 4.3	Data Breaches reported from 2018-2020	102
Figure 6.1	Usage of AI Tools in Europe	196

TABLE OF ABBREVIATIONS

ACH	**Automated Clearing House**
AEPD	**Agencia Española de Protección de Datos (Spanish DPA)**
AIAAA	**AI Algorithm Auditing Authority**
AILD	**AI Liability Directive (EU, draft)**
AIFRA	**AI-in-FinTech Regulatory Authority**
ADR	**Alternative Dispute Resolution**
ADPPA	**American Data Privacy and Protection Act**
AML	**Anti-Money Laundering**
ATAF	**Appellate Tribunal for AI in FinTech**
API	**Application Programming Interface**
AGI	**Artificial General Intelligence**
AI	**Artificial Intelligence**
APAC	**Asia-Pacific**
ANI	**Artificial Narrow Intelligence**
ACH	**Automated Clearing House**
BIS	**Bank for International Settlements**
BIPA	**Biometric Information Privacy Act (Illinois, US)**
BNPL	**Buy-Now-Pay-Later**
BIS	**Bureau of Indian Standards**
CCPA	**California Consumer Privacy Act**
CBDC	**Central Bank Digital Currency**
CISO	**Chief Information Security Officer**
CFT	**Combating the Financing of Terrorism**
CRS	**Common Reporting Standard**
DPB	**Data Protection Board (India)**
DeFi	**Decentralised Finance**
DPDP Act	**Digital Personal Data Protection Act, 2023 (India)**
DLT	**Distributed-Ledger Technology**
EIOPA	**European Insurance & Occupational Pensions Authority**
EPO	**European Patent Office**
EMEA	**Europe, Middle East & Africa**
EU	**European Union**
EVM	**Ethereum Virtual Machine**
XAI	**Explainable Artificial Intelligence**

FCRA	**Fair Credit Reporting Act (US)**
FAT	**Fairness, Accountability & Transparency (principle)**
FATF	**Financial Action Task Force**
FCA	**Financial Conduct Authority (UK)**
FinTech	**Financial Technology**
FEMA	**Foreign Exchange Management Act (India)**
FTC	**Federal Trade Commission (US)**
GDPR	**General Data Protection Regulation (EU)**
GPAI	**Global Partnership on AI**
GELSI	**Governance, Ethical, Legal & Societal Implications**
GLBA	**Gramm-Leach-Bliley Act (US)**
GDP	**Gross Domestic Product**
HIPAA	**Health Insurance Portability & Accountability Act (US)**
HFT	**High-Frequency Trading**
HITL	**Human-in-the-Loop**
ICA	**Indian Contract Act, 1872**
IRDAI	**Insurance Regulatory & Development Authority of India**
IoT	**Internet of Things**
KPI	**Key Performance Indicator**
KYC	**Know Your Customer**
LGPD	**Lei Geral de Proteção de Dados (Brazil)**
MiCA	**Markets in Crypto-Assets Regulation (EU)**
NPCI	**National Payments Corporation of India**
NSAI	**National Strategy on Artificial Intelligence (India)**
NFC	**Near-Field Communication**
NPL	**Non-Performing Loan**
P2P	**Peer-to-Peer (lending)**
PMLA	**Prevention of Money-Laundering Act (India)**
PE	**Private Equity**
RTGS	**Real-Time Gross Settlement**
RS	**Regulatory Sandbox**
RegTech	**Regulatory Technology**
RBI	**Reserve Bank of India**
RBI Act	**Reserve Bank of India Act, 1934**
RPA	**Robotic Process Automation**
SEBI	**Securities & Exchange Board of India**

SEC	**Securities and Exchange Commission (US)**
SSI	**Self-Sovereign Identity**
SWIFT	**Society for Worldwide Interbank Financial Telecommunication**
TIPs	**Target Instant Payment Settlement (EU)**
TILA	**Truth in Lending Act (US)**
UPI	**Unified Payments Interface (India)**
US	**United States**
UBI	**Usage-Based Insurance**
VC	**Venture Capital**
XAI	**Explainable Artificial Intelligence**

LIST OF CASES

A

Asian News International (ANI) v. OpenAI, (2024)

D

D'Aloia v. Persons Unknown, (2024)

F

Federal Trade Commission v. DoNotPay, Inc., (2024)

FTC v. LendingClub Corp. (N.D. Cal. 2018-2021)

Forrest v. Meta Platforms Inc., (2024)

Federal Trade Commission v. Rytr, (Consent Settlement, 2024)

H

Huskey v. State Farm Fire & Cas. Co., (2023)

I

In re Clearview AI, Inc., (2023)

Internet and Mobile Association of India v. RBI (Supreme Court of India, 2020)

In re Hashfast Technologies LLC, (2016)

J

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

N

Naruto v. Slater, (2018)

R

Roberto Mata v. Avianca, Inc., (2023)

S

Securities & Exchange Commission v. QZ Asset Management Ltd., (2024)

State v. Loomis, (2016)

T

Thaler v. Perlmutter, Civil Action No. 22-1564 (D.D.C. 2023)

Thaler v. Vidal, (2022)

U

United States v. Coscia, (2017)

LIST OF STATUES

A. Statutes specific to India

1. Banking Regulation Act, 1949
2. Companies Act, 2013
3. Consumer Protection Act, 2019
4. Digital Personal Data Protection Act, 2023
5. Foreign Exchange Management Act, 1999
6. Indian Contract Act, 1872
7. Information Technology Act, 2000
    a. IT (Reasonable Security Practices & SPDI) Rules, 2011
    b. IT (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021
8. Payment and Settlement Systems Act, 2007
9. Prevention of Money-Laundering Act, 2002
10. Reserve Bank of India Act, 1934

B. Statutes specific to United States and Europe

a. United States

1. Algorithmic Accountability Act of 2022 (draft)
2. Bank Secrecy Act, 1970
3. California Consumer Privacy Act (CCPA), 2018
4. California Privacy Rights Act (CPRA), 2020
5. Connecticut Data Privacy Act, 2022
6. Electronic Fund Transfer Act, 1978
7. Equal Credit Opportunity Act, 1974
8. Fair Credit Reporting Act, 1970
9. Gramm-Leach-Bliley Act, 1999
10. Truth in Lending Act, 1968
11. Utah Consumer Privacy Act, 2022
12. NYCRR Part 200 – Virtual-Currency "BitLicense," 2015

b. Europe (EU & UK)

1. Artificial Intelligence Act, Regulation (EU) 2024/1689

2. Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554
3. Digital Services Act (DSA), Regulation (EU) 2022/2065
4. Directive (EU) 2015/2366 on Payment Services (PSD2)
5. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679
6. Market-Surveillance Regulation, Regulation (EU) 2019/1020
7. Markets in Crypto-Assets Regulation (MiCA), Regulation (EU) 2023/1114
8. Equality Act, 2010 (United Kingdom)
9. Financial Services & Markets Act 2023 – Digital Securities Sandbox Regulations (United Kingdom)

CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

1.1.1 Fintech and AI Integration in the Financial Sector

For many centuries, the financial sector has been a cornerstone of global economies which represent stability, conservatism and a methodical approach to change. Despite the uncertainties of a new era, this dawn has foreshadowed a time of drastic upheaval with machinery serving to spur the transformation at a rapid pace. Behind the transformation revolutionizing finance are Artificial Intelligence and Financial Technology which weave together, domains which have intersected to refashion the very threads of the economic arena. The term “fintech” which stands for “financial technology” serves as a general word for technology that is utilised to improve, modernise, digitise or undermine the conventional financial services. FinTech, despite the fact that there is not a single definition that applies to all instances of it, it was described by the Financial Stability Board of the Bureau of Indian Standards (BIS) as “technologically enabled financial innovation that may result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services (Board, 2023).”

Alternatively, FinTech can be also understood as the fusion of financial institutions and cutting-edge technology to develop, improve and also to automate the supply of banking and finance. Fintech describes programmes, formulas and mobile, and desktop applications. Sometimes it also involves with hardware, such as piggy banks with internet access. Fintech platforms make it possible to perform routine chores like cheque deposits, money transfers between accounts, bill payments and financial aid applications. Additionally, they also enable complex technical ideas like peer-to-peer lending and cryptocurrency exchanges.

1.1.2 The Role of Banks in the Era of Fintech Innovations

Banks have traditionally been the primary financial intermediaries, facilitating payments, granting loans and offering investment products. Since the emergence of financial technology solutions, the banking industry has found itself undergoing significant changes in how it operates and serves its customers. While some FinTech

innovations compete with traditional banking services, many others complement them. As banks seek to modernize their operations and offer customers enhanced convenience, they are working closely with financial technology start-ups to help streamline internal processes, strengthen the services provided and ensure optimal customer satisfaction through collaborative innovation. FinTech refers broadly to the utilization of innovative technologies meant to enhance and computerize the conveyance and application of fiscal services. The financial technology sector possesses a vast assortment of technical solutions, from mobile transaction capabilities to cryptographic system platforms, each of which seeks to furnish customers with novel monetary offerings and assistance through creative utilization of evolving technologies (Walden, 2020).

The breadth of activities encompassed under FinTech spans a diversity of financial operations, extending from funds transfers and credit requests to investment and crowdfunding opportunities, though this spectrum is by no means exhaustive. Start-ups and established companies alike can be considered part of the FinTech domain if they use technology to disrupt or improve traditional financial service models. Examples: Digital wallets (e.g., Apple Pay, Google Wallet), peer-to-peer lending platforms (e.g., LendingClub, Prosper), robo-advisors (e.g., Betterment, Wealthfront) and cryptocurrency exchanges (e.g., Coinbase) are all examples of FinTech.

1.1.3 AI's Pervasive Influence Across Industries

From healthcare to entertainment, transportation to e-commerce, AI's influence is pervasive. Due to its unrivalled facility in sophisticated data examination, self-guided learning mechanisms and prognostic rendering, a vast assortment of industries have found this tool to be exceptionally precious. In the realm of finance, these capabilities have found a particularly receptive audience. Financial decisions, whether they pertain to investments, loans, or risk assessment, are deeply rooted in the analysis of vast datasets. Patterns, trends and anomalies within these datasets can offer insights that are invaluable to financial institutions. AI, with its capacity to rapidly sift through and deduce patterns within these datasets in a manner unmatched by human cognition, has proven itself a true field-altering force. Parallel to the rise of AI is the evolution of Financial Technology or FinTech. A journey through the ancestry of FinTech would follow the establishment of electronic banking, the rise of digital exchanges and the emergence of platforms enabling online commerce. However, in its current avatar, FinTech represents much more than just digitized financial services. Through decentralizing authority over currency and democratizing access, blockchain

technology portends a reordering of established relationships between financial service providers and their clients by enabling novel modes of engagement, novel means of effecting exchanges and novel approaches to tailoring and disseminating financial instruments. Through the rapid proliferation of innovations such as mobile banking, peer-to-peer lending networks, digital currency portfolios and computerized investment advisors, today's consumer has integrated a diverse array of cutting-edge financial technologies into both their everyday routine and long-term strategy in a manner which would have seemed scarcely imaginable even as recently as the near past. Although an intertwining of the two domains heralds prospects aplenty, it moreover brings with it a suite of difficulties to solve.

1.1.4 The Impact of IoT in Fintech

While distributed innovations of Artificial Intelligence and Fin-Tech synergistically modernize, interconnected apparatuses of the Internet of Things subtly interweave to intricately undergird an environment of seamless data-sharing and augmented judgment across a system in constant communication. The melding of IoT's sprawling web of devices together with AI's problem-solving aptitude has birthed FinTech answers that respond swiftly to the societal needs while also weaving themselves intricately into the very fabric of everyday lives. From wearable payment devices to asset tracking systems, the synergy between IoT and AI in FinTech enables a seamless blend of the physical and digital worlds, enhancing consumer experiences while adding layers of complexity to the evolving financial ecosystem.

1.1.5 The Convergence of AI and Fintech

The integration of AI into FinTech, while promising unparalleled efficiencies, also introduces complexities that were previously uncharted in the financial sector. In today's globally integrated economy, the origination, intermediation and ramifications of a monetary exchange may each occur within independent nations across divergent boundaries. With the increasingly borderless reality of financial technologies intertwining globally through artificially intelligent systems, an novel degree of multinational collaboration has become vitally necessary. These regulatory institutions around the globe now confront the dual difficulties of deciphering the nuances of artificial intelligence and financial technology while also cooperating to ensure uniform regulations, safeguarding the interests of both consumers and establishments equally. These emerging FinTech platforms, with their bold claims of enhanced efficiency, velocity and novelty, have swiftly achieved distinction, fundamentally altering intuition of and interchange with monetary mechanisms. While technological progress

invariably yields countervailing consequences, an opposing facet also emerges. While the digital platforms praised to be finance's future have also emerged as hubs attracting a more advanced class of financial lawbreakers, their development paradoxically enables both opportunities and new threats.

1.1.6 Legal and Regulatory Framework for FinTech in India

The Information Technology Act of 2000 is the law, in India that addresses cybercrime and electronic commerce. Its main purpose is to recognize records and digital signatures. This act indirectly impacts AI applications in the FinTech sector regarding data privacy, data security and cybercrimes which are essential for data management and consumer protection. The Reserve Bank of India (RBI) issued guidelines that have an impact on FinTech operations. As the central banking institution of India RBI's guidelines cover aspects such as payments, e wallets and online banking. Although these guidelines aren't specifically focused on AI they are crucial for FinTech companies integrating AI technologies in areas like automated customer service, fraud detection and algorithmic trading. The Payment and Settlement Systems Act of 2007 establishes a framework for payment systems in India with the RBI designated as the authority for overseeing them. This Act is relevant to FinTech applications involving payment systems that often incorporate AI to enhance security and efficiency. The Digital Personal Data Protection Act 2023, aimed at safeguarding individuals personal data by establishing a Data Protection Authority. To ensure compliance, this act will be crucial for AI applications that handle amounts of data. The Reserve Bank of India (RBI) has issued guidelines to regulate lending platforms that often utilize AI algorithms for credit scoring and loan disbursement. These guidelines have been put in place to promote practices and safeguard borrowers. Under the Consumer Protection Act of 2019 provisions have been included to protect consumers against trade practices, which can also extend to FinTech services. This can indirectly impact AI driven FinTech services in terms of transparency and fairness. The RBI has introduced a 'regulatory sandbox' framework allowing FinTech companies, including those utilizing AI technology to test products and services under the supervision of regulators within a controlled environment. This framework aims to encourage innovation in AI applications, within the FinTech sector.

1.1.7 Emerging Challenges in AI and Fintech

With the growing intricacy and complexity in these platforms, an unwitting vulnerability emerges, as with Pandora's fabled container, that is difficult to close once

opened. Cybercriminals, always on the lookout for the next big opportunity, have quickly adapted, leveraging the technology that powers these platforms to orchestrate elaborate financial heists. Traditional financial crime prevention mechanisms, which were designed in a time where financial transactions were more straightforward and less digitally reliant, now find themselves in uncharted waters. These mechanisms, though robust in their time, are ill-equipped to handle the nuances and complexities introduced by AI-driven financial operations. The challenge is akin to using a net designed to catch fish to capture smoke; the very nature of the problem has changed.

One of the most insidious manifestations of this new breed of crime is AI-powered fraud. Through technological progress in artificial intelligence and information examination, criminals have gained the means to artificially fabricate financial identities which can convincingly mimic authentic accounts. These AI-generated profiles (Inscribe, 2022) can mimic genuine financial transactions so accurately that they can deceive even the most advanced detection systems. For instance, by analyzing vast amounts of data, AI can generate patterns of financial behaviour' that seem entirely legitimate. These synthetic profiles, complete with fabricated financial histories, can then be used to apply for loans, credit cards, or other financial instruments. The widespread damages inflicted by such deception encapsulate both immediate monetary setbacks endured by establishments along with a creeping corrosion of belief in the integrity and reliability of artificially intelligent fiscal technologies. Another emerging challenge is algorithmic manipulations, particularly in high-frequency trading (HFT) environments. In these ultra-fast, AI-driven trading ecosystems, even a minor manipulation can lead to significant market distortions. Malicious actors, armed with their adversarial AI models, can introduce data or patterns that mislead trading algorithms. This can result in artificial market movements, allowing these actors to reap substantial profits while leaving unsuspecting investors in the lurch.

Financial market manipulations not only destabilize markets by deceptive means but also undermine trust in the system, thereby spawning wider reverberations throughout the economy as uncertainty spreads. Though blockchain technology's incorporation into financial technology promises a more transparent and secure new epoch, reconciling its singular challenges will prove difficult. Blockchain, with its decentralized architecture, ensures that data, once entered, is immutable. While blockchain's decentralization (Balal, 2021) can provide notable advantages, an overreliance on this feature risks exposing critical vulnerabilities within the system. Erroneous or fraudulent entries, once recorded on the blockchain, become an indelible part of the record. This immutability means that even if a fraudulent transaction is

detected, rectifying it becomes a complex challenge. The implications of such irreversible entries can range from financial losses to legal complications, especially in scenarios where the blockchain is used for contractual or transactional purposes.

1.1.8 Privacy Concerns in AI-Driven Fintech

The issue of data privacy stands out as one of the most pressing ethical matters circulating around how information is collected and used in today's world. In an era where data has become akin to black gold, the very design of AI-powered financial platforms demands access to enormous troves of personal and economic particulars to perform at their highest capacity. Every transaction, every query, every interaction becomes a data point, feeding into complex algorithms that continuously learn and adapt. Although data-driven approaches promise to boost user experiences, their reliance on personal information risks compromising privacy in ways that warrant serious consideration. Without stringent safeguards, this treasure trove of data can become a target for breaches, leading to unauthorized access and potential misuse. The far-reaching implications of security lapses stretch beyond mere monetary impacts as they contribute to an abrading of belief in the framework itself as well as prospective long-term ruin to its renown. Beyond data privacy, the potential for biases in AI decision-making is a growing concern. While AI systems based on machine learning can be highly effective, the quality of their training data ultimately determines how well they perform their functions. If this data carries historical biases or inaccuracies, the AI system can inadvertently perpetuate or even amplify these biases. One potential way an AI-driven credit scoring system could be considered is if it evaluated applicants through an algorithm accounting for various financial and personal factors. If trained on historically biased lending data, the system might consistently disadvantage certain demographic groups, leading to unfair loan denials or higher interest rates. These biases, whether wilfully or unwittingly introduced, could have deep socio-economic consequences, propagating inequities while weakening the very pledge of impartiality that technology aims to provide. Though its inner workings remain inscrutable to even its users, the ambiguous characterization "black box" denotes mechanisms whose processes defy transparent comprehension on deployment (Kenton, 2023). Given the stakes in FinTech where choices carry weighty economic consequences, this absence of openness is especially troubling. When an automated system proposes to refuse a personal loan application or marks someone as a potential fraud risk, that individual maintains a basic human right to obtain a comprehensible account of the thinking that led to such a significant determination. However, with deep learning models and other complex AI systems, providing a clear, understandable rationale can be a daunting

challenge. This obscurity raises critical questions about accountability, transparency and the right to explanation.

1.1.9 Regulatory Challenges in the Age of AI and Blockchain

Through decades of careful consideration, a comprehensive framework of oversight had been constructed around the finance industry to reinforce dependability, equity and uprightness through times of fluctuating economy. Though financial transactions and the tools facilitating them were more clearly defined at the time these regulations were fashioned, the world in which we now operate has progressed in complexity, rendering such guidelines potentially outdated without proper re-examination. Enter AI, with its dynamic algorithms and self-learning capabilities and the landscape shifts dramatically. The traditional regulatory frameworks, which were predicated on transparency and predictability, now grapple with AI systems that are continuously evolving and, in some cases, operate in ways that are not entirely transparent. Parallel to the rise of AI in finance is the growing prominence of blockchain technology. Lauded for its potential to revolutionize everything from payments to contracts, blockchain carries its set of regulatory conundrums. At its core, the blockchain provides an openly distributed record that is permanently unchanging and consistently clear. Although these capabilities hold the potential for improved protection and visibility, their implementation also brings novel difficulties. For instance, the decentralized nature of blockchain raises questions about jurisdiction and accountability. If a fraudulent transaction occurs on a blockchain platform, identifying the responsible entity and taking corrective action becomes complex. Additionally, while the unchanging nature of blockchain, one of its most praised qualities, does provide strengths, it similarly can carry weaknesses from a viewpoint of governance. Once having been recorded onto the blockchain, amending or removing that recorded transaction becomes an impossibility. This ensures data integrity but also means that erroneous or fraudulent entries become a permanent part of the record. In a sector where rectifying mistakes is crucial, this poses significant challenges.

In light of these challenges and opportunities, this research seeks to critically analyze the intricate dance between AI and FinTech. The primary objective is to understand the complexities, identify gaps in existing legislation and suggest frameworks and solutions that ensure a harmonious, transparent and ethically sound integration of these technologies in the financial realm.

1.2 SCOPE OF THE STUDY

1.2.1 Jurisdictional Scope:

It is Primarily centered on India, focusing on its legal, technological and financial aspects concerning AI-driven FinTech. Comparative analysis with the European Union and United States, particularly concerning its EU AI Act 2023, AI Blueprint Bill by United States and regulatory framework on AI in FinTech.

1.2.2 Technological Scope:

There will be comprehensive examination of AI integration within the FinTech sector, Also a detailed exploration of the role and implications of blockchain technology in conjunction with AI in financial systems. Exploring the impact of the Internet of Things (IoT) on Financial Technology (FinTech) platforms, particularly in how it interacts with and enhances AI-driven systems.

1.2.3 Legal and Regulatory Scope:

Study of the legal challenges, complexities and implications posed by AI and blockchain technology in financial operations, with special emphasis on those that transcend international borders. Examination of the ethical dimensions of AI's role in the financial sector, especially concerning privacy, biases and potential misuse. Liability considerations, especially in the context of AI-driven financial errors or crimes.

1.2.4 Comparative Aspect:

There will be comparison of the regulatory frameworks, guidelines and provisions related to AI-driven FinTech between India, EU and US. Analysis of the similarities, differences and areas of potential alignment or divergence between the three jurisdictions.

1.2.5 Limitations:

The study will not delve deeply into other associated technologies in FinTech unless they have a direct relation or impact on AI-driven systems. While the study touches upon the ethical dimensions of AI in FinTech, it will not be an exhaustive philosophical discourse on AI ethics but will remain anchored to its legal and financial implications.

1.3 STATEMENT OF PROBLEM

The integration of Artificial Intelligence (AI) into the financial technology (FinTech) sector signifies a transformative era, promising unparalleled efficiency and innovation. However, this ground-breaking amalgamation, while revolutionary, also introduces a plethora of challenges, especially concerning legal frameworks, ethical considerations and the emergence of sophisticated financial crimes.

AI-driven FinTech platforms, in their pursuit to redefine financial operations, have inadvertently become epicentres for a new breed of cybercrimes. These crimes, which harness the very technology that underpins these platforms, not only jeopardize the financial assets and data of individuals and institutions but also significantly erode trust in AI-driven financial systems. Traditional financial crime prevention mechanisms, designed for a pre-AI era, find themselves ill-equipped to detect and counter these AI-specific threats, highlighting an urgent need for evolved countermeasures.

Among the emerging crimes are:

1. **AI-Powered Fraud:** Leveraging advanced machine learning models, fraudsters can now mimic genuine financial transactions, making their fraudulent activities harder to detect. For instance, they can create synthetic financial profiles that blend seamlessly with genuine ones. These synthetic profiles, backed by fabricated financial histories, can be used to apply for loans or credit cards, leaving financial institutions at a loss when these synthetic entities default (Bao, 2020).

2. **Algorithmic Manipulations:** In the age of high-frequency trading (HFT) powered by AI algorithms, there's a rising threat of market manipulations. Malicious actors can deploy adversarial AI models to mislead trading algorithms, causing artificial market movements. This can lead to significant financial gains for the perpetrators while causing substantial losses for unsuspecting investors. Such manipulations can destabilize financial markets, eroding investor confidence and leading to broader economic implications (Azzutti, 2024)

3. **Data Breaches:** With their vast datasets, AI-driven platforms become prime targets. Through employing Artificially Intelligence instruments, those engaged in digital wrongdoing have the means to rapidly detect failings and thereby purloin information, bringing about considerable financial and reputational injury. A major security flaw within a prominent financial exchange, for example, could potentially compromise the sensitive personal records of countless individuals, leaving their financial information and identification vulnerable to exploitation and pilfering as

a direct result of such an uncontrolled leakage of closely guarded data to nefarious hands (Lehmann, 2023).

4. **Deepfake Frauds:** Using AI, fraudsters can create hyper-realistic but entirely fake content. This could manifest as fabricated financial statements or even fake video communications from bank officials, leading to misinformation, financial losses and eroded trust. Investors could be misled by deepfake earnings calls, causing them to make ill-informed investment decisions (Abbas, 2023).

5. **Smart Contract Exploits:** As blockchain becomes integral to FinTech, it becomes susceptible to AI-driven attacks. Malicious AI models can exploit vulnerabilities in smart contract codes, leading to unauthorized fund transfers or data manipulations. For instance, a flawed smart contract could be exploited to release funds without meeting the stipulated conditions (André Beganski, 2023).

6. **AI-Enhanced Phishing Attacks:** Cybercriminals leverage AI to craft highly personalized phishing emails or messages. By analyzing vast amounts of data, AI can generate messages that mimic genuine communications from banks or financial institutions, leading to data theft. Victims, believing these communications to be genuine, might divulge sensitive financial information (Basit, 2021).

7. **Sentiment Manipulation:** AI tools can be manipulated to spread fake news or misinformation to influence stock prices or cryptocurrency values. For instance, an AI-driven botnet might flood social media with positive news about a cryptocurrency, leading to a buying frenzy and subsequent sell-off by the criminals for profit. Such manipulations can lead to volatile market conditions, causing significant financial losses for unsuspecting investors (Ienca, 2023).

8. **IoT-Driven Data Manipulation:** The infusion of the Internet of Things (IoT) within AI-driven FinTech platforms presents a double-edged sword. On one hand, IoT offers real-time data insights and the promise of a seamlessly integrated financial experience. On the other, it widens the attack surface for a host of sophisticated financial crimes. The vast array of interconnected IoT devices, from smartwatches to home assistants, can be covertly manipulated to feed distorted data into financial systems. Malicious actors can exploit these vulnerabilities to deceive AI algorithms, potentially leading to fraudulent transactions, erroneous credit assessments, or manipulated trading decisions (Meola, 2023).

9. **Device Hijacking for Financial Gains:** IoT devices, if not securely configured, can be hijacked to serve as gateways for unauthorized financial activities. Imagine a smart home system being used to confirm false transactions or a wearable device manipulated to approve unwarranted expenses. Such crimes can go undetected due to their real-time nature and the trust placed in personal devices (Abbas SG, 2021).

10. **Eavesdropping and Information Theft:** The omnipresent nature of IoT devices poses a significant threat to data privacy. Illicit eavesdropping by compromised devices can capture sensitive financial information, transactional data, or even insider information, making them invaluable tools for criminals to gain unfair advantages or commit fraud (Intelligence, 2024)

11. **IoT Botnets in Financial Attacks:** By harnessing a network of compromised IoT devices, cybercriminals can orchestrate large-scale Distributed Denial of Service (DDoS) attacks on financial institutions, causing system outages, hampering critical financial operations and eroding trust in digital financial services (Islam U, 2022).

The swift adoption of AI in FinTech magnifies cross-border implications in global financial markets. The "black box" nature of certain AI algorithms raises concerns about transparency, accountability and fairness, especially in critical areas like credit approval and fraud detection.

While the promise of blockchain's potential to enhance transparency and security within Financial Technology applications remains hopeful, harnessing its full utility introduces a unique set of complex difficulties that must still be overcome. Blockchain's immutable nature, while preventing unauthorized data alterations, can also pose challenges in rectifying erroneous or fraudulent entries. By way of example, any fraudulent transaction committed to the blockchain becomes remarkably intractable to subsequently retract, inevitably inducing unrelenting pecuniary deprivation. Furthermore, the ethical dimensions of AI in FinTech are becoming increasingly prominent. As AI systems increasingly handle extensive personal and financial information, worries regarding privacy, possible prejudices in automated judgments and data misapplication become paramount. These concerns necessitate a rigorous examination of the ethical foundations of AI's role in the financial sector.

Given this backdrop, this research seeks to critically analyze the intersection of Artificial Intelligence and FinTech, focusing on contemporary challenges, legal issues, AI-associated financial crimes and the evolving regulatory landscape. The primary objective is to understand the complexities introduced by AI in the financial domain, identify gaps in existing legislation, suggest frameworks and solutions that ensure a harmonious, transparent and ethically sound integration of these technologies in FinTech.

1.4 LITERATURE REVIEW

[BOOKS/BOOK CHAPTER]

Aggarwal traces how data-hungry FinTech models collide with long-standing privacy doctrines such as the U.S. Gramm-Leach-Bliley Act and the EU GDPR. He argues that "hyper-personalised" credit and robo-advice services now make raw transaction data re-identifiable, requiring regulators to shift from notice-and-consent toward fiduciary duties of loyalty and care. The chapter anticipates provisions in the EU AI Act that impose explicit data-governance obligations on high-risk financial systems and recommends similar statutory guard-rails for India's DPDP Act. **(Aggarwal, 2024)**

This MIT-Press monograph charts the regulatory journey from the UK's PSD2 mandate to global API standards, showing how open-data rules let AI firms build real-time credit and budgeting tools atop bank rails. The authors warn, however, that data-access asymmetries could entrench BigTech oligopolies unless competition law and sandbox licences evolve in tandem. Their framework underpins ongoing RBI and EU initiatives that couple API openness with algorithmic-risk oversight. **(Zachariadis & Ozcan, 2022)**

Across 18 chapters the volume blends legal theory with case-law on AI-enabled fraud, insider trading and money laundering. It advocates a "regulatory-technology alliance" in which supervisors deploy sup-tech analytics to audit black-box credit and trading models in real time. Several contributors call for mandatory explainability reports—precursors to fairness statements now contemplated by the UK FCA and EU AI Act. **(Lui & Ryder, 2023)**

Basly shows how AI-driven market-making, oracle feeds and risk engines supercharge DeFi protocols, shrinking latency but magnifying flash-loan and oracle-manipulation

attacks. He proposes a three-layer governance stack—open-source code audits, algorithmic "kill-switches," and liability-backed insurance pools—to align with MiCA-style consumer-protection rules. The discussion positions AI as both an efficiency catalyst and a compliance flash-point for tokenised finance. **(Basly, 2024)**

Chen charts FinTech's shift from "payments 1.0" to AI-driven robo-advice and autonomous trading, correlating exponential machine-learning patent growth with venture-capital inflows. He argues that big-tech "platform banks" exploit licensing gaps by operating in the grey area between financial and non-financial regulation, advocating an activity-based regime similar to the UK's FCA sandbox. The chapter's regulatory-arbitrage analysis supports this thesis's call for harmonised AI governance across India, the EU and the US, particularly on licensing, capital requirements and algorithmic-risk audits. **(Chen, 2018)**

Kulhari shows how IoT-driven mass profiling erodes informational self-determination and evaluates blockchain-based self-sovereign identity (SSI) as a countermeasure. While SSI can decouple authentication from data hoarding, the chapter warns of new attack surfaces and governance vacuums if nodes operate across jurisdictions with divergent privacy laws. The author calls for hybrid models—blockchain anchoring plus off-chain GDPR/DPDP-compliant personal-data stores—to reconcile immutability with erasure rights. For FinTech KYC providers, the analysis clarifies why decentralised identity must be paired with clear liability allocation and supervisory oversight. **(Kulhari, 2018)**

Shackelford advances a "polycentric" governance model—layering industry codes, multistakeholder standards, and domestic law—to manage the security, privacy, and competition challenges of an IoT-saturated economy. He critiques pure self-regulation as insufficient for high-stakes sectors like digital payments and advocates baseline statutory duties (e.g., breach notification, algorithmic audit). The chapter's call for interoperable standards aligns with cross-border payment-security frameworks now under discussion at the BIS. For FinTech policymakers, it underscores that device-level rules must dovetail with financial-services regulation to avoid supervisory gaps. **(Shackelford, 2021)**

Surveying global developments up to 2017, Walker introduces "FinTech law" as a composite field spanning payments, digital assets, RegTech and cyber-security. He advocates an adaptive legislative technique—principles plus sandboxes—to keep pace with AI-driven innovation while preserving prudential integrity. Early Singaporean

experiments (e-KYC, MAS sandbox) are analysed as proof-of-concept, offering lessons for jurisdictions such as India that later embedded sandbox clauses in the RBI's 2020 framework. The chapter's historical lens contextualises today's debates on AI accountability and cross-border licensing. **(Walker, 2017)**

[JOURNAL ARTICLE/REVIEW ARTICLE/SURVEY ARTICLE]

Using game-theoretic modelling, the authors show how reinforcement-learning agents can tacitly collude on pricing without explicit communication, challenging traditional antitrust tests that rely on human intent. They urge securities regulators to extend algorithmic-trading rules to cover "emergent collusion" and to mandate audit-trail retention for forensic reconstruction. **(Azzutti, Ringe, & Stiehl, 2024)**

Analysing 2,200 papers (2010-2023), the study finds exponential growth in AI-finance research, with governance, explainability and data-protection rising fastest post-GDPR. It pinpoints under-explored niches—cross-border liability and ESG-aligned credit models—signalling fertile ground for future legal scholarship. **(Bahoo, Cucculelli, Goga, et al., 2024)**

Ferrara categorises bias sources—data, model and deployment—and reviews mitigation tactics such as counterfactual testing and adversarial debiasing. Financial-credit examples reveal how small label skews cascade into systemic exclusion, underscoring regulators' push for algorithmic-impact assessments and reverse-burden-of-proof rules. **(Ferrara, 2024)**

This systematic review shows evidence of disparate impacts in 63 % of ML-credit-scoring studies, even when protected features are omitted. The authors call for statutory access-to-data rights for auditors and mandatory counter-part tests, reinforcing the EU AI Act's high-risk finance tier. **(Garcia, Garcia, & Rigobon, 2024)**

Synthesising 200+ papers on the Governance, Ethical, Legal and Societal Implications (GELSI) of AI-enhanced OSINT, the authors show how machine-learning scrapers upend traditional intelligence cycles by automating data harvesting from social media, blockchains and leaked financial filings. Efficiency gains come at the price of privacy erosion, mission creep and dual-use risk—concerns acutely felt in finance where OSINT feeds fraud-detection and market-surveillance engines. The review calls for sector-specific codes that combine data-minimisation, audit logging and proportionality tests with financial-regulator oversight. Its findings reinforce the need for harmonised

standards before OSINT-driven RegTech tools scale globally. **(Ghioni, Taddeo, & Floridi, 2024)**

Critiquing the techno-legal mantra "code is law," the authors contend that AI's emergent behaviours require ex-ante safety cases, continuous monitoring and legally enforceable override switches. They urge legislators to treat high-risk financial AI akin to medical devices—licensed, audited and recallable—thereby bridging computer-science safety engineering with prudential regulation. **(Judge, Nitzberg, & Russell, 2024)**

Lifshitz argues that latent cyber-risk in smart-contract and DeFi platforms cannot be patched ex post and therefore advocates statutory "security-by-design" mandates akin to privacy-by-design under the GDPR. He outlines a phased lifecycle—threat modelling, code audit, formal verification, and post-deployment bug-bounty—that developers must document to qualify for liability shields and regulatory sandboxes. The piece contends that embedding security early is cheaper than litigating post-breach and bolsters consumer-trust—critical for AI-driven payment rails that process real-time data. Its recommendations dovetail with incoming EU Cyber-Resilience Act obligations and could inform India's draft Digital Payments Security Controls. **(Lifshitz, 2024)**

Drawing on case studies of robo-advice, algorithmic credit scoring and automated AML screening, the authors show how opaque decision pathways blur lines of contractual and tortious liability. They propose a three-tier "algorithmic accountability regime": (i) ex-ante impact-assessments focusing on bias and data-minimisation, (ii) continuous logging plus model-risk dashboards for regulators, and (iii) compulsory insurance or reserve capital for high-autonomy, high-risk systems. The article emphasises that disclosure alone is insufficient; meaningful redress requires auditability and a clear chain of human responsibility—principles echoed in the EU AI Act and India's DPDP Act. For FinTech firms, the findings translate into concrete compliance tasks such as federated-learning architectures and tamper-evident audit trails to satisfy future supervisory reviews. **(Uzougbo, Adeyemi, & Singh, 2024)**

Reviewing Brazil's draft AI Bill alongside its 2020 General Data Protection Law (LGPD), the authors praise the rights-based orientation but flag weak enforcement capacity and over-broad sandbox exemptions. They recommend transplanting LGPD mechanisms—Data Protection Impact Assessments, Data Protection Officers, sanctions matrix—into the AI bill to avoid compliance gaps, especially in banking and

payments where AI adoption is fastest. The piece highlights Brazil's central-bank "Open Finance" agenda as a test bed for risk-based AI supervision, providing comparative lessons for other emerging markets. **(Belli, Curzi, & Gaspar, 2023)**

Bickley and Torgler argue that ethical governance must be embedded in an AI system's "cognitive architecture," not bolted on later. They map how rule-based, hybrid and neural architectures differ in their capacity for traceability, value alignment and moral reasoning. For FinTech regulators, the article implies that licensing criteria should examine an algorithm's architectural transparency before approving robo-advice or credit models. The authors also call for architecture-specific audit tools, anticipating the EU AI Act's technical-documentation requirements. **(Bickley & Torgler, 2023)**

Applying economic-analysis tools, the authors weigh negligence, strict-liability, and no-fault insurance models against AI's defining traits—opacity, autonomy, scalability, and multi-actor supply chains. They warn that overly strict rules could chill innovation, yet lax regimes externalise risk onto consumers and by-standers (e.g., investors harmed by errant trading bots). Their preferred solution is a tiered system: compulsory insurance for "high-autonomy, high-risk" AI (including algorithmic trading) plus evidential presumptions that shift the burden of proof to operators when logs are unavailable. The framework dovetails with the draft EU AI Liability Directive and offers a roadmap for emerging markets harmonising FinTech risk with consumer protection. **(Buiten, de Streel, & Peitz, 2023)**

Kramcsák dissects the GDPR's "legitimate interests" ground and concludes it can seldom justify large-scale scraping of personal data for AI training because the processing typically fails the necessity and balancing tests. He suggests that controllers adopt layered anonymisation, data-protection-impact assessments, and opt-out mechanisms to strengthen the balancing exercise. For FinTech developers mining social-media or transaction feeds, the article offers a compliance playbook that can head off supervisory fines and class actions. It also underscores the need for sector-specific guidance from data-protection authorities on model development. **(Kramcsák, 2023)**

Neilson tests an AI "robo-author" that drafts personalised investment statements for Australian clients and benchmarks them against human advisers. Quantitative scoring shows comparable suitability but higher linguistic clarity, while a qualitative audit flags disclosure gaps that could breach ASIC's best-interest duty. The author argues for a twin-layer regime: algorithmic pre-vetting plus post-advice human certification. This

hybrid approach mirrors Australia's draft Digital Advice Design Rules and offers a useful template for India's forthcoming SEBI robo-advice guidelines. **(Neilson, 2023)**

Pavlidis illustrates how graph neural networks lift suspicious-activity detection by 27 % over rule-based systems but also inflate false positives that can breach due-process rights. He proposes proportional oversight: lighter audits for low-risk models, stringent validation for high-risk cross-border tools—an approach aligned with FATF guidance on AI-enabled AML. **(Pavlidis, 2023)**

Tallberg et al. survey 260 international-level initiatives—standards bodies, trade deals, and soft-law principles—and find that finance ranks among the top three "high-stakes" sectors driving AI-governance agendas after health and defence. They argue that fragmented forums (OECD, FATF, BIS, G20) risk regulatory arbitrage unless stitched together by interoperability rules on data flows, model audits, and liability. The article proposes a "networked minilateralism" model: small clusters of like-minded regulators piloting hard-law experiments (e.g., algorithmic-impact assessments for cross-border payments) that can later scale through treaties. For FinTech lawmakers, the piece underscores why domestic sandboxes and DPDP-style privacy acts must plug into emerging global norms to avoid exclusion from data and capital markets. **(Tallberg et al., 2023)**

The authors demonstrate that training fairness-aware models often requires "special-category" data (e.g., race), yet Article 9 GDPR largely forbids such processing without explicit consent. They propose a narrowly tailored statutory exception—modelled on Recital 71—to permit bias audits while retaining strong safeguards and purpose limitation. Their analysis is pivotal for credit-scoring FinTechs seeking to prove non-discrimination without breaching data-protection law. The paper thus bridges equal-treatment principles and privacy rules, a balance India's DPDP 2023 must also strike. **(van Bekkum & Zuiderveen Borgesius, 2023)**

Vesala dissects how AI training, text-and-data mining, and generative outputs collide with EU copyright exceptions and competition doctrine. She finds current TDM and temporary-copying provisions too narrow, exposing developers to infringement claims and risking market concentration if only large platforms can license datasets at scale. The article proposes broadened exceptions paired with compulsory-licensing or data-sharing remedies to maintain innovative rivalry—ideas equally relevant to AI-driven robo-research in capital markets. Her analysis underscores why FinTech firms

deploying generative analytics must track both IP and antitrust exposures in the EU. **(Vesala, 2023)**

The authors argue that interest-based ad targeting via the Topics API violates GDPR's data-minimisation principle by processing more personal data than necessary, a cautionary lesson for behavioural-scoring FinTechs. They recommend purpose-binding model architectures and federated-learning to reconcile personalisation with privacy law. **(Witt & De Bruyne, 2023)**

Building on public-interest theory, the authors contend that AI regulation must prioritise collective welfare over narrow efficiency gains. They propose public-value impact assessments and "duty-of-loyalty" rules that oblige providers to mitigate systemic risks—ideas especially pertinent to retail-finance robo-advisers and credit engines. Züger and Asghari also back open-data mandates to curb information asymmetries between BigTech-FinTech platforms and regulators. Their framework aligns with today's calls for algorithmic-accountability boards at central banks. **(Züger & Asghari, 2023)**

Reviewing 180 empirical papers, the authors conclude that transparency cues—such as plain-language model rationales—significantly boost customer trust and adoption. They warn that opaque chatbots can breach mis-selling rules and advocate embedding explanation layers to satisfy forthcoming FCA and RBI disclosure standards. **(Hentzen, Hoffmann, Dolan, & Pala, 2022)**

Yap and Lim propose a statutory "Fairness Reporting Statement" akin to financial prospectuses: AI providers would publish bias-impact metrics, mitigation steps, and audit results, all subject to securities-style civil liability for misstatements. They contend this disclosure model harmonises the Equality Act's non-discrimination aims with data-protection limitations on processing sensitive attributes. Applying the framework to credit scoring, the authors show how mandatory reporting could surface disparate-impact risks before large-scale deployment. Their blueprint offers legislators a concrete tool to operationalise the EU AI Act's transparency duties or India's nascent algorithmic-accountability bill. **(Yap & Lim, 2022)**

Ahern dissects how EU prudential rules struggle to keep pace with AI-centric FinTech sandboxes, creating "transition costs" that deter scale-ups. He proposes a staged authorisation model that rewards firms for furnishing bias-audits and cyber-resilience

tests, reducing friction while safeguarding consumers. The piece offers a blueprint for upgrading India's and Brazil's sandbox frameworks. **(Ahern, 2021)**

This conceptual review diagnoses three ethical flashpoints in AI-powered peer-to-peer lending: privacy erosion, algorithmic bias, and exclusion of digitally marginalised groups. Framing the discussion through the Belmont principles, the authors propose statutory "duty-of-explanation" norms and third-party fairness audits—recommendations mirrored in the RBI's NBFC-P2P Guidelines (2017) and Europe's draft AI Act. By emphasising enforceable accountability rather than voluntary codes, the article provides a legal template for governing P2P platforms in India's emerging FinTech statute. **(Anshari, Almunawar, & Masri, 2021)**

Ashta and Herrmann catalogue AI use cases—from anti-fraud monitoring to micro-loan underwriting—and stress that "black-box" opacity undermines prudential supervision and customer trust. They highlight merger-and-acquisition trends whereby large incumbents buy AI start-ups to lock in talent and data advantages, raising competition-law questions. The paper recommends mandatory explainability and sandbox pilots before high-stakes models reach scale, mirroring the RBI and FCA sandbox logic. Their overview frames the risk-benefit calculus regulators must strike when approving new FinTech entrants. **(Ashta & Herrmann, 2021)**

Hendershott et al. map machine-learning advances in text mining for asset-price prediction and fraud detection, then highlight unresolved legal gaps: cross-border data flows, accountability for model bias and harmonised explainability standards. They call for interdisciplinary research that unites computer science, behavioural finance and comparative law—a research agenda this thesis pursues across India, the EU and the US. Their synthesis supplies both technical context and a clear set of regulatory questions for future scholars. **(Hendershott, Zhang, Zhao, & Zheng, 2021)**

Reviewing 200+ papers, Milana and Ashta trace AI's evolution from rule-based trading bots to deep-learning credit and ESG analytics, noting a sharp post-2015 spike in unstructured-data applications. They highlight regulatory blind spots—explainability, model-risk governance, and data-protection compliance—as the key barriers to mainstream adoption. The authors call for joint standards by financial supervisors and data-protection authorities, pre-empting the EU's draft AI Act and IOSCO's 2022 consultative report on AI/ML risk management. Their synthesis provides empirical backing for this thesis's argument that legal harmonisation is as critical as technical accuracy. **(Milana & Ashta, 2021)**

Survey evidence shows incumbents experiment with a wider spectrum of AI tools than FinTech start-ups, yet both groups foresee collaboration—not head-to-head competition—as the dominant market dynamic. Respondents rate BigTechs, rather than each other, as the greatest strategic threat given data-network effects. Incumbents also anticipate a 9 % workforce reduction from automation, raising labour-law and reskilling questions. The study implies that antitrust and licensing regimes must evolve to accommodate new AI-centric alliances between banks and FinTechs. **(Zhang, Ashta, & Barton, 2021)**

Fenwick and Vermeulen argue that future-proof regulation must foster collaborative "ecosystems" where banks, BigTechs, and start-ups share APIs under clear liability and data-governance rules. They champion regulatory sandboxes and proportional compliance tiers to let AI-heavy entrants scale without undermining stability. Case studies from MAS Singapore and the UK FCA illustrate how sandbox findings feed directly into binding codes. The article offers a roadmap for India's RBI and European supervisors looking to formalise sandbox learnings into permanent rulebooks. **(Fenwick & Vermeulen, 2020)**

Using Malaysian micro-lending data, the authors show that community-designed machine-learning models raise credit-approval rates for thin-file borrowers by 18 %, yet still hinge on transparent data-governance. They argue that "human-centric AI" must dovetail with robust consent and grievance mechanisms—principles now echoed in India's Digital Personal Data Protection Act 2023. The paper thus links technical inclusion gains to legal duties of fairness and explainability, underscoring why sandbox guidelines should mandate bias-testing and disclosure. Its mixed-methods evidence supports this thesis's stance that lawful AI design is prerequisite to sustainable FinTech inclusion. **(How, Cheah, Khor, & Chan, 2020)**

Using copula-based tail-dependence and variance-decomposition methods on 2017–2020 data, the authors find that AI/robotics equity indices, green bonds and Bitcoin provide short-run diversification but exhibit heavy tail co-movement during crises. These results warn portfolio-managers—and prudential regulators—against over-relying on novel assets for systemic-risk buffering. The study also underscores classification challenges: AI equity ETFs fall under conventional securities law, green bonds under emerging sustainability disclosure regimes, and crypto under fragmented or absent frameworks. Such heterogeneity complicates unified capital-adequacy and stress-testing standards for AI-driven asset-allocation algorithms. **(Huynh, Hille, & Nasir, 2020)**

Kapsis sketches a future where permissionless cryptocurrencies operate alongside central-bank platforms, forming a "two-tier" settlement architecture. He analyses EU AMLD5, FATF Travel-Rule guidance, and PSD2 to show regulators' struggle to balance innovation with systemic-risk safeguards. The paper recommends a functional approach—licensing by activity, capital, and custody risk—which anticipates the EU Markets-in-Crypto-Assets (MiCA) regime and India's proposed Digital Asset Bill. His framework is directly relevant to FinTech firms building AI-driven crypto-payment rails. **(Kapsis, 2020)**

Mhlanga shows how AI-driven identity checks and mobile-credit scoring can expand formal finance to underserved groups, but he also flags algorithmic opacity that may violate equality norms in many data-protection statutes. The article links inclusion outcomes to the strength of local privacy laws, arguing that weak consent and audit provisions invite discriminatory lending. By framing digital inclusion as a regulatory as well as technological challenge, Mhlanga provides an early legal rationale for India's proposed personal-data fiduciary duties in FinTech. **(Mhlanga, 2020)**

Examining VPAs' default female personas, the authors argue that anthropomorphic design choices can encode and reinforce gender stereotypes, potentially breaching GDPR principles of data-protection by design and non-discrimination. They advocate mandatory Data-Protection Impact Assessments (DPIAs) that evaluate not only privacy risks but also socio-ethical externalities such as bias in voice interfaces for banking apps. The article warns that biased VPAs integrated into FinTech channels could skew user interaction patterns and trust. By linking gendered design to regulatory compliance, the piece broadens the fairness debate beyond data to interface choices in AI-driven finance. **(Ní Loideáin & Adams, 2020)**

The authors survey ML-driven threat-hunting, intrusion-detection, and fraud-scoring systems that already shield online-banking and payments rails. Case studies show deep-learning detectors cutting time-to-response from hours to seconds, yet adversarial attacks and data-poisoning remain open vectors. Zeadally et al. urge "defence in depth": privacy-by-design, continuous model retraining, and immutable audit logs to meet financial-sector compliance tests. Their dual-edge analysis underpins why supervisors (e.g., EU-DORA, RBI master directions) now pair real-time AI security with mandatory resilience audits. **(Zeadally, Adi, Baig, & Khan, 2020)**

Focusing on EU equality law, the author shows how indirect-discrimination rules struggle with black-box AI that proxies protected traits via seemingly neutral variables.

He proposes mandatory algorithmic-impact assessments, minimum transparency thresholds and a reversal of the burden of proof once plaintiffs make a prima-facie case of disparate impact. Credit-scoring and robo-advice are flagged as high-stakes domains where bias can systematically skew access to capital. The paper supplies concrete legal levers—disclosure, auditing, and injunctive relief—that regulators worldwide can adapt to FinTech contexts. **(Zuiderveen Borgesius, 2020)**

Ballell constructs an analytical matrix that links five "disruptive features" of AI—opacity, autonomy, scalability, unpredictability, and data-hungriness—to fault-based liability, data-protection, and IP doctrines. He shows how AI undercuts the long-standing neutrality and functional-equivalence principles that anchor uniform commercial law, arguing for a risk-tiered adaptation rather than piecemeal exceptions. For FinTech, his framework predicts heightened product-liability exposure when autonomous trading or credit models malfunction, unless lawmakers clarify safe-harbour and audit-trail duties. The article therefore provides a blueprint for activity-based AI regulation that several central banks, including the RBI, are now exploring. **(Ballell, 2019)**

Using a survey of Spanish retail investors, the study finds that perceived usefulness, ease of use and—critically—trust in algorithmic competence drive intention to adopt robo-advisers. Trust, in turn, rises when platforms display certification seals and offer clear explanations of portfolio logic, hinting at the regulatory value of standardised disclosure. The authors caution that privacy concerns and algorithmic opacity can negate technical advantages, dampening uptake. Their behavioural insights support policy moves toward fairness-reporting statements and audit badges for automated financial advice. **(Belanche, Casaló, & Flavián, 2019)**

Bertino et al. propose a blockchain-anchored audit layer that timestamps every data-pipeline event—collection, preprocessing, model training—to create tamper-evident logs for regulators and customers. They argue this "trust fabric" mitigates both algorithmic opacity and data-manipulation risk in AI-driven finance, aligning with emerging IOSCO calls for immutable audit trails in trading algorithms. The authors caution, however, that on-chain transparency must be balanced with GDPR erasure rights, pointing to hybrid on/off-chain architectures. Their design blueprint is directly applicable to RegTech solutions in Indian and EU sandboxes. **(Bertino, Kundu, & Sura, 2019)**

Content analysis of 40 IoT manuals finds that only 31 % mention password hygiene and a mere 15 % offer firmware-update guidance—gaps that pose clear risks for connected payment devices and smart-home wallets. The authors argue that regulators should mandate minimum-security labels akin to energy-efficiency stickers, a proposal later mirrored in the UK's Product Security and Telecoms Infrastructure Act 2022. For FinTech firms integrating IoT endpoints (e.g., wearable pay bands), the study underscores supply-chain liability and the need for contractual security clauses. It feeds into this thesis's call for cyber-hygiene standards in India's draft Digital Payments Protection Rules. **(Blythe, Sombatruang, & Johnson, 2019)**

Chander argues that IoT devices—many of which now process payments or transmit financial data—defy the GATT/GATS goods–services split, creating tariff and data-localisation ambiguities. He illustrates the stakes with an FTC enforcement action against a Taiwanese "smart-cam" vendor whose security flaws exposed user credit-card details. The article proposes a WTO work-programme on digital product classification, anticipating cross-border FinTech frictions over hardware-borne data flows. Its analysis helps frame how payment-enabled wearables or "smart" POS terminals might be taxed and regulated in India-EU trade talks. **(Chander, 2019)**

Using Italian vacancy and task-content data, the authors show that occupations most exposed to AI automation also demand higher cognitive, social and digital skills. They warn that finance may face a "skills-barbell": routine clerical roles shrink while data-science and compliance jobs expand. Policymakers are urged to fund re-skilling schemes and to adapt labour-law definitions of employee control when algorithms allocate tasks. Their findings help banks anticipate workforce realignment as AI-driven process automation accelerates. **(Colombo, Mercorio, & Mezzanzanica, 2019)**

Das surveys machine-learning adoption in payments, lending and trading, warning that signal–noise confusion and pro-cyclical feedback can trigger systemic risk—an issue now squarely in the remit of financial-stability regulators. He calls for "algorithmic circuit-breakers" and activity-based oversight, ideas echoed in recent BIS and IOSCO consultations on AI governance. The article equips legal scholars with a policy blueprint that balances innovation with prudential supervision. **(Das, 2019)**

Hua et al. offer a panoramic scan of FinTech—from blockchain settlements to AI-driven reg-tech—highlighting how open APIs, cloud adoption and real-time analytics reshape competitive boundaries. They argue that regulation must migrate from entity-based licences to activity-based rules that follow data flows across banking, BigTech

and telecom players. Early Chinese regulatory sandboxes are cited as proof that staged experimentation can unleash innovation while containing systemic risk. The paper thus provides policymakers a menu of trend-driven priorities for future-proof FinTech legislation. **(Hua, Huang, & Zheng, 2019)**

The authors position "middle-out" governance between top-down statutes and bottom-up industry norms, using GDPR sandboxes and API standards as illustrative hybrids. They argue such modular, scalable instruments are vital for fast-evolving AI/FinTech ecosystems, where rigid hard law risks obsolescence yet pure self-regulation lacks accountability. Case studies from EU open-banking and e-identity directives show how soft-law codes can crystallise into binding norms via delegated acts. The paper supplies a governance blueprint for regulators seeking balance between innovation and consumer protection. **(Pagallo, Casanovas, & Madelin, 2019)**

Siciliani shows how AI-heavy "RegTech" and "SupTech" tools upend the Basel capital matrix by compressing risk-reporting cycles from months to near real-time. He warns that faster data does not automatically equal better oversight unless supervisors also recalibrate stress-testing models and accountability lines. The piece calls for activity-based licensing that captures cloud-native FinTech lenders otherwise skirting bank-like buffers—an idea later echoed in the EU's Digital Operational Resilience Act. For Indian regulators, the article underscores why the RBI sandbox must evolve into a permanent risk-monitoring platform rather than a time-boxed experiment. **(Siciliani, 2019)**

Cath argues that effective AI governance requires layering technology-specific controls (e.g., formal verification, audit trails) atop broad human-rights and consumer-protection norms. She categorises regulatory tools into ex-ante design standards, continuous monitoring, and ex-post liability, stressing that no single lever suffices. Financial-sector examples—robo-advisers, fraud-detection ML—illustrate the need for dynamic oversight that keeps pace with model drift and adversarial attacks. Her multidimensional template supports this thesis's claim that FinTech regulation must integrate technical, ethical, and legal safeguards from the outset. **(Cath, 2018)**

Lui and Lamb analyse post-crisis conduct-risk rules in the UK/EU and propose "augmented intelligence" pipelines—AI outputs buffered by human review—to satisfy fiduciary and fairness duties. Their case studies show that explainable AI coupled with board-level accountability rebuilds consumer trust faster than black-box automation. The paper thus positions human-in-the-loop governance as a legal compliance strategy,

anticipating later regulatory sandboxes that mandate audit trails for automated advice. **(Lui & Lamb, 2018)**

Nemitz argues that opaque, self-optimising algorithms can displace human autonomy, threatening equality before the law and due-process rights—concerns acute when AI allocates credit or flags AML risks. He advocates a "constitutional" AI governance triad: legality (clear rules), accountability (human override), and transparency (explainability). For FinTech firms, this translates into design duties that document model logic and embed human-in-the-loop triggers for high-impact decisions. The article's rights-centric lens foreshadows the EU AI Act and informs India-EU adequacy talks. **(Nemitz, 2018)**

Reed argues that AI's autonomy erodes three legal pillars—intent, causation, and foreseeability—forcing a shift from actor-based to outcome-based regulation. He proposes a layered model: technology-neutral duties of care at the base, sector-specific rules (e.g., algorithmic-trading safeguards) in the middle, and adaptive co-regulatory sandboxes on top. In FinTech this means embedding mandatory escalation triggers and maintaining immutable audit trails for high-speed trading or credit scoring. Reed's framework bridges tort theory and prudential supervision, offering legislators a menu of tools calibrated to risk and autonomy. **(Reed, 2018)**

Poudel maps the fragmented radio-frequency, protocol, and cloud stacks that power consumer IoT and shows how vendor lock-in stifles true device interoperability. He argues that walled-garden ecosystems push users toward single-brand "data silos," impeding portability rights and amplifying privacy risk in payments wearables and smart-home wallets. The article calls for technical standards coupled with privacy-by-design mandates to pre-empt unfair trade-practice and data-protection violations. Its interoperability critique foreshadows clauses on open APIs now found in India's Account Aggregator and EU Data Act proposals. **(Poudel, 2016)**

Maras catalogues the explosive growth of consumer IoT and shows how weak default settings, opaque data flows, and cross-device analytics create "perpetual surveillance" risks for financial data captured by wearables and smart-home pay devices. She argues that existing notice-and-consent models cannot handle continuous sensing, calling instead for privacy-by-design mandates and default encryption. For regulators, the article foreshadows clauses later found in the EU GDPR and India's DPDP Act, which impose data-minimisation and accountability duties on device vendors. Her analysis

frames why FinTech firms integrating IoT endpoints must include contractual cyber-security warranties. **(Maras, 2015)**

Čerka and colleagues analyse how traditional fault-based tort and product-liability doctrines falter when autonomous systems act with limited human control. They canvass alternative regimes—strict liability, vicarious liability, and insurance pools—and favour a risk-based system where high-autonomy AI triggers compulsory no-fault insurance funded by operators. The authors illustrate the stakes with algorithmic-trading flash crashes, where causation chains are opaque and losses cascade in milliseconds. Their framework anticipates current debates on who pays when AI credit or trading engines misfire in regulated financial markets. **(Čerka, Grigienė, & Sirbikytė, 2015)**

Ferreira and colleagues find that deep-learning and hybrid neuro-evolutionary models outperform classic technical-analysis in short-horizon trading, yet few papers address market-manipulation or model-risk governance. They call for regulator-approved back-testing standards, real-time circuit breakers and immutable audit logs to curb flash-crash cascades. The article flags a compliance gap: while securities law polices human insider trading, algorithmic sentiment-harvesting remains loosely governed. Its recommendations echo IOSCO's push for algorithmic-trading control frameworks in global markets. **(Ferreira, Gandomi, & Cardoso, 2021)**

Gunning et al. outline DARPA's XAI programme and describe prototype methods—SHAP, LIME, counterfactuals—that reveal model reasoning without crippling accuracy. They argue that explainability is non-negotiable for high-stakes domains such as robo-advisory and automated lending, where regulators and consumers must validate decision logic. The paper introduces a dual-metric test—**performance** × **explainability**—suggesting systems that excel in only one dimension should be barred from critical tasks. Its principles already surface in the EU AI Act's "high-risk" explainability mandate and the US OCC's model-risk-management guidance for banks. **(Gunning, Stefik, Choi, Miller, Stumpf, & Yang, 2019)**

Surveying predictive-policing pilots and AML (anti-money-laundering) analytics, Raaijmakers shows how ML classifiers outperform rule-based systems in anomaly detection but also amplify false positives and privacy intrusions. He notes that financial-crime units increasingly share models with mainstream law-enforcement, blurring sectoral oversight lines. The article calls for privacy-by-design, bias testing, and post-deployment audit logs to satisfy both data-protection law and evidentiary standards in

court. Its recommendations map neatly onto the compliance obligations now appearing in EU AMLA proposals and India's updated PMLA guidelines. **(Raaijmakers, 2019)**

Covering data collection, feature engineering, model training and deployment, the survey catalogues where bias enters AI pipelines and reviews mitigation techniques (re-sampling, adversarial debiasing, counterfactual testing). Financial-risk scoring appears as a prime use-case where small label skews cascade into systemic exclusion. The authors stress that technical fixes must pair with legal levers—impact assessments, transparency duties, and disparate-impact audits—to achieve durable fairness. Their taxonomy underpins many of the bias-testing provisions now embedded in draft EU and US financial-AI bills. **(Ntoutsi, Fafalios, Gadiraju, et al., 2020)**

Surveying 250+ studies, the authors show how computational-argumentation frameworks can generate step-by-step justifications that meet regulators' "meaningful explanation" standards for automated decisions. They highlight early pilots in credit scoring and robo-advice where argument graphs help compliance staff trace feature-weight disputes and fairness checks. The survey urges embedding argumentation modules at design time rather than retrofitting black-box models—echoing the EU AI Act's emphasis on ex-ante transparency. For FinTechs facing explainability mandates from the RBI or ESMA, the paper offers a catalogue of mature techniques ready for deployment. **(Vassiliades, Bassiliades, & Patkos, 2021)**

Bredt outlines how AI can cut costs, tailor services and spawn new business models, but stresses that public-sector roadmaps—such as Germany's 2018 Federal AI Strategy—must embed ethics-by-design and supervisory-technology (sup-tech) tools. He urges policymakers to address algorithmic bias and systemic-risk build-up through activity-based oversight and mandatory audit trails. The paper positions central banks as "AI platform regulators" responsible for real-time monitoring of automated credit and trading systems. Its recommendations foreshadow proposals in the BIS "sup-tech" workstream and India's RBI sandbox expansion. **(Bredt, 2019)**

[CONFERENCE PAPER]

The authors combine exploratory-data analysis with an AI trading engine that introduces a custom reward-loss function to maximise risk-adjusted returns in volatile crypto markets. Back-tests on Bitcoin and S&P 500 data demonstrate superior Sharpe ratios versus baseline technical indicators. They note, however, that regulatory constraints on automated trading differ sharply between securities law and largely

unregulated crypto exchanges. The paper therefore highlights the compliance gap facing multi-asset robo-traders and the need for cross-jurisdictional algorithmic-trading rules. **(Al-Ameer & Al-Sunni, 2021)**

Indian banking papers in this volume demonstrate chatbot deployments that cut service times yet reveal gaps in vernacular NLP and redress mechanisms. Several authors urge regulators to expand the RBI sandbox to cover conversational AI and to clarify liability when bots mis-advise customers—a consumer-protection angle rarely quantified elsewhere. These proceedings supply concrete evidence for drafting sector-specific rules on disclosure, escalation and data-retention in AI customer interfaces. **(Amity University & IEEE, 2020)**

Papers in this volume document AI-driven robotic-process automation and smart-contract pilots that cut settlement times by up to 60 %, but authors warn that labour-law and consumer-protection rules lag behind the technology. Several panels call for the Reserve Bank of India (RBI) to widen its regulatory sandbox so banks can test algorithmic processes under supervisory tech (sup-tech) oversight. Contributors also flag legal ambiguities over liability when automated workflows fail, recommending statutory safe-harbour provisions paired with compulsory audit logs. Overall, the proceedings give empirical heft to arguments that India's FinTech law must evolve from entity-based to activity-based regulation. **(Amity University, IEEE UK & RI Section, & IEEE, 2019)**

Several ASONAM papers apply cross-platform social-graph mining to predict equity momentum and detect credit-card fraud, achieving 10–15 % precision lifts—but at the cost of intensive personal-data scraping. A keynote warns that such "surveillance finance" risks breaching GDPR purpose-limitation and could trigger securities-law scrutiny if social sentiment is used for market manipulation. Authors advocate privacy-preserving graph embeddings and regulatory guidance on legitimate versus insider-trading-adjacent analytics. The proceedings therefore spotlight the collision between cutting-edge AI and evolving data-protection and market-integrity regimes. **(Brandes, Reddy, & Tagarelli, 2018)**

Surveying fragmented national approaches, Erdélyi and Goldsmith warn that AI developers will forum-shop unless states converge on core principles of safety, transparency, and human oversight. They sketch a treaty-style framework managed by a new "International Artificial-Intelligence Organization," modelled loosely on the IMO and IAEA, with inspection powers and tiered sanctions. For FinTech, the paper

predicts that cross-border payment and credit models would fall under a "high-risk" tier requiring pre-market conformity assessments—echoing later provisions in the EU AI Act. Their call for binding global norms underscores why bilateral data-adequacy and open-banking deals must anticipate supranational AI rules. **(Erdélyi & Goldsmith, 2018)**

[REPORTS/POLICY NOTE/POLICY COMMENTARY/OTHERS]

KPMG's mid-year briefing notes that VC funding fell sharply in H1-23, yet AI remained the "bright spot," with investors funnelling capital into generative-AI chatbots, fraud-detection engines and reg-tech platforms that automate compliance checks. The report predicts consolidation as distressed assets seek acquirers with strong AI capability and highlights regulators' growing insistence on explainability and cyber-resilience before authorising new products. ESG-linked blockchain pilots and "AI for payments" experiments round out the key themes. For lawmakers, the findings underscore why sandbox pathways must couple innovation incentives with tougher operational-resilience tests. **(KPMG, 2023)**

The latest dashboard sizes the AI-in-FinTech market at **USD 18.31 billion (2025)** and projects **USD 53.30 billion by 2030** (23.8 % CAGR), driven chiefly by anti-fraud analytics, conversational banking and robo-advice engines. North America and Asia-Pacific are flagged as the fastest adopters, but the analysts add a caveat: growth assumes "continued regulatory clarity on data-localisation and algorithmic transparency." Segment analysis shows fraud-management tools outpacing credit-scoring in revenue share, mirroring supervisory pressure on AML/CTF compliance. These numbers give legislators a quantitative baseline when calibrating proportional compliance costs for start-ups versus incumbents. **(Mordor Intelligence, 2024)**

The release projects the global AI-in-FinTech market to jump from US $9.15 billion (2022) to US $11.59 billion (2023) at a 26.8 % CAGR, citing fraud-detection and personalised banking as prime drivers. North America leads due to strict AML mandates and venture funding, while APAC shows the fastest growth. Regulators are warned that generative-AI chatbots and credit bots will scale rapidly, demanding clearer sandbox pathways and capital rules. The data provide hard numbers that contextualise legal-policy debates on AI investment trends. **(Research and Markets, 2023)**

The IMF flags gen-AI's promise for code generation, portfolio simulation, and AML case summarisation, but lists new risks: hallucinated outputs, IP infringement, data

leakage, and concentration of model providers. It urges supervisors to extend model-risk-management rules (validation, stress tests, audit trails) to foundation-model use cases in banks. The note also recommends cross-border cooperation on cyber and cloud resilience, echoing FS-BIS workstreams. Its guidance offers global benchmarks for lawmakers drafting AI clauses in securities and banking legislation. **(Boukherouaa, 2023)**

Gasser hails the EU's draft AI Act as a "constitutional moment" that shifts global norms toward a risk-based, fundamental-rights-centric model of AI oversight. He highlights mandatory conformity assessments, transparency obligations, and severe fines as key enforcement levers that will shape product design well beyond Europe's borders. The commentary notes particular ramifications for FinTech vendors whose credit or fraud models fall into the Act's "high-risk" tier, triggering compulsory human oversight and documentation. By positioning ethics and market access as inseparable, Gasser's piece signals the extraterritorial pull the EU framework will exert on India-EU data-adequacy and payment-services negotiations. **(Gasser, 2023)**

Analysing the draft AI Liability Directive (AILD) and revised Product Liability Directive (PLD), the authors show that black-box systems could slip through fault-based and strict-liability nets, leaving victims without effective redress. Although framed around medical AI, the critique applies equally to algorithmic credit scoring or robo-advice, where causal opacity complicates proof of defect. They advocate reversing the burden of proof and introducing sector-specific presumptions of causality for high-risk AI. Their arguments inform the broader FinTech debate on who bears loss when automated decisions mis-allocate credit or trigger market failures. **(Duffourc & Gerke, 2023)**

The 8th-edition Hackcelerator targets "market-ready" AI solutions for KYC, credit-risk and green-finance reporting. Finalists undergo a live MAS sandbox where they must demonstrate fairness metrics, robustness tests and human-in-the-loop controls before receiving fast-track licensing support. Organisers cite past cohorts that scaled commercially within 12 months, suggesting contests can operationalise ethical-AI principles while accelerating deployment. The programme's rubric offers other regulators a playbook for balancing speed-to-market with prudential oversight. **(Oliver Wyman & Monetary Authority of Singapore, 2023)**

1.5 RESEARCH GAP

The integration of AI with Fin-tech (financial sectors) presents novel opportunities and challenges, however after the review of literature it is revealed that there are significant research gaps. Specifically, there's limited exploration on the synergy between IoT and AI-driven FinTech systems, especially concerning security and legal challenges such as data privacy and regulatory compliance. The convergence of blockchain with AI given the irreversible nature of blockchain transactions, lacks in-depth legal analysis on issues like smart contract disputes, regulatory oversight in decentralized system and aligning AI's decision making process with fixed and unchangeable nature of blockchain records. Additionally, the complexities of AI operations across international borders such as compliance with varying international data protection laws and handling the cross-jurisdictional legal disputes. The attribution of liability for AI-induced financial irregularities, a comparative study of AI-driven FinTech regulations between India, EU and US is needed to understand the divergent legal framework and their potential harmonization. Furthermore, the implications of Digital Personal Data Protection Act (DPDP) Act 2023 are not yet fully explored in terms of data localization requirements, consent mechanisms and the cross-border flow of personal data in AI algorithms.

1.6 RESEARCH OBJECTIVES

1. To analyze the legal challenges associated with AI-driven financial errors, crimes and the implications of combining blockchain technology in financial systems.

2. To critically evaluate the effectiveness of India's legal framework in addressing emerging challenges and issues related to the integration of AI in the financial technology.

3. To assess the legal intricacies of AI-driven financial operations that transcend international borders, with a particular focus on potential conflicts of jurisdiction and international cooperation.

4. To explore and compare the evolving regulatory frameworks in the EU and US in response to advancements in AI within the fintech sector, aiming to identify key strategies, developments and best practices that could inform and enhance India's approach in this domain.

5. To conduct a comprehensive analysis of the key similarities and differences in the regulatory approaches towards AI in fintech in the EU, US and India, focusing on how these approaches are shaped by each region's unique legal, economic and technological contexts

1.7 RESEARCH QUESTIONS

1. What legal challenges and implications evolved when AI-driven financial systems encounter errors, crimes, or integrate with blockchain technology?

2. How current Indian Legal Framework is dealing with new issues and challenges that emerged after integrating AI in Financial Technology?

3. How do AI-driven financial operations that operate across international borders navigate legal intricacies, especially concerning conflicts of jurisdiction and international cooperation?

4. How are the regulatory frameworks in the EU and US evolving to keep pace with the rapid advancements in AI within the fintech sector and what lessons can India learn from these evolutions?

5. What are the key similarities and differences in the regulatory approaches to AI in fintech among the EU, US and India and how do these approaches reflect each region's unique legal, economic and technological landscapes?

1.8 HYPOTHESIS

The current legal framework of India is not competent to deal with the issues and challenges posed by the integration of Artificial Intelligence in Financial Technology.

1.9 RESEARCH METHODOLOGY

1. Doctrinal Research: To understand the existing legal frameworks and the exact provisions that relate to Artificial Intelligence in Financial Technology (Fin-Tech).

Examination of legal documents such as statutes, rules and regulations along with Secondary Data such as Academic articles, Research Papers, white papers/working papers and reports have been reviewed to gather background information and understand existing perspectives on the topic. Specific cases where AI-driven platforms have posed legal challenges have been analyzed in detail. Given the rapidly evolving nature of AI in FinTech, it is imperative to start with a comprehensive understanding of the current legal landscape. Doctrinal research provides clarity on what the law states and sets the foundation for further analytical and comparative insights.

2. Analytical Research: While doctrinal research presents the law, analytical research provides the necessary depth by critiquing and analyzing the principles, logic and implications of these laws. By doing so, it aims to unearth potential gaps, ambiguities, or areas of improvement within the legal provisions. Researcher uses analytical research to delve deeper into the reasons, implications and underlying principles of the legal provisions related to AI in FinTech.

3. Comparative Analysis: Given that India has drafted its DPDP Act 2023 by referring to the EU GDPR 2016, a comparative study becomes essential. Researcher uses comparative analysis to compare the legal frameworks related to AI in FinTech in India with that of the EU and US, focusing on similarities, differences and potential areas of alignment. It not only provides insights into how India might have adapted or diverged from the GDPR, however it also offers potential lessons or recommendations for the future, ensuring robust data protection in the realm of AI-driven FinTech. Furthermore, considering the US significant advancements and unique approach in AI, incorporating a comparison with the US frameworks has broadened the understanding of different regulatory environments and helped in identifying best practices that could be adopted in India.

CHAPTER 2

FINTECH: HISTORICAL EVOLUTION, DEFINITION AND APPLICATION

"The advance of technology is based on making it fit in so that you don't really even notice it, so it's part of everyday life." **— Bill Gates**

2.1 INTRODUCTION TO FINANCIAL TECHNOLOGY (FINTECH)

The swift progression of digital technology has caused an enormous shift in the financial sector, giving rise to the key driver of sectorial innovation—financial technology, or Fintech. Fintech is where finance and technology meet. It allows companies and customers alike to do financial things in a more accessible and efficient manner. Once upon a time, financial system was relied on manual processes and physical banking infrastructures. Although some businesses and individuals still use manual financial processes, the vast majority of us use a digital financial ecosystem powered by automation, artificial intelligence (AI), blockchain, and data analytics. Not only has this transformation occurred in bakeries and financial services, but it has also brought along with it new regulatory and consumer challenges, as well as changed market conditions. Because of the heavily it is relied on technology for financial transactions, it is needed to understand what Fintech means at a basic level, what place it occupies in the reshaping of financial services, and what potential it now has to affect our global economy.

2.1.1 Meaning of Fintech

The integration of technology into offers by financial services organisations to increase their use and delivery to consumers is known as financial technology, or fintech. From helping consumers to handle their money using online banking and mobile apps to building whole new financial ecosystems including cryptocurrencies and blockchain-based platforms, it covers everything (Dorfleitner, Hornuf, Schmitt, & Weber, 2017). Fintech ideas have transformed conventional financial systems and banking. Although the financial industry once mostly relied on manual and paper-based systems, technology developments have digitized these procedures, thereby increasing efficiency, accessibility and speed (Brummer & Yadav, 2018). Fintech today refers to a broad spectrum of uses including mobile banking, digital payments, peer-to-peer lending, robo-advisors and cryptocurrencies (Cai, 2018).

"The use of technology to deliver financial services in new and innovative ways aimed at enhancing customer experiences and creating efficiencies for service providers" (Schueffel, 2016), is the most usually recognised definition of Fintech. Since Fintech encompasses developments like artificial intelligence (AI), big data analytics and blockchain to simplify and automate financial operations, this perspective catches the core of its wide breadth.

Fintech plays more than only improving conventional financial products. By bringing platforms like peer-to-peer lending and crowdsourcing—which avoid conventional financial intermediaries—it has upset whole financial ecosystems (Cai, 2018). Moreover, distributed financial products—which run without central authority or middlemen—have made possible by technology like blockchain (Brophy, 2019).

By enhancing efficiency, cutting costs and extending access to financial products—all of which have created new regulatory challenges—fintech has radically changed the financial services sector (Dorfleitner et al., 2017; Schueffel, 2016). This development shows the major influence ongoing technology progress has on the global financial scene.

2.1.2 Technological Advancements in the Financial Sector

Over the past few decades, technological improvements have fundamentally changed the financial industry. The established financial institutions have been disrupted by digital technology integration, which has thrown up many inventive, accessible alternatives for both individuals and corporations. The emergence of digital banking marks among the most important developments. Although formerly financial transactions needed physical visits to bank offices, online banking and smartphone apps have changed the client experience using the internet and mobile technology (ALT, Beck, & Smits, 2018). Along with improving convenience, this change has cut running expenses for banking organisations. Originally, it is established in the 1970s. Technologies like automated clearing houses (ACH) have recently skyrocketed in scale, enabling trillions of dollars in transactions yearly through safe automated systems (Bauer & Hancock, 1995; Frame et al., 2001). Big data and artificial intelligence (AI) have transformed financial services still more. By allowing financial institutions to examine enormous volumes in real time, these technologies help to improve decision-making in fields such as credit scoring, fraud detection and personalised financial advice (Gomber et al., 2017). For instance, by examining previously unreachable or too expensive consumer behaviour, machine learning algorithms now let lenders more

precisely evaluate creditworthiness (Berger et al., 2007). This has especially for underprivileged groups democratised access to financial services.

Furthermore, cryptocurrencies and blockchain technology have brought a dispersed financial environment that questions established financial middlemen. From payments to smart contracts and financial asset trading, blockchain offers a clear and safe way for documenting transactions that affects everything. The capacity of blockchain to replace middlemen helps lower transaction costs and enhances the efficiency of cross-border payments and other financial services. (World Bank, 2021).

These developments are a part of a larger digital shift in the financial industry since they reach underprivileged areas thereby promoting financial inclusion. For instance, millions of people without regular bank accounts have been able to engage in the financial system thanks to mobile money platforms such as M-Pesa in Kenya, therefore fostering economic growth in underdeveloped areas (World Bank, 2021).

By removing obstacles to entrance and allowing the growth of Fintech companies running with more nimble, customer-centric business models, technology has fundamentally changed the competitive scene of finance. By using technologies including artificial intelligence, big data and blockchain to provide more customised and efficient financial services, these start-ups challenge established financial institutions to innovate or risk becoming outdated (Shim & Shin, 2016).

2.2 HISTORICAL EVOLUTION OF FINTECH

The historical development of fintech follows a dynamic course, seeing how financial services and technologies have steadily melded to revolutionize the economic landscape. The word “fintech” might be new, but the use of technology to improve the financial process started long ago. For several decades, technological innovations have integrated themselves into financial processes. They have transformed and reformed them in many ways that are mostly good. At the most basic and most beneficial level, technology has made many finance processes much easier. It is not limited anymore to manual, labor-intensive, paper-based systems. Moving from handwritten ledger entries to sophisticated digital structures has reshaped customer interactions with financial institutions—not only are these spaces more efficient; they offer a significantly greater level of financial inclusion and an expanded palette of customer experiences. Gaining comprehension of this historical development gives important glimpses into today’s

fintech innovations and supplies a context for the potentially transformative new technologies.

2.2.1 Early Forms of Fintech: Transition from Paper-Based Systems to Digitalization

Time Period	**Development**	**Significance**
Pre-1950s	Manual Ledgers and Paper-based systems	Basic financial record-keeping; labor-intensive, prone to error
1960s-1970s	Automated Teller Machines (ATMs)	Enabled self-service banking, increased customer convenience
1970s	Automated Clearing Houses (ACH)	Facilitated electronic payments, reduced dependency on checks
1971	NASDAQ (Electronic Stock Exchange)	Revolutionized trading through electronic, quicker transactions
1973	SWIFT Network	Standardized international transactions and improved security
1990s	Internet and Online Banking	Enabled remote financial management and secure digital transactions

Table 2.1 Summarizes key stages in the early fintech evolution

Beginning with conventional paper-based systems handling financial transactions, financial technology—also known as Fintech—started to evolve long before the digital age. Early in the 20th century, ledgers were used to document loans, withdrawals and deposits, thereby depending mostly on hand methods for banking operations. Though rigorous and safe, these procedures took time and prone to human mistake.

Automation started to show up in financial systems by middle of the 20th century. The Automated Clearing House (ACH) developed in the 1970s marks one of the first major financial technology advances. Mostly for payroll and bill payments, ACH let banks electronically move money between institutions, therefore dramatically lowering the need for paper checks and hand-written entries. Based on (Bauer and Hancock, 1995), the ACH system set the foundation for more complex digital payment systems found today.

Another significant turning point was the arrival of automated teller machines (ATMs) in the late 1960s, therefore bringing a change from in-person banking to self-service. In 1967, Barclays Bank set up the first ATM, which let users withdraw money from a machine rather than a bank teller. (Payments Association, 2024) states that this was a turning point from labour-intensive banking activities to the early phases of digitalisation in financial services.

Electronic stock exchanges like NASDAQ and the Society for Worldwide Interbank Financial Telecommunications (SWIFT) first emerged in the 1970s and 1980s after ACH and ATMs developed. Established in 1971, NASDAQ was the first completely electronic stock market worldwide, enabling quicker transactions and trade order digitising. SWIFT standardised international payments, allowing cross-border transactions using safe messaging, hence lowering the dependence on manual banking procedures (Dahlberg et al., 2008).

Online banking evolved as financial services migrated towards digitalisation in the 1990s into a major change in consumer interaction with their banks. Originally presented by established financial organisations, online banking gave consumers the ease of handling their money from anywhere, which finally developed into mobile banking systems. The emergence of the internet and the creation of more safe online systems, including SSL encryption, let banks provide digital services without endangering security (Arner et al., 2016).
Early iterations of Fintech developed from physical checks and manual ledger entries to automated systems including ACH, ATMs and finally online banking from paper-based operations. These developments set the stage for the Fintech revolution, therefore allowing more progress in blockchain, digital currencies and artificial intelligence in finance.

2.2.2 Key Milestones in Fintech Development

Through a sequence of major events that have transformed the financial scene, the financial technology (Fintech) industry has undergone notable evolution during the past several years.

Year/Period	Development	Significance
1967	First ATM by Barclays Bank	Enabled 24/7 banking access, reduced dependency on bank tellers
1970s	Automated Clearing House (ACH)	Enabled electronic fund transfers, reduced reliance on checks
1971	NASDAQ established	First fully electronic stock exchange, introduced digital trading
1973	SWIFT (Society for Worldwide Interbank Financial Telecommunications)	Standardized secure cross-border banking transactions
1980s	Introduction of Credit & Debit Cards	Transformed cash-based economy to digital transactions
1990s	Online Banking launched	Allowed customers to conduct transactions remotely
2008	Bitcoin & Blockchain introduced	Paved the way for decentralized finance (DeFi) and cryptocurrencies

2010s	Mobile Payment Platforms (Apple Pay, Google Wallet, Alipay, etc.)	Enabled contactless and digital payments, increasing financial accessibility
2015-Present	Artificial Intelligence (AI) in Finance	Revolutionized fraud detection, credit risk assessment, and personalized banking

Table 2.2 Summarizes the key milestones of Fintech

1. **Automated Teller Machines (ATMs):** The ATM was one of the first big innovations in financial technology. In 1967, Barclays Bank unveiled the first ATM, giving consumers the option to withdraw cash without first seeing a bank teller. By extending client convenience and supporting 24/7 fund access, this breakthrough transformed banking (The Payments Association, 2024). ATMs grew in capability over time to include check deposits, balance searches and even money transfers, so enabling further banking automation.

2. **Credit Cards:** The mid-20th century arrival of credit cards also signalled a major development in fintech. A big change from conventional paper-based payment methods was that credit cards let users make cashless transactions. Credit card firms like Visa and MasterCard grew internationally by the 1970s, which helped to be widely adopted. Modern breakthroughs in electronic payments and other advancements in safe online transactions followed from the digitisation of credit card transactions (Neely, 2021).

3. **Online Banking:** In the 1990s, online banking was a radical breakthrough. It first let consumers pay bills from their personal computers, check accounts and move money. Improvements in SSL encryption, which guaranteed the confidentiality of private financial data and internet connectivity helped to make this possible. Early in the 2000s, several big banks had completely included online banking into their product lines, therefore forming a pillar of contemporary financial services. (The Payments Association, 2024)

4. **Mobile Payments:** An additional important turning point in Fintech evolution is the emergence of mobile payments. Companies including Apple, Google and Samsung debuted mobile payment systems including Apple Pay, Google Wallet and Samsung Pay as cell phones proliferated the 2010s. By means of near-field communication (NFC) technology, these systems offer contactless payments, therefore enabling consumers to make purchases with a tap of their phone. Since then, mobile payments have exploded especially in East Asia, where mobile-first

financial solutions have given millions of people before unheard-of access to financial services (Zavolokina et al., 2016).

5. **Blockchain and Cryptocurrencies:** Blockchain technology and cryptocurrencies have lately marked a more recent turning point in Fintech. Underlying cryptocurrencies like Bitcoin, blockchain—the distributed ledger technology—allows safe and open peer-to-peer transactions free from middlemen. With their alternative digital currency and introduction of ideas like smart contracts and distributed finance (DeFi), cryptocurrencies have upended established finance since Bitcoin's launch in 2009. Constant evolution of these technologies shapes the global financial systems' future (Brophy, 2019; The Payments Association, 2024).

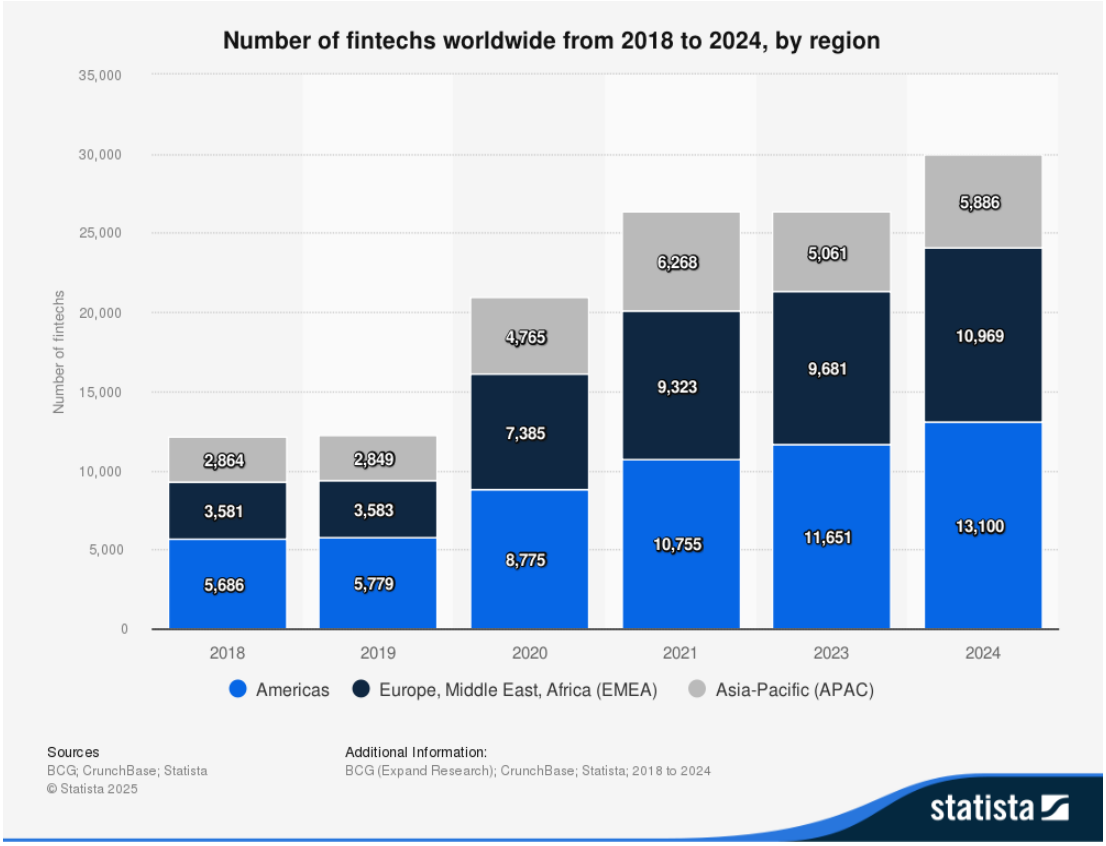

Figure 2.1: Number of Fintechs Worldwide from 2018 to 2024, by region
Source: Statista

The graph illustrates the growth of fintech companies worldwide from 2018 to 2024 across Americas, Europe, Middle East, Africa (EMEA), and Asia-Pacific (APAC) regions. The APAC region shows the highest increase in fintech numbers, reaching 13,100 by 2024, reflecting strong fintech expansion in emerging markets.

These benchmarks mark major turning points that have shaped the linked and vibrant financial environment of today. From credit cards and ATMs to mobile payments and blockchain, every one of these technologies has helped to improve the accessibility, efficiency and security of financial services all around.

2.3 KEY COMPONENTS AND TECHNOLOGIES DRIVING FINTECH

The rapid evolution of financial technology is driven by several core components and emerging innovations that have revolutionized the financial sector. Fintech encompasses a wide range of technologies that enhance efficiency, security, and accessibility in financial services. These advancements have not only streamlined banking operations but also facilitated new business models such as decentralized finance (DeFi), peer-to-peer lending, and AI-powered financial solutions. This section explores the fundamental technologies enabling fintech, including mobile banking, cryptocurrencies and blockchain, payment gateways, smart contracts, peer-to-peer lending, and InsurTech. Each of these elements plays a critical role in reshaping the global financial landscape, improving transaction security, automating processes, and extending financial services to underserved populations.

2.3.1 Mobile Banking

One of the most ground-breaking aspects of financial technology, mobile banking lets customers do banking tasks right from their tablets or cell phones. Originally providing merely balance checks, fund transfers, bill payments and even investment management, it evolved from early online banking solutions and currently offers a wide range of functionality via mobile devices. Mobile banking has grown, thanks to the large general usage of smartphones and advancements in mobile internet technologies.

The convenience with which one may access banking anywhere and anytime is one of the key factors driving acceptance of mobile banking. It gives consumers 24/7 access to their accounts, therefore eliminating the need for real visits to bank branches (Manser Payne et al., 2018). Furthermore, the development of safe mobile apps has raised user confidence by addressing privacy and security concerns, particularly in view of biometric authentication and encryption (Kumar et al., 2020).

From a commercial aspect, particularly in impoverished areas, mobile banking has allowed financial institutions to reach once underprivileged individuals. The

technology has made “branchless banking,” (Alt, Beck, & Smits, 2018) claims possible by providing financial services to individuals living in rural areas where traditional banking infrastructure is limited. Encouragement of financial inclusion has been much enhanced by many hitherto unbanked persons being able to access banking services through mobile phones.

Mobile banking has integrated modern technologies, including artificial intelligence (AI), beyond traditional banking amenities. AI-powered chatbots like Bank of America’s Erica and HDFC Bank’s EVA provide instant customer support, while fraud detection systems such as JPMorgan’s COiN analyze transactions to identify suspicious activities. Additionally, AI-driven personal finance assistants, like Citi’s Cash Flow Insights, offer spending analysis and financial planning based on user behavior. Artificial intelligence supported mobile banking apps offer quick fraud detection, customised financial advice and automatic savings plans. Artificial intelligence has enhanced the user experience by helping mobile banking to be more sensitive to personal needs and intelligible (Manser Payne et al., 2018).

Rising mobile wallets like Apple Pay and Google Pay have assisted consumers to manage digital currencies and make contactless purchases, thereby further integrating mobile banking with digital payments. Now a major component of the whole ecosystem of mobile financial services, mobile wallets provide seamless communication between banking and commerce (Shaikh & Karjaluoto, 2015).

Mobile banking has changed the financial sector ultimately by offering accessibility, security and convenience. Its influence in supporting financial inclusion and combining cutting-edge technology like artificial intelligence has made it a fundamental player in the development of contemporary financial services.

2.3.2 Cryptocurrencies and Blockchain in Fintech

By bringing distributed, open and safe methods for handling financial transactions, cryptocurrencies and blockchain technology have transformed the financial technology (Fintech) space. Originally presented in 2008 with the release of Bitcoin, the first cryptocurrency, Satoshi Nakamoto was an unidentified entity. This signalled the start of a new era of distributed digital currencies and financial procedures, therefore transforming conventional banking systems (Nakamoto, 2008).

Blockchain first found mostly use in the development of Bitcoin, a distributed cryptocurrency run on a peer-to-peer network that avoids conventional financial

intermediaries like banks. By means of proof-of-work (PoW), a consensus mechanism enabling participants to validate transactions and add them to the blockchain without depending on a central authority, Bitcoin presented the idea of distributed trust (Swan, 2015.). This substantially transformed the way digital assets may be distributed and under control, therefore altering payments and asset management in the digital economy (Böhme et al., 2015).

Blockchain, a distributed digital ledger that logs transactions in a sequence of blocks connected together via cryptographic techniques, forms the core of bitcoin technology. Blockchain technology lets users conduct peer-to-peer transactions faster, more transparently and more securely without involving middlemen like banks or payment processors (Du & Le, 2022). Blockchain's immutability—once data is entered into a block, it cannot be changed or deleted—ensures the integrity of transactions. Blockchain technology goes beyond only financial transactions. It finds use in everything from smart contracts—self-executing agreements with the terms of the agreement directly coded into code. Once pre-defined criteria are satisfied, smart contracts automatically execute and enforce transactions, hence improving efficiency and lowering the necessity for human involvement (Kayani & Hasan, 2024).

Built on blockchain technology, cryptocurrencies such Bitcoin, Ethereum and ripple act as distributed digital currency. Since no central government controls these currencies, they represent a revolutionary advancement in the field of finance. Introduced as a digital substitute for fiat money, Bitcoin has attracted interest because of its distributed character, capacity to enable cross-border transactions free from middlemen and possible support of financial inclusion (Cretarola, Figà-Talamanca, & Grunspan, 2021).

Introduced in the second stage of blockchain evolution, smart contracts presented new chances to electronically enforce commercial agreements and automate processes. Originally created on platforms like Ethereum, smart contracts let transactions be executed automatically provided conditions are met. Many Fintech products including insurance, distributed lending platforms and even supply chain finance now heavily rely on these concepts. Blockchain has also been welcomed in sectors such cross-border payments, where it minimises the need for middlemen, therefore reducing costs and expediting world transactions. This application has especially assisted in locations with poor banking infrastructure, where the traditional financial system has been unwilling to update (Deloitte, 2020).

Following Bitcoin, Ethereum included distributed apps (DApps) and smart contracts, hence broadening the possibilities for the blockchain outside basic financial transactions. These developments made it possible for Decentralised Finance (DeFi), whereby users may lend, borrow and trade assets on distributed networks free from traditional financial institutions. Growing quickly, DeFi provides openness, reduced transaction fees and more direct access to financial markets (Du & Le, 2022). The global cryptocurrency industry has expanded significantly, owing to the emergence of hundreds of digital currencies such as Ethereum, Litecoin, and Ripple, which offer alternative methods for value exchange. Including cryptocurrencies into the more general Fintech scene, a movement known as Decentralised Finance (DeFi) has evolved using blockchain technology to supply financial products free from middlemen, such as banks or brokers. DeFi apps promote openness and cut costs by allowing users lend, borrow and exchange assets in a distributed manner (García-Corral et al., 2022). Moreover, the rise of Security Token Offerings (STOs) and Initial Coin Offerings (ICOs) has given start-ups new means to raise money in the digital sphere by means of blockchain-based platforms, so avoiding traditional venture capital channels and reaching worldwide investors straight (Tasca & de Roure, 2014).

Although blockchain and cryptocurrencies have many benefits—including reduced transaction costs and improved security—they also present difficulties, especially with relation to legislative environments. Concerns regarding fraud, market volatility and consumer protection (Cretarola, Figà-Talamanca, & Grunspan, 2021) drive many nations that are still developing rules and procedures to control bitcoin use. Furthermore, although having great potential, blockchain technology is still in its infancy and scalability and energy consumption are key issues.

Blockchain's promise in fintech is growing as governments all around look at new applications including Central Bank Digital Currencies (CBDCs). Blockchain especially in undeveloped places offers not just security and efficiency but also a way to democratise financial services access (World Bank, 2021). Still, there are significant challenges particularly with relation to scalability, energy consumption and legal systems. Authorities and governments are still discussing how best to keep an eye on bitcoin markets without stifling development (Böhme et al., 2015). Innovations like Central Bank Digital Currencies (CBDCs) and ongoing blockchain infrastructure development will probably help to define world finance going ahead. As financial institutions look for methods to use blockchain for more efficiency and openness, its application in cross-border payments and trade finance will keep increasing (Kayani & Hasan, 2024).

All things considered, blockchain and cryptocurrencies have evolved into essential parts of the Fintech ecosystem since they offer distributed, quick, safe ways for financial transactions. Their capacity to challenge established financial systems opens the path for a time when finance will be more transparent, creative and easily available.

2.3.3 Payment Gateways and Digital Wallets in Fintech

Crucially fuelling the Fintech revolution and changing consumer and business transaction behaviour are payment gateways and digital wallets. Together, they offer flawless, safe and quick ways for online payments, which helps digital financial services be quickly adopted all around.

Between buyers and sellers, payment gateways serve as middlemen allowing and handling online transactions. The payment gateway safely passes the payment data from the customer to the merchant and subsequently contacts the bank to either approve or reject a purchase made online from products or services. This method guarantees secured and safe encryption of sensitive data, including credit card numbers (Khando et al., 2023). Well-known payment gateways that easily fit e-commerce systems and are therefore essential for the survival of online companies are Stripe, PayPal and Authorize.Net.

Apart from handling payments, payment gates are crucial for improving security by means of tokenisation and encryption, therefore safeguarding user data during transactions. Preventing fraud and guaranteeing customer confidence in digital transactions depend on this additional degree of security (alt, Beck, & Smits, 2018).

Digital wallets—also known as e-wallets—are mobile or software-based programs that save payment data for a user so they may swiftly and safely make purchases online or in-store. Digital wallets link credit cards, bank accounts, even bitcoin holdings in one handy platform, therefore providing a more integrated approach than conventional payment methods. Among the well-known digital wallets available are Apple Pay, Google Wallet and Alipay (Ruseva et al., 2023).

Among other things, digital wallets let you store loyalty cards, personal identification and enable near-field communication (NFC) for contactless payments. Particularly in underdeveloped areas with insufficient conventional banking infrastructure, these wallets have proved quite helpful in advancing financial inclusion (Naik, 2016). By doing away with physical cards or currency, they also enable quicker and more effective transactions.

Digital wallets have seen unheard-of expansion as the COVID-19 epidemic speeds the change towards contactless payments. Their seamless connection with both online and physical stores makes them vital in the Fintech environment since it lets customers finish transactions with only a tap of their mobile devices (Ruseva et al., 2023).

The continuous digital change of the financial services sector depends on both payment gates and digital wallets. Tech companies, banks and Fintech start-ups are getting more and more competitive as more customers and businesses adopt these technologies in order to develop and offer upgraded services. Still, issues including security threats, privacy issues and the necessity of laws persist (alt, Beck, & Smits, 2018).

Digital wallets and payment gateways taken together are main accelerators of the Fintech revolution. While changing the global financial scene, they provide consumers quick, safe and easy ways of payment.

2.3.4 Smart Contracts in Fintech

Smart contracts are self-executing agreements with directly written in code terms of agreement. Running on blockchain technology, they guarantee that the contract runs automatically whenever pre-defined requirements are satisfied, therefore eliminating middlemen like banks or legal entities. Nick Szabo first popularised the idea of smart contracts in the 1990s, but it really took off with the creation of blockchain systems like Ethereum, which let for more sophisticated and bespoke contracts (Buterin, 2013).
Blockchain systems, most especially Ethereum, which runs contracts using the Ethereum Virtual Machine (EVM) write smart contracts. These agreements work by putting in place set guidelines decided upon by everybody involved. The blockchain automatically runs the contract if these requirements are satisfied, therefore removing the need for third-party validation or manual application. Blockchain's distributed character guarantees openness, security and immutability, so once a smart contract is put into use it cannot be changed (Khan et al., 2021).

Smart contracts—which let users participate in peer-to-peer lending, insurance and derivatives trading free from traditional financial middlemen—are used extensively in applications in decentralised finance (DeFi). They also support automated escrow services, whereby assets or money is stored until particular needs are met then released automatically (Macrinici et al., 2018).

One of main advantages of smart contracts is their efficiency. Contractual enforcement and dispute resolution's time and cost involved can be reduced by automating chores.

In financial markets, where delays or human mistakes can be expensive, they are particularly helpful (Khan et al., 2021). Moreover, as they depend on blockchain, smart contracts offer better security and tamper-resistance, therefore reducing the fraud risk. Beyond banking, smart contracts have found uses in real estate, where they may automate property transfers and supply chain management, where they allow real-time tracking and agreement execution between manufacturers and suppliers (Cuccuru, 2017). Smart contracts in insurance can automatically start claims and pay-outs upon specific criteria being satisfied, therefore enhancing openness and lowering delays (Macrinici et al., 2018).

Smart contracts have various difficulties even if they have great promise. Legal ambiguity is a major issue since not every country accepts smart contracts as legally enforceable. Smart contracts also rely just on the code they are created in. As evidenced by the infamous DAO attack in 2016, where weaknesses in a smart contract resulted in the theft of millions of dollars in cryptocurrencies, bugs or vulnerabilities in the code may cause major financial losses (Buterin, 2013).

To fully realise smart contracts, the evolution of legal frameworks and standards will be very crucial. Cooperation among technologists, legal experts and authorities will be vital in tackling these issues and opening new chances for automation and efficiency in the digital economy as more sectors use blockchain and smart contracts (Khan et al., 2021).

2.3.5 Peer-to-Peer Lending and Crowdfunding Platforms in Fintech

Two main financial breakthroughs inside the Fintech ecosystem that have drastically changed the way companies and people access finance are peer-to-peer (P2P) lending and crowdfunding. These sites act as middlemen between lenders (investors) and borrowers (companies or people), therefore linking them straight without via conventional banks. P2P lending, sometimes referred to as crowdlending, lets people or small businesses borrow money from a collection of investors. Online sites like Lending Club and Prosper link borrowers to lenders depending on their risk profiles and loan parameters, therefore facilitating this lending process (Lenz, 2016). By giving borrowers who might not be eligible for conventional bank loans an alternative—often at reasonable interest rates—P2P lending sites democratise access to credit. Since P2P lending earns interest on the money lent, one major benefit for investors is the possibility for more returns. Because loan default is a possibility, these assets are riskier than conventional savings or bonds, though. Although the platforms usually evaluate borrower creditworthiness, the ultimate choice rests with the individual investors, so

P2P lending is a desirable but risk-filled solution (Maier, 2016). Raising money from many people—usually via internet platforms—for projects, companies, or businesses is known as crowdsourcing. Reward-based, equity-based and donation-based crowdsourcing are just a few of the several forms available. While equity crowdfunding lets people participate in businesses in exchange for shares or revenue-sharing agreements, reward-based crowdfunding lets people support a project in return for a good or service (Bruton et al., 2015). Start-ups wishing to raise modest sums of money from many bankers now choose crowdsourcing, thanks to the large part of sites like Kickstarter and Indiegogo. Particularly, in the early phases of development, democratising the investment process gives entrepreneurs access to funds that would not be accessible through conventional venture capital or bank loans (Assenova et al., 2016). Crowdfunding helps financial inclusion by allowing those without traditional funding sources to support innovative initiatives. However, certain crowdsourcing platforms lack control, which puts investors—especially in equity crowdfunding—where businesses may collapse and leave no return on investment under danger (Kgoroeadira et al., 2019). Underlying P2P lending and crowdsourcing are digital platforms leveraging data analytics, blockchain technology and smart contracts to promote openness, cut costs and guarantee safe transactions. The websites provide prospective investors or lenders thorough information about borrowers or entrepreneurs, therefore guiding their judgements. As the sector grows in guaranteeing the accuracy and security of the loan and funding activities, blockchain and smart contracts are expected to be more crucial (Khan et al., 2021).

Essential components of the Fintech market now are P2P lending, crowdsourcing and alternatives for traditional finance. These platforms have democratised money by letting people and businesses access funds more readily and by offering new investment opportunities. Still, the sector suffers with control problems and default risk. So, its sustainable development depends on ongoing innovation and monitoring.

2.3.6 Insurtech (Insurance Technology) in Fintech

A fast growing subset of Fintech, insurtech—insurance technology—applies technology advancements to the insurance sector. Using developing technologies such artificial intelligence (AI), blockchain, big data and the Internet of Things (IoT). Insurtech seeks to increase efficiency, customer experience and profitability (Chakravaram et al., 2020). From underwriting and claims processing to risk analysis and customer service, Insurtech is changing established insurance paradigms by

combining various technologies. There are technological advancements in insurtech such as AI, Blockchain Technology, Big Data and IoT.

Especially in risk assessment and claims management, artificial intelligence is vitally essential for Insurtech. Artificial intelligence systems can provide consumers more accurate risk profiles by processing massive amounts of data, so facilitating more customised insurance products. Artificial intelligence (AI) can automatically handle claims by means of data analysis from sources including dashcam footage or accident reports, therefore reducing human involvement and hastening claims settlements (Hsu et al., 2020). From this follows faster, more efficient processing as well as improved client experience.

Blockchain's ability to enhance openness and security is encouraging inclusion of technology into insurance. Blockchain smart contracts improve efficiency and reduce fraud by letting insurance claims be automatically handled when specific requirements are met. Blockchain also ensures the immutability of records, which makes data handling difficult and creates mistrust between consumers and insurance companies (KPMG, 2019).

Big data analytics help companies to compile and evaluate vast amounts of consumer data, therefore enhancing underwriting accuracy and customising products to fit particular customer requirements. Wearables or smart home sensors are IoT devices that let insurers gather real-time data that can be utilised to offer usage-based or behaviour-based insurance plans or more dynamically analyse risks (Lin & Chen, 2020). By offering digital-first platforms that enhance client connection and service delivery, Insurtech is upsetting the established insurance value chain. To remain competitive and meet the needs of a more tech-savvy clientele, traditional insurance companies are working ever more closely with Insurtech start-ups. Without ever having to visit a physical office, digital platforms let consumers buy insurance, process claims and get paid just a few clicks (Peterson & Konstantowicz, 2021). Insurtech has developed chatbots and artificial intelligence-driven customer care platforms with 24/7 assistance that answer questions and lead consumers through the claims process. For insurers, this lowers running costs and raises client satisfaction. Insurtech has difficulties despite its promise, mostly with relation to data protection and legislation. Particularly with regard to artificial intelligence-driven risk assessment and the usage of consumer data in real-time, many nations' regulatory systems still lack complete adaptation to the fast technological developments. To solve these problems, numerous

areas are starting regulatory sandboxes—where innovative business models might be evaluated in a regulated context.

Looking forward, the continuous integration of IoT, blockchain and artificial intelligence into insurance systems will assist to streamline operations and enhance personalising even more. But insurers will have to overcome the growing problems with data security and client confidence if they are to fully appreciate the benefits of Insurtech. Insurtech is a transformational tool inside the insurance industry using artificial intelligence, blockchain, big data, IoT to boost profitability, customer experience and productivity. As Insurtech grows, it will not only change the way insurance is offered but also make it more personalised and easily available for customers all around.

2.4 FINTECH APPLICATIONS IN THE FINANCIAL INDUSTRY

The integration of financial technology (Fintech) has significantly reshaped the global financial landscape, enhancing efficiency, accessibility, and innovation across various financial services. From retail banking and investment management to lending, payments, and insurance, Fintech solutions are redefining how financial institutions and consumers interact. The adoption of artificial intelligence (AI), blockchain, big data analytics, and digital platforms has led to faster transactions, automated processes, and personalized financial services, improving overall customer experience and financial decision-making. With the continuous advancement of digital financial tools, Fintech is bridging gaps in traditional banking systems, streamlining operations, and expanding financial inclusion worldwide. This section explores the diverse applications of Fintech in the financial sector, analyzing its impact on banking, wealth management, credit services, and risk assessment**.**

2.4.1 Retail Banking and Customer Interactions

Particularly with relation to consumer contact with banking services, fintech advancements have drastically transformed retail banking. Mostly, integration of fintech into retail banking aims to improve operational efficiency, client experience and provide tailored financial services. Using mobile banking, artificial intelligence (AI), data analytics, blockchain and other technologies, fintech solutions have changed the client-bank interaction.

Among the most clear outcomes of fintech in retail banking is mobile banking. Mobile apps let customers access a wide range of banking services—including money transfers,

bill payments and account management—without visiting a physical branch. Given simplicity and increased customer satisfaction, this has promoted financial inclusion. Artificial intelligence and machine learning have found use in tailored banking experiences created by fintech companies. By use of massive consumer data analysis, AI-driven systems may offer tailored financial products and services. Through automated, algorithm-based financial guidance, robo-advisors, for instance, help users make investment decisions free from human participation. Apart from helping banks cut costs, this automation allows customers access financial assistance around-the-clock, hence improving general involvement.

Banks nowadays are using big data to better understand consumer preferences and behaviour. Modern data analytics technologies allow companies in the financial sector track credit scores, personal financial targets and spending trends. This data allows tailored financial solutions including credit cards or pre-approved loans to be shown. Furthermore, data analytics helps banks to foresee future consumer needs, so enabling banks to actively engage with customers and so improve retention and satisfaction (Parminder et al., 2022). Another major field where Fintech has transformed retail banking is transaction security using blockchain technology. Blockchain's distributed character guarantees honest and safe transactions, therefore reducing the opportunities for fraud and data leakage. Several banks are testing blockchain technologies to offer faster and more safe cross-border payment options, hence improving processes including foreign money transfers (Chakravaram et al., 2021).

Conventional banking to Fintech-driven platforms has helped banks adopt a customer-centric approach. Faster transactions, more tailored services and better financial management options made possible by digital tools help consumers. This development has made banking more accessible and practical for customers especially in rural or impoverished areas where physical branches are rare. The evolution of FinTech has reshaped retail banking, enhancing customer interactions through seamless digital experiences and personalized financial solutions. Fintech has transformed consumer contacts with banks, hence transforming retail banking. By means of mobile banking, artificial intelligence, data analytics, blockchain and other technologies, banks can now provide more customised, effective and safe services, so improving consumer happiness and supporting financial inclusion.

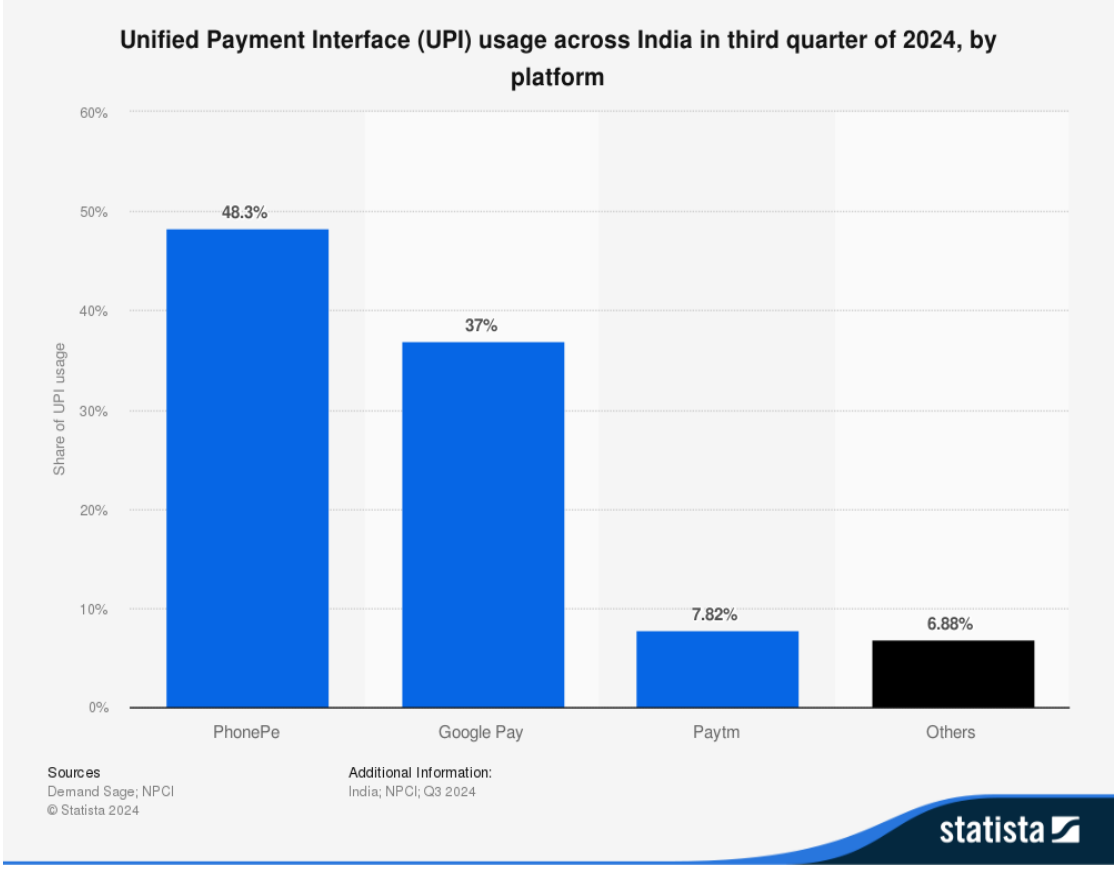

Figure 2.2: Unified Payment Interface (UPI) usage across India in third quarted of 2024, by platform
Source: Statista

2.4.2 Investment Management and Robo-Advisors in Fintech

Rising robo-advisors—who use algorithms and automation to manage investment portfolios at a cheaper cost than conventional human advisers—have changed investment management. Robo-advisors build diversified portfolios usually comprising low-cost ETFs by analysing consumer profiles including their risk tolerance and financial goals. Early in the 2000s, platforms like Betterment and Wealthfront pioneered this technique, democratising access to wealth management services by reducing entrance barriers and expenses (Gaspar & Oliveira, 2024).

Using mean-variance analysis, Robo-advisors shine in maximising portfolio allocations and offer hands-off portfolio management requiring minimal to no client interaction. To keep the client's intended asset allocation, these systems constantly monitor and rebalance portfolios, so improving convenience and lowering the necessity for human control (Gaspar & Oliveira, 2024).

Beyond only cost effectiveness, robo-advisors scalability has made investment management available to a wider spectrum of investors—especially those with less

wealth. This has created new opportunities for financial inclusion by letting regular investors access diverse portfolios that would otherwise need large minimums from traditional wealth managers (Reher & Sokolinski, 2024).

Robo-advisors do have difficulties even if their low costs, easy-to-use interfaces and scalability have helped them become somewhat well-known. These include worries around the openness of algorithmic conclusions and investor profiling techniques as well as the limits of automated advise, especially for complicated financial demands (Gaspar & Oliveira, 2024).

2.4.3 Payments and Money Transfers in Fintech

The financial technology (Fintech) industry has drastically changed the way money transfers and payments are handled. Transactions are now faster, more safe and more easily available. Driven by developments in mobile technology, blockchain and peer-to-peer (P2P) platforms, digital payments today represent a sizable share of worldwide financial activity.

The below figure highlights the most influential technologies shaping the payments industry, with **instant/real-time payments (75%)** and **open banking APIs (68%)** leading the way. AI and machine learning (45%) are also gaining traction, reflecting their role in fraud detection and automation within digital payments. The financial services sector has seen a fundamental shift from cash-based transactions to digital payments. Consumers now make payments online and at physical points of sale using fintech tools as PayPal, Apple Pay and Google Pay, which have transformed By including their personal devices—such as wearables and cell phones—into the payment process, these platforms provide users more convenience and contactless payments using near-field communication (NFC) technology (Khando et al., 2023).

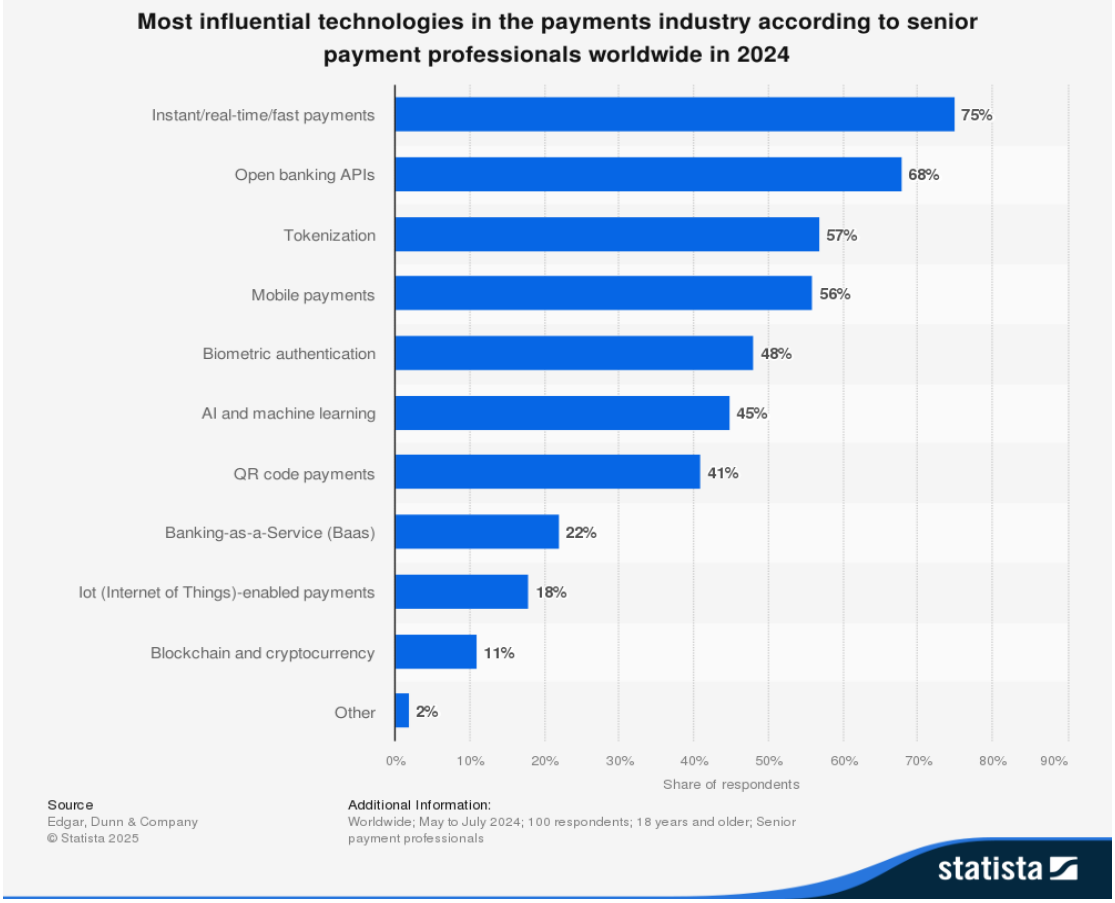

Figure 2.3: Key Technologies Shaping the Payments Industry in 2024
Source: Statista

By allowing customers to quickly send and receive payments, e-wallets have also helped to improve digital money transfers. Usually less costly than regular bank transactions, these websites eschew traditional banks. Especially in underdeveloped nations with insufficient conventional banking infrastructure, e-wallets have shown to be quite important in raising financial inclusion (IMF, 2023).

Mobile payments have grown especially in countries where smartphone use is high. Mobile payments have showed how they might narrow the gap in financial inclusion on platforms like Alipay in China and M-Pesa in Kenya. These platforms provide impoverished groups essential financial services (BIS, 2020) by allowing users save money, pay bills and move money without a bank account. Particularly in nations dependent on cross-border transfers, mobile payments have also helped to speed international remittances and reduce transaction costs.

Blockchain technology—especially with cross-border transactions is another incredible breakthrough in the Fintech landscape. Bitcoins and Ethereum permit distributed and

safe peer-to-peer payments without middlemen. Blockchain-based payments provide transparency and reduced transaction times and costs especially in international transfers, where traditional systems are occasionally slow and costly due of intermediaries (BIS, 2021).

While the spread of digital payments has numerous benefits, it also raises legal difficulties and cybersecurity risks. Authorities are focused on creating standards for consumer protection while driving invention in payment technology (IMF, 2023). A component of its global financial reform agenda, the G20 has given boosting efficiency and transparency of cross-border payments (BIS, 2020).

In the end, digital payments and money transfers have tremendously improved financial transaction accessibility, speed and simplicity. As Fintech advances financial inclusion, innovations like blockchain and mobile payments progressively challenge accepted banking standards.

2.4.4 Lending and Credit in Fintech

Fintech has revolutionised credit services and lending, therefore shifting the focus from traditional banks to more rapid, easily accessible, automated methods. Fintech financing democratises credit availability, reduces risk assessments and enhances client experiences by means of current technology such machine learning, alternative data sources and automated algorithms.

One obvious example of Fintech's impact on lending is peer-to- peer (P2P) lending, which links borrowers directly with investors over internet platforms, therefore eschewing traditional banks. P2P lending platforms like LendingClub and Prosper (Berg, Fuster, & Puri, 2022) offer unsecured personal loans, which enable investors possible larger earnings while providing more conveniently available credit alternatives for borrowers. These platforms routinely assess credit risk by leveraging alternative data outside of traditional credit ratings, thereby improving financial inclusion for individuals and businesses deprived by traditional banks (Di Maggio et al., 2022).

Advanced algorithms and big data analytics applied by fintech lending systems help to optimise the credit scoring process. Examining vast amounts of data, machine learning models more precisely predict borrower creditworthiness than more conventional methods (Gambacorta et al., 2019). For people without a traditional credit history especially, this use of alternative data—from utility bill payments to social media activity—has improved risk assessment and increased credit availability (Fuster et al., 2019).

The rise of fintech has significantly contributed to the popularity of the Buy-Now-Pay-Later (BNPL) model, which allows consumers to make upfront purchases and pay for

them over time. Companies such as Klarna and Afterpay have rapidly acquired market share providing this credit alternative immediately at the point of sale, usually with no interest or penalties for consumers should payments be completed on time (Berg et al., 2022). Younger consumers, who might choose this flexible payment approach over conventional credit cards, have especially found resonance in BNPL offerings.

Fintech lending creates risk management and legal issues even if it has democratised credit availability. Fintech lenders have to manage changing regulations meant to safeguard consumers and foster innovation by means of several regulatory frameworks. Furthermore unresolved are issues with credit risk, openness and data privacy especially as alternative lending mostly depends on non-financial data.

With more flexible and easily available loan possibilities, fintech lending and credit platforms have eventually changed the financial scene. Strong algorithms and alternative data have expanded credit availability to vulnerable people even if BNPL is still somewhat young. Still, the industry fights constantly to control hazards and satisfy regulations.

2.4.5 Insurance and Risk Management in Fintech

Fintech, commonly referred to as Insurtech, has changed conventional methods of risk management and insurance product development when included into the insurance sector. Using modern technologies such artificial intelligence (AI), blockchain, big data analytics and machine learning, Insurtech offers more reasonably priced, customised and safe insurance products. Apart from streamlining procedures, these technologies help companies to better manage client expectations and risk.

Insurance companies might quickly review vast amounts of data using data analytics and artificial intelligence, therefore improving the accuracy of risk assessments and pricing strategies. Artificial intelligence reduces human participation and error by automating underwriting, fraud detection, claim processing and underwriting. These tools also enable insurance firms create more tailored policies by means of consumer behaviour patterns and financial histories (Rupeika-Apoga & Marano, 2023). Blockchain systems improve insurance business security and openness. The unchangeable ledger of blockchain lets everyone involved in a transaction look over and check records, therefore reducing fraud. Smart contracts, based on blockchain, let insurance claims to be automatically executed once pre-defined criteria are met, therefore simplifying claims processing and reducing disagreement. For instance, more in demand parametric insurance—where pay-outs are automatically triggered by

specific events like natural disasters—driven by Insurtech solutions. On-demand and usage-based insurance (UBI) models made possible by insurtech innovations Consumers can now get insurance coverage especially suited for their needs often in real time. Artificial intelligence and data analytics help insurance firms to provide dynamic policies that vary depending on specific activity or situation by means of this degree of customisation. Modern risk management techniques mirror fintech developments. These instruments enable companies to forecast and reduce risks connected to financial instability, regulatory compliance, cybersecurity and other aspects as well. Stress-testing models, for example, allow insurers better prepare for unpredictability by approximating the financial effect of different scenarios such economic downturns or climate change (ISACA, 2020).

Insurtech offers many benefits, but there are also legal ones as well as the need of strong cybersecurity policies. Since they rely more on digital tools, insurance companies have greater concerns regarding data security and privacy. Particularly in view of the worldwide move towards digital financial services (Rupeika-Apoga & Marano, 2023), regulatory structures are still developing to handle these issues.

By using artificial intelligence, blockchain and big data analytics finally, Insurtech has transformed risk management in the insurance sector. These developments present fresh chances to increase efficiency and customisation as well as problems demanding solutions by better cybersecurity and regulatory oversight.

2.4.6 Wealth Management and Personal Finance in Fintech

Mostly driven by technical breakthroughs such artificial intelligence (AI), big data and blockchain, fintech has fundamentally transformed wealth management. These developments have democratised access to complex financial products and services hitherto reserved for high-net-worth individuals, therefore enabling wealth management more easily and affordably for a greater range of investors. The rise of robo-advisors marks among the most significant fintech developments in wealth management. Using computers, robo-advisors independently manage portfolios to offer tailored investing recommendations based on individual financial goals, risk tolerance and investment preferences. Eliminating the need for human counsellors greatly reduces the cost of investment management, so enabling professional wealth management to more people (PwC, 2022). Sites like Betterment and Wealthfront have become somewhat well-known due to their low costs and simplicity of use; they provide consumers automated rebalancing and tax-loss harvesting strategies to maximise returns and let them create financial goals, including retirement or savings for a major

purchase (Headinger et al., 2024). Combining this technology with artificial intelligence and machine learning enables more exact portfolio management, which may be changed in real-time depending on the state of the market (Ferreira 2019).
Fintech tools have improved personal money management much beyond wealth control. Apps and internet tools let people more quickly monitor their spending, handle debt and create future financial plans than they could have years before. Data analytics is used by tools like Mint and YNAB (You Need A Budget) to enable users classify their expenditure, create budgets and acquire understanding on how to maximise their financial situation (World Finance Council, 2019).

Personal finance systems are also including AI-powered financial planning tools, which provide more customised advise on risk management, savings and investments. By means of user data analysis, expenditure pattern identification and recommendation of actionable strategies for enhancing financial stability, these platforms can help to make financial literacy and proactive wealth management more realistic (Paiva et al., 2019).

Although Fintech has improved personal money and asset management significantly, problems still exist mostly related to data security and regulatory compliance. Safeguarding this data becomes crucial as more personal financial data gets digital. Particularly with regard to managing AI-driven financial advice and verifying these platforms are providing fair and objective suggestions, authorities are still adjusting to the quick-paced changes brought about by Fintech (PwC, 2022).

Looking ahead, by providing more safe and open ways for asset management and financial transactions, the combination of blockchain and decentralised finance (DeFi) can transform wealth management even further. Wealth management is likely to become much more tailored, safe and easily available to people all across the economic spectrum as these technologies keep developing.

2.5 IMPACT OF FINTECH ON TRADITIONAL FINANCIAL INSTITUTIONS

The rapid evolution of financial technology has significantly disrupted traditional financial institutions, reshaping their operational models, service delivery, and market strategies. Fintech innovations have introduced more efficient, cost-effective, and customer-centric alternatives, forcing banks and financial service providers to adapt to a rapidly changing digital ecosystem. While fintech has enabled greater financial inclusion and streamlined processes, it has also posed regulatory challenges and risks to legacy banking structures. The following subsections explore the various dimensions of fintech's impact on traditional financial institutions, including disruptions to banking

services, its role in financial inclusion, and the challenges it presents to existing financial models.

2.5.1 Disruption to Traditional Banking and Financial Services by Fintech

The emergence of fintech has fundamentally changed established banking and financial services, therefore changing the operations and client interaction of financial organisations. Mobile technologies, blockchain, artificial intelligence (AI) and data analytics—which have changed the financial scene by providing faster, more customised and more accessible financial services—drive this upheaval. There are key areas of disruption, they are:

1. **Customer-Centric Innovations**: Fintech companies have concentrated on building user-friendly, customer-centric systems that streamline wealth management, lending and payments as well as other operations. Digital payment solutions and mobile banking apps have given users easy access to their money, therefore lowering the demand for in-person banking and supporting a digital first approach. Customers are moving to digital alternatives since these platforms provide more convenience and accessibility than conventional banks.

2. **Lower Costs and Increased Efficiency**: Because they run with less overheads than established banks, fintech firms can provide more competitive rates for products such loans and investments. By directly matching borrowers with lenders at cheaper rates, peer-to- peer (P2P) lending platforms have lessened the demand for banks as middlemen (Berg et al., 2022). Furthermore, the incorporation of artificial intelligence has automated credit scoring and fraud detection, thereby enhancing efficiency and lowering operational expenses for financial institutions as well as for consumers (Rupeika-Apoga & Marano, 2023).

3. **Threat to Legacy Systems**: Because they depend on legacy systems, traditional banks are finding it difficult to adjust to these new technology. Maintaining these antiquated systems is expensive and less suited to the agile, creative ideas presented by Fintech companies. Banks are therefore under more and more pressure to digitally change their processes or risk losing market share. Moreover, the cost of modernising these outdated systems can be outrageous, which makes it difficult for traditional banks to deal with more tech-driven, agile Fintech startups.

4. **Collaboration Between Fintech and Traditional Banks**: Reacting to these upheavals, many major financial institutions have started working with fintech startups to exploit their technical innovation. Through this collaboration, banks can offer digital products while maintaining their fundamental banking procedures. For instance, many large banks have embraced blockchain technology to speed cross-border payments and cut transaction times. These partnerships highlight how traditional banks are evolving to remain relevant in a society going digital.

The rise of Fintech has created new regulatory problems since these companies might run outside the traditional banking regulatory structures. Data privacy and cybersecurity concerns abound given the volume of sensitive financial data Fintech companies handle. Policymakers aim to create adaptable models and regulatory sandboxes allowing innovation to blossom while ensuring consumer safety and financial stability.

In the end, the Fintech revolution is forcing incumbent banks to rethink their business models, adopt new technologies and offer more consumer-centric products. This disturbance offers financial industry innovation and development possibilities even if it causes problems.

2.5.2 Fintech's Role in Financial Inclusion and Reaching Underserved Populations

Especially by offering poor and unbanked populations all over financial services, fintech has been crucial in increasing financial inclusion. Lack of infrastructure, records, or credit history has historically prohibited many people in rural or economically impoverished places access to financial services. Using innovations in mobile technology, digital payments, blockchain and digital payments, fintech solutions have helped to close this divide and advance financial inclusion. Among other ways Fintech has contributed to advance financial inclusion is by use of mobile banking and mobile payment platforms. Mobile platforms like M-Pesa have been especially important in providing basic financial services including savings, transfers and payments in countries including sub-Saharan Africa (BIS, 2020) even to individuals without official bank accounts. Previously excluded from the financial system, persons who receive these services via mobile phones can now more effectively participate in economic activities.

Fintech has also had an impact in India. Simple and more accessible financial transactions have come via digital wallets as Paytm and Airtel Money and mobile money apps. Previously unreachable to millions, the government's initiatives towards

digital financial inclusion via programs like Jan Dhan Yojana and Aadhaar-linked bank accounts have increased the number of people with official financial services (Asif et al., 2023).

By means of digital credit scoring and peer-to- peer lending, fintech platforms have also improved credit availability for impoverished groups. By leveraging alternative data—such as mobile usage patterns and social media activity—fintech firms can analyse creditworthiness in a more inclusive manner and therefore let people without traditional credit histories apply for loans (Sokolinski et al., 2022). Particularly helped by this are small and medium-sized firms (SMEs) as well as those living in developing nations who occasionally struggle to obtain loans from reputable banks.

Blockchain technology has further contributed even more for financial inclusion by letting dispersed financial systems. Blockchain-based solutions eliminate middlemen, therefore reducing transaction costs and allowing low-income individuals to access more reasonably priced financial services. Especially in areas lacking strong financial infrastructures, blockchain also offers enhanced security and openness (Anakpo et al., 2023).

Notwithstanding these advances, achieving real financial inclusion with Fintech remains a challenge. Two main challenges—especially in far-off locations—are digital literacy and internet access to. Furthermore, legislative issues regarding consumer safety, privacy, and security must be resolved to guarantee the continuous expansion of Fintech solutions in financial inclusion (Asif et al., 2023). Fintech has been largely in charge of raising financial inclusion by offering impoverished people easily available and imaginative financial solutions. For millions of people—especially in poor areas—mobile banking, digital lending platforms and blockchain technology have opened new prospects. Fintech will thus need continuous efforts to tackle infrastructure and regulatory challenges if it is to completely realise its promise in expanding financial inclusion worldwide.

2.5.3 Challenges and Risks Fintech Presents to Traditional Financial Models

As well as challenges to traditional financial structures, fintech's fast expansion has introduced significant innovations to financial products. As fintech questions the received knowledge, banks and other financial institutions are under growing pressure to innovate or risk going extinct.

One of the main dangers Fintech poses is disintermediation—the elimination of long-standing middlemen such banks. Blockchain, peer-to-peer lending and digital wallets allow Fintech start-ups to match customers with vendors or lenders straight forwardly. This lessens the demand for conventional financial institutions acting as middlemen, therefore lowering their market share. For borrowers without established credit histories, for instance, peer-to-peer lending sites like Lending Club and Prosper have provided substitutes for bank loans, therefore subverting the predominance of banks in consumer lending.

Operating with legacy systems that are expensive to maintain and less adaptable than Fintech platforms, which rely on more recent, more efficient technologies, traditional banks are Changing these systems to match the quickness and efficiency of Fintech rivals calls for large investment, therefore taxing conventional institutions financially. Being more technologically advanced, fintech companies provide services such real-time payments, automated credit scoring and tailored client experiences at reduced operational costs, therefore challenging conventional banks' ability to compete on both price and service (Rupeika-Apoga & Marano, 2023).

Operating in a fast changing digital environment often faster than current regulations, fintech platforms For established institutions—which are highly regulated—this generates a degree of uncertainty and challenges their ability to innovate under tight compliance limitations. Fintech firms' activities are further complicated at the same time by changing laws on data privacy, fraud prevention and cybersecurity. As digital financial services expand, cybersecurity and data privacy have taken front stage. Often targets of cyberattacks are fintech services, which aggregate enormous volumes of personal financial data. This puts Fintech firms and their consumers at danger and begs questions about the security of consumer data handled and kept (Asif et al., 2023). While younger Fintech companies must quickly scale their security measures, traditional banks—who also suffer from cyberattacks—often have more established policies and procedures for controlling security risks.

Fintech's arrival has also set consumer expectations. Often beyond what conventional banks offer, digital platforms deliver quicker, more convenient, tailored services. This has changed consumer behaviour to demand flawless, user-friendly digital experiences, which forces established companies to improve their digital products if they are to keep market share. Moreover, the emergence of robo-advisors and AI-driven financial services has made wealth management more easily available to a larger population,

therefore challenging established financial advisers and wealth management organisations (Rupeika-Apoga & Marano, 2023).

Fintech creates dangers and difficulties to established financial institutions even while it offers great chances for innovation and financial inclusion. Legacy institutions that want to survive and flourish in this new environment have to make investments in digital transformation, welcome alliances with Fintech companies and create plans to lower growing risks—especially with relation to cybersecurity and regulatory compliance.

2.6 CURRENT TRENDS AND INNOVATIONS IN FINTECH

Fintech is rapidly evolving, with Artificial Intelligence (AI), Machine Learning (ML), Blockchain, Smart Contracts, RegTech, and Open Banking playing a transformative role in financial services. AI and ML enhance trading, fraud detection, credit scoring, and personalized financial services, while Blockchain and Smart Contracts improve transparency, security, and efficiency in financial transactions. RegTech is revolutionizing compliance by automating regulatory processes, reducing costs, and ensuring real-time risk monitoring. Meanwhile, Open Banking and API-based ecosystems are fostering financial inclusivity, competition, and innovation by enabling secure third-party access to banking data. While these advancements present immense opportunities, they also raise regulatory, ethical, and security challenges, requiring careful oversight to ensure fairness, transparency, and data protection in the evolving fintech landscape.

2.6.1 Artificial Intelligence and Machine Learning in Fintech

Offering improved capacities for data analysis, decision-making and automation, artificial intelligence (AI) and machine learning (ML) have become crucial elements in the development of Fintech, hence transforming conventional financial systems. Among many facets of finance, including trading, risk management, fraud detection, credit scoring and customer service, these technologies are transforming others. By allowing real-time data analysis and decision-making, artificial intelligence and machine learning have become rather important in changing algorithmic trading. By processing enormous volumes of market data, AI-driven systems may find trading trends, automatically run trades and maximise portfolio management techniques. Much faster than conventional methods, this technology improves trading accuracy, reduces human mistake and fits to market changes (El Hajj & Hammoud, 2023). One of the best examples of how artificial intelligence-driven automation has democratised access to

professional wealth management services are Robo-advisors, which utilise ML to optimise investment portfolios based on customer risk profiles. (Cao, 2021).

Fraud detection is yet another important use for artificial intelligence and machine learning in finance. Analysing user behaviour and transaction patterns, machine learning techniques identify abnormalities suggesting possible fraud. These systems keep ahead of developing hazards since they learn from fresh data, which helps them to grow constantly. Likewise, artificial intelligence is used in risk management, whereby financial organisations evaluate credit risk using predictive models, therefore guiding more accurate and data-driven lending and investment decisions (Cao, 2021).

Conventional credit scoring systems depend on small datasets like credit history, which might prevent a sizable fraction of the population from being able to get loans. By using other data sources—such as utility payments, smartphone usage and social media activity—AI and ML solve this problem to offer a more complete evaluation of an individual's creditworthiness. For underprivileged groups especially, this has increased credit availability and made the lending process more inclusive.
By means of consumer data analysis, AI and ML enable customised financial services by means of bespoke financial advice, offers and products. By use of behavioural analytics and client segmentation, banks and Fintech firms can generate tailored suggestions depending on personal preferences, hence enhancing customer loyalty and happiness.

Although artificial intelligence and machine learning offer many advantages for fintech, there are also drawbacks especially related to ethics, data protection and regulation. Financial organisations have to negotiate difficult regulatory environments to make sure artificial intelligence systems follow data security rules and keep openness in automated decision-making procedures. Furthermore under closer examination by both customers and authorities alike are ethical questions about the possible prejudice in artificial intelligence algorithms (Cao, 2021).

Notwithstanding these obstacles, the future of artificial intelligence and machine learning in finance seems bright since these technologies keep developing and provide even more financial inclusion, precision and efficiency.

2.6.2 Blockchain and Smart Contracts in Financial Services

Among the most revolutionary developments in the financial services industry, blockchain technology and smart contracts drastically change how agreements are enforced, trust is created and transactions are handled. Across a broad spectrum of financial services—including payments, insurance, trade finance and lending—these technologies have improved openness, efficiency and security.

A Distributed Ledger Technology (DLT), blockchain lets transactions be securely, transparently and unchangeable recorded. By means of cryptographic techniques, a network of nodes verifies every transaction, so guaranteeing data integrity and hence lowering the need for middlemen (Garcia et al., 2024). By removing central points of failure and providing a substitute for conventional clearinghouses and financial intermediaries—which are prone to delays and mistakes—the distributed character of blockchain lowers operational risks (Weerawarna, Miah, & Shao, 2023).
Cross-border payments, where blockchain helps solve problems of high transaction costs and long processing times are among the most obvious uses for it in financial services. Conventional cross-border payments involve several middlemen, each of whom adds expenses and can take several days. Blockchain-based systems, on the other hand, enable almost immediate and less expensive transactions, hence greatly improving efficiency (Garcia et al., 2023). Smart contracts are self-executing agreements with directly written in code terms of agreement. These agreements are kept on the blockchain and automatically enforce or execute terms upon defined criteria. Particularly in trade finance, insurance claims processing and real estate transactions (Peer-to-Peer Networking and Applications, 2023), smart contracts speed up procedures and save costs by eliminating intermediaries like lawyers or brokers.
Among the most well-known venues for creating smart contracts is Ethereum. It lets creators of Distributed Apps (DApps) automate lending, borrowing and asset transfers, hence transforming the Decentralised Finance (DeFi) ecosystem (Buterin, V., 2023).

Adoption of smart contracts and blockchain offers financial institutions several important advantages including:

Transparency: The public ledger system of blockchain guarantees that every transaction is seen by users, therefore lowering fraud.
Efficiency: Smart contracts help to reduce hand-made mistakes and administrative costs by automating challenging financial chores.

Security: The cryptography systems of blockchain technology stop illegal access and data modification.

Legislative ambiguity, scalability and privacy issues over data still present difficulties nonetheless. Blockchain systems such as Ethereum reveal scalability problems that impede their capacity to quickly process high number of transactions. Many nations devoid of thorough legislation addressing blockchain and smart contracts impede general application of these technologies even more.

By increasing security, openness and efficiency, blockchain and smart contracts will at last transform financial services. Notwithstanding currently existing challenges, these technologies have great potential to simplify and change financial processes.

2.6.3 Regulatory Technology (RegTech) and Compliance Solutions

Regulatory technology, sometimes known as RegTech, is the application of current technologies including Artificial Intelligence (AI), blockchain and big data analytics to simplify and improve financial services industry regulatory compliance. RegTech is supposed to help banks fulfil their legal obligations, reduce their non-compliance risk and manage the ever more complicated regulations. It also seeks to increase in these respects efficiency. There are key benefits and applications of Regtech such as Automating Compliance Process, Real-time Monitoring and Reporting and Risk Management.

RegTech technologies automate many of the frequently tedious compliance chores including regulatory reporting, Know-Your-Customer (KYC) validation, Anti-Money Laundering (AML) processes. Automation reduces human error, saves money and accelerates the reporting process—all of which are vitally critical as regulatory systems becoming more complex. For example, AI-powered solutions can quickly review vast amounts of data to identify any regulatory violations and contact compliance management, therefore ensuring timely action (Garcia et al., 2023).

Among RegTech's most valuable offerings is its ability to give real-time regulatory reporting and monitoring. Unlike certain traditional methods occasionally dependent on regular reports, RegTech solutions enable financial companies to continuously monitor compliance, so enabling them to immediately adapt to any regulatory change or new risk. Early anomaly detection made possible by this real-time capability is also quite beneficial in managing financial misbehaviour and fraud related risks. (Mueller, 2020)

RegTech uses big data and machine intelligence to provide financial firms strong tools for managing regulatory risk. Before things become more serious, these tools can track customer activity, uncover questionable transactions and even project prospective compliance issues. For example, machine learning techniques can identify tendencies of fraudulent behaviour, therefore ensuring that financial institutions stay compliant and lowering risks. (Packin 2023).

RegTech is progressively adding blockchain technology into its systems to improve security and openness. The unchangeable ledger of blockchain guarantees honest and simple auditable record-keeping, therefore ensuring accuracy of compliance data. Smart contracts, for instance, can be used to autonomously enforce legal obligations, running tasks like transaction approvals when prerequisites are satisfied (Olaiya et al., 2024). RegTech has various difficulties even with its potential. Combining RegTech solutions with current legacy systems in financial firms can be challenging and expensive. Furthermore, issues of data privacy and cybersecurity loom big, especially as RegTech systems depend on the processing of enormous volumes of sensitive information. Regulatory authorities are still creating plans for the general acceptance of these technologies and verifying that they satisfy compliance criteria stays a challenge (Olaiya et al., 2024).

Looking ahead, the combination of RegTech with Supervisor Technology (SupTech)—used by authorities to better their supervisory functions—will probably help to increase openness and efficiency even further. RegTech is predicted to be increasingly important as these technologies develop in enabling dynamic regulation, therefore enabling financial firms and authorities to react faster and more precisely to changes in the regulatory environment (Mueller, 2020).

2.6.4 Open Banking and API-Based Ecosystems

In the financial services industry, open banking is a revolutionary development whereby third-party suppliers may access banks data using Application Programming Intervals (APIs). From conventional bank-centric operations to an open ecosystem where banks, Fintech companies and other third parties cooperate to provide creative financial goods and services, this paradigm changes the scene. For financial institutions, open banking improves client experience, stimulates rivalry and creates fresh income sources.

APIs provide safe data interchange between banks and outside providers (TPPs), hence enabling open banking. Customers can exchange their financial data with other service providers and access a wide range of financial tools, including budgeting apps, investing platforms and loan services, by using APIs, therefore avoiding leaving their main banking platform (Zachariadis & Ozcan, 2022).

A major legislative action in Europe helping open banking was the adoption of Payment Services Directive 2 (PSD2). If consumers provide permission, this control requires banks to distribute consumer data to authorised TPPs. Likewise, nations like the UK and South Korea have created uniform open banking systems to boost competitiveness and inspire creativity (Choice, 2024).
There are benefits of open banking such as Enhanced Customer Experience, Innovation and Competition, Increased Financial Inclusion.

Through control over their financial data, open banking enables consumers. APIs let them more quickly switch between providers, obtain customised financial products and compare services. Data democratisation drives innovation since fintech startups can create unique products providing tailored financial services. Open banking increases competitiveness by letting non-bank companies access financial data, so pushing traditional banks to develop their offerings. Because of their agility, fintechs are more suited to provide customer-centric services, therefore producing a more dynamic and competitive financial environment (Zachariadis & Ozcan, 2022). By means of API-based systems enabling the extension of banking services to underprivileged groups, open banking has the potential to increase financial inclusion. Fintech services built on open banking APIs can provide reasonably priced and easily available financial solutions, like digital wallets and micro-loans, in areas where traditional banking is scarce (Choose, 2024).

2.7 CONCLUSION

In conclusion, this chapter provided a comprehensive understanding of the technological advancements shaping the Fintech revolution and their profound impact on the financial sector. By tracing the historical evolution of Fintech, researcher highlighted the gradual transition from traditional financial systems to fully digital platforms. The discussion on key technologies, including AI, ML, blockchain, mobile banking, and cryptocurrency, demonstrated how these innovations are driving efficiency, personalization, and accessibility in financial services. Furthermore, researcher explored how Fintech applications, such as robo-advisors and peer-to-peer lending, are transforming retail banking, wealth management, and investment services.

The disruptive influence of Fintech on traditional financial institutions was also examined, emphasizing the need for adaptation and innovation to remain competitive. Lastly, emerging trends like open banking and RegTech were discussed, showcasing their role in enhancing regulatory compliance and promoting financial inclusion. While Fintech continues to reshape the financial landscape, challenges such as data security and regulatory complexities remain crucial considerations.

Now turning to one of the most significant technologies altering the financial landscape—AI—researcher proceed to "Chapter 3: Artificial Intelligence: Evolution, Nature and Emerging Dimensions". Following its early years and examining how artificial intelligence has evolved financial services, particularly in fintech, this chapter will explore the expansion of this technology. Researcher shall examine the expanding dimensions of artificial intelligence with an eye on its capacity for learning, adaptation and intelligent decision-making inside the financial ecosystem. Artificial intelligence presents new chances for innovation as well as challenges like blunders, ethical dilemmas and blockchain technology integration while it is revolutionising tasks like fraud detection, risk assessment and customer personalising.

CHAPTER 3

ARTIFICIAL INTELLIGENCE: EVOLUTION, NATURE AND EMERGING DIMENSIONS

"Our intelligence is what makes us human, and AI is an extension of that quality." — **Yann LeCun**

3.1 INTRODUCTION TO ARTIFICIAL INTELLIGENCE (AI)

Artificial Intelligence (AI) has emerged as one of the most transformative technologies of the 21st century, reshaping industries, economies, and everyday life. AI refers to the simulation of human intelligence in machines, enabling them to learn, reason, and perform tasks that typically require human cognition. From simple rule-based algorithms to advanced machine learning models, AI has evolved significantly, driving innovation across various domains, including healthcare, finance, education, and governance. In the context of financial technology (Fintech), AI plays a pivotal role in automating processes, improving decision-making, and enhancing user experiences. As AI continues to evolve, its ethical, regulatory, and operational implications become increasingly significant, warranting a deeper examination of its fundamental principles, applications, and challenges.

3.1.1 Meaning of Artificial Intelligence (AI)

In computer science, Artificial Intelligence (AI) is the discipline devoted to designing systems or machines able of doing tasks usually requiring human intelligence. Among these chores are those of perception, language comprehension, learning, problem-solving and decision-making. From Artificial General Intelligence (AGI), which seeks to replicate human cognitive capacities across a wide range of activities, to narrow artificial intelligence (which focusses on performing specific tasks such speech recognition or facial identification), Artificial Intelligence (AI) spans a vast array of technologies (Stanford HAI, 2020).

Analysing vast amounts of data allows Artificial Intelligence (AI) to identify trends, generate predictions and change with fresh data. Systems that depend on Machine Learning (ML)—a subset of artificial intelligence that lets systems "learn" from data, hence improving performance over time without explicitly programming—show this most well. Whereas unsupervised learning aims to find hidden patterns in data without

specified labels, supervised learning entails training algorithms on labelled data (Caltech Science Exchange, 2024).

Deep learning, the use of neural networks to replicate human brain processes—has advanced artificial intelligence in automaton, decision-making and predictive analysis. But as technology advances and finds fresh uses in many sectors, AI's definition changes as well.

3.1.2 Overview of AI's Impact on Various Industries, with a Focus on Fintech

Across several sectors, artificial intelligence (AI) has shown transforming power, bringing fresh efficiencies, automating difficult operations and providing superior predictive capability. While its influence on Fintech has been particularly significant, its application in sectors including retail, manufacturing and healthcare has changed established business structures.

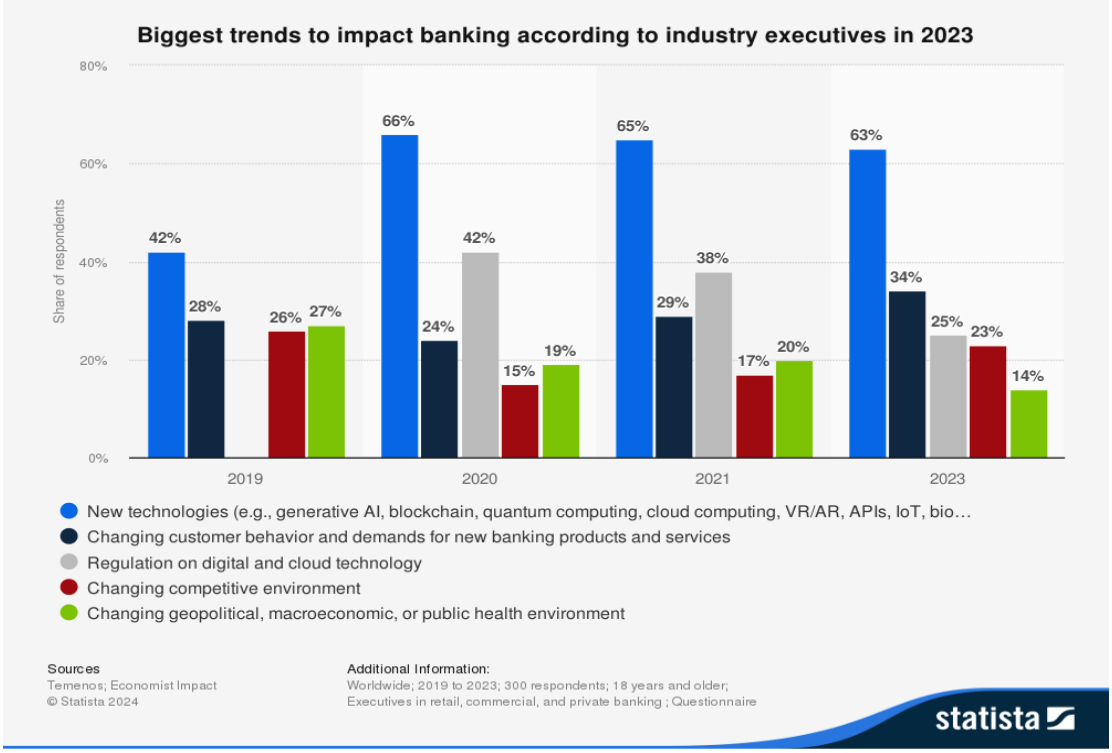

Figure 3.1: Trends Impacting Banking in 2023

Source: Statista

According to a Statista (2024) survey**,** 63% of banking executives identified *new technologies*—including AI, blockchain, and cloud computing—as the biggest factors shaping the banking industry in 2023. This highlights the growing reliance on AI for fraud detection, risk assessment, and customer service automation. As financial institutions embrace AI-driven solutions, regulatory frameworks must evolve to balance innovation with consumer protection.

3.2 EVOLUTION OF AI IN FINANCIAL SERVICES

The evolution of Artificial Intelligence (AI) in financial services has been marked by significant milestones, transforming the fintech industry. Early AI models in the 1980s and 1990s focused on risk assessment, algorithmic trading, and fraud detection, laying the groundwork for modern AI-driven financial systems. The 2000s saw AI's integration into fraud prevention and Anti-Money Laundering (AML)**,** enabling real-time detection of suspicious transactions. The 2010s introduced robo-advisors and AI-powered credit scoring, improving financial inclusion and personalized investment strategies. More recently, open banking, AI-driven personalized financial services, and blockchain integration have revolutionized the fintech landscape, enhancing security, efficiency, and accessibility. While AI continues to drive financial innovation, challenges such as regulatory compliance, algorithmic bias, and data security remain critical considerations for its future adoption.

3.2.1 Early Developments in AI: Historical Background

Artificial intelligence (AI) originated in the middle of the 20th century when the idea of building computers able of intelligent behaviour was first presented. John McCarthy first used the word "AI" in 1956 during the Dartmouth Conference, generally considered as the formal field of study's founding event. Early days of artificial intelligence research concentrated on symbolic artificial intelligence, in which computers would be programmed to follow human-like reasoning across a set of established rules (Turing Institute, 2023).

Expert systems, computer programs that replicated the decision-making capacity of human specialists in particular disciplines such financial planning and medical diagnostics—developed under artificial intelligence during the 1960s and 1970s. These systems prepared the way for the rule-based methods that would be essential in early artificial intelligence implementations in many fields, including banking (MDPI, 2023).

But given inadequate computer capacity and the primitive state of algorithms, AI's powers stayed constrained during this period. AI research acquired fresh impetus only in the 1990s and 2000s with developments in Machine Learning (ML) and neural networks. From symbolic AI to statistical AI (arXiv, 2021), these methods let systems learn from vast datasets without explicit programming for every task.

Early adopters of artificial intelligence in the financial services industry started with risk assessment systems and algorithmic trading in the 1980s and 1990s. Mostly utilising rule-based systems and basic statistical techniques, early artificial intelligence

models in finance were used for credit scoring, fraud detection and risk management. Today's more complicated machine learning-driven financial systems (Cao, 2021) were born out of AI applications expanding to more sophisticated domains like automated trading and portfolio management as computational capabilities developed.

Therefore, especially in the financial services sector, the early history of artificial intelligence, marked by both symbolic and statistical methods, offered a vital basis for the fast development of current artificial intelligence.

3.2.2 Key Milestones in AI Adoption within Fintech

Artificial intelligence (AI) has been transformingly incorporated into the financial technology (Fintech) industry at numerous important turning points during the past few years. From fraud detection to automated trading and client personalising, these benchmarks show how artificial intelligence has changed several parts of financial services.

1. **Algorithmic Trading and High-Frequency Trading (1990s-2000s)**: Algorithmic trading was among the first uses of artificial intelligence in the financial industry. AI-enabled systems were created to automate trading operations by the late 1990s, therefore enabling institutions to run trades at rates and quantities much beyond human capability. High-Frequency Trading (HFT), largely dependent on artificial intelligence algorithms to study vast databases and run orders in milliseconds, changed the stock markets. In banking, where speed and data analysis are highly important, this milestone prepared the ground for more advanced applications of artificial intelligence.

2. **Fraud Detection and Anti-Money Laundering (2000s)**: Among the most important developments has been in the field of fraud prevention. Artificial Intelligence (AI) is absolutely essential in fraud detection and prevention within the financial sector since it helps companies to quickly identify dubious conduct. Conventional fraud detection methods, manual inspection and rule-based systems, usually prove insufficient given the scale and complexity of financial crimes nowadays. Artificial intelligence has reduced the risk of undetectable fraud by means of advanced Machine Learning (ML) models able of assessing vast amounts of financial data, pattern identification and prediction of fraudulent activity. AI-driven machine learning algorithms find fraudulent activity using both supervised and unsupervised learning methods. Using labelled cases of fraud, supervised models—trained on past data—predict future fraudulent transactions. Conversely,

unsupervised models uncover patterns that depart from the norm by means of anomaly detection, therefore suggesting novel, hitherto undetectable forms of fraud (MDPI, 2022). Unsupervised learning is especially useful for spotting new fraud methods, such cyberattacks on financial networks, since this capacity to recognise anomalies. One major benefit of artificial intelligence for fraud prevention is real-time processing capabilities. Rather than after the fact, AI systems may identify and highlight dubious behaviour as it happens by tracking transaction data streams. This lets financial institutions act right away to stop fraud, whether that means stopping a transaction or notifying the account owner. Particularly in credit card fraud detection, artificial intelligence has proved revolutionary since models monitor thousands of transactions per second to find unusual trends.

Big data helps artificial intelligence also in fraud detection. The technique gets more effective in spotting fraud the bigger and more varied the dataset used to teach artificial intelligence models is. Unprecedented transaction data now available to financial institutions allows AI systems to create reliable predictive models by means of analysis. By enabling these systems to process enormous datasets in real-time and hence improve their scalability, cloud-based platforms help.

These developments notwithstanding some difficulties. False positives—where actual transactions are labelled as fraudulent—are one of the main problems. High false positive rates can tax consumer frustrations and overwhelm fraud detection staff. Furthermore severely burdening financial institutions is AI systems' need for constant updates and retraining to be successful against fresh fraud techniques (MDPI, 2022). Early artificial intelligence systems made use of rule-based models; but, as machine learning techniques evolved, AI can now learn from previous fraud tendencies and project future fraud activities in real time. This has particularly proven successful in payment systems and digital transactions where artificial intelligence scans millions of transactions and finds anomalies in seconds (Maple et al., 2023). Detecting fraud completely depends on studying enormous volumes of transaction data in real-time, AI-driven systems to identify suspicious behaviour. These technologies enable financial companies stop losses by means of better tendency of fraud detection via learning from prior mistakes. As the Fintech sector developed, artificial intelligence became fairly important for Anti-Money Laundering (AML) operations and fraud detection. Artificial intelligence systems using Machine Learning (ML) could identify odd transaction trends suggesting possible fraud. Since it let financial institutions more quickly and successfully stop

fraud, online transactions grew and this program proved indispensable (Ridzuan et al., 2024). Modern fraud protection strategies still revolve around artificial intelligence's basic predictive powers.

3. **Robo-Advisors and Automated Financial Planning (2010s)**: Robo-advisors offer a unique use of artificial intelligence (AI) in specialist financial services by means of automated investment management and financial advising founded on algorithms. These systems provide customised portfolios fit for clients' financial objectives, risk tolerance, investment times by minimum human interaction. Artificial intelligence provided made possible Robo-advisors could be performing among other important chores portfolio management, risk analysis, and financial forecasting. These systems can review vast volumes of data in real-time using machine learning algorithms, thereby providing investment advice usually more accurate and data-driven than those of conventional financial advisers. Their application depends on their capacity to customise financial recommendations. Robo-advisors create portfolios that satisfy personal tastes using information on a client's income, spending patterns, financial goals and risk tolerance. Robo-advisors' access to personal financial data including cash management practices and savings strengthens this personalising (Belanche, Casaló, & Flavián, 2019) (Byrum, J., 2022). The ability of robo-advisors to always adjust portfolios to fit evolving customer financial demands and market conditions is one of their primary advantages. Through mean-variance optimization—which balances the expected return against the risk— (Capponi, Olafsson, & Zariphopoulou, 2019) can show how AI-driven systems may maximise portfolios. Dynamic rebalancing of portfolios depending on real-time market data is made possible by this procedure; human advisers would not be able to reproduce manually on such a broad basis. Furthermore, robo-advisors let customers match their investments with personal ethical principles by progressively including features like tax-loss harvesting, automated rebalancing and even socially conscious investing (SRI) preferences (Beck, A.D., 2021; Byrum, J., 2022). Notwithstanding its benefits, artificial intelligence-driven robo-advisors nevertheless have difficulties, mostly related to ethical decision-making and client confidence. Sometimes the lack of personal touch causes customers to feel cut off from their financial management. Furthermore, even if artificial intelligence can evaluate and process enormous volumes of data, it is not immune to prejudices in the data or the algorithms themselves, which can result in distorted financial advice (Capponi, Olafsson, & Zariphopoulou, 2019). Moreover, the regulatory scene for robo-advisors is still

changing since different countries impose different degrees of supervision. For example, robo-advisors in the US have to follow the same securities rules as human financial advisers, therefore guaranteeing that they behave in their clients' best interests (Byrum, J., 2022). AI-powered robo-advisors are opening sophisticated investment management to a larger audience. Although ethical and legal issues must be taken care of in order to realise their full potential, their capacity to continuously monitor and change portfolios depending on real-time data offers a great advantage over conventional advice services. With robo-advisor artificial intelligence has democratised investment management. Analysing a user's financial goals, risk tolerance, market environment, these AI-powered apps offer customised investing advice. Robo-advisors serve to make wealth management more universally accessible by providing reasonably cost alternatives for human financial counsellors (Jiao et al., 2021). Early 2010s robo-advisor introduction signalled a sea change in financial technology artificial intelligence. By providing automated, data-driven investing advice at a fraction of the cost of traditional human advisers, these AI-powered systems democratised financial planning. Early adopters with little sums advanced portfolio management skills are Betterment and Wealthfront. Already managing billions of dollars worldwide, robo-advisors offer customised investing plans based on client profile and risk tolerance.

4. **AI-Powered Credit Scoring and Lending (2010s)**: By improving accuracy, speed and inclusivity in evaluating creditworthiness of people and companies, Artificial Intelligence (AI) has transformed risk management and credit scoring. Many times limited to a small range of financial data, traditional credit scoring systems made it challenging for those with little or no credit history to obtain financial services. By include alternative data sources including utility payments, social media activity and expenditure patterns, artificial intelligence has broadened the range of data utilised for credit evaluations and produced more inclusive and inclusive credit profiles (Noriega et al., 2023).

   By analysing vast amounts of data and seeing trends sometimes missed by conventional statistical models, artificial intelligence—especially machine learning—has made more complex modelling of credit risk possible. By use of gradient boosting and neural networks, older techniques as logistic regression (Suhadolnik et al., 2023) provide higher accuracy forecasts of default or delinquency. From new data, artificial intelligence models learn continuously, improving their forecasts over time and increasing risk assessments. The capacity

of artificial intelligence to process enormous volumes of real-time data has greatly shortened the time needed for credit determinations. Now that financial organisations can automatically score credit, loan approvals or denials are possible right away. Particularly in digital lending platforms, this has not only improved operational efficiency but also allowed lenders to service more consumers on scale. Particularly by spotting high-risk consumers and tracking continuous financial activity, artificial intelligence also is quite important for risk management. Real-time flaging of possibly fraudulent behaviour and anomaly in transaction patterns enabled by AI-driven systems Learning from past fraud events, these systems adapt to new challenges and give financial institutions a dynamic method of handling risk (Sari et al., 2024). The capacity of artificial intelligence to evaluate people without conventional credit records is one of its main benefits for credit scoring. By using alternative data, artificial intelligence systems provide a more comprehensive credit evaluation, therefore extending financial services to hitherto underprivileged populations such small enterprises and people in developing economies (Noriega et al., 2023). Growing financial inclusion drives more people today to be able to obtain credit and loans. Using artificial intelligence for credit analysis is difficult. Among the problems are the opacity of artificial intelligence models, frequently referred to as the “black box” dilemma, which calls for consideration on credit decision openness and responsibility. Furthermore, incorrect control of the bias probability in artificial intelligence systems could produce biassed outcomes. Ethical rules and explainable artificial intelligence models should help to overcome these constraints thereby guaranteeing the fairness and dependability of credit systems driven by artificial intelligence. (Suhadolnik et al., 2023). More inclusive credit rating systems have improved loan availability by means of artificial intelligence application. By using new data sources—utility payments and social media activity—AI enables lenders to evaluate the creditworthiness of people without conventional credit backgrounds. Especially in less developed areas, this technology has improved financial inclusion (Garcia et al., 2023). Through altering credit scoring methodologies, artificial intelligence has opened access to credit by creating creditworthiness-assessed alternative data sources such utility payments and social media conduct. This has allowed poor communities and small businesses without established credit histories financial institutions to contact (Cao, 2021). Credit has become more inclusive and accessible as artificial intelligence can analyse many datasets and find trends in financial behaviour. Sometimes traditional credit scoring systems left out folks without a recognised credit history. But as artificial intelligence-driven credit scoring systems emerged, fintech businesses

started evaluating creditworthiness more holistically with alternative data—utility payments and social media activity. For once underprivileged groups, this historic event has been crucial in increasing credit access (Muthukannan et al., 2020). AI could be able to assess enormous volumes of non-traditional data, so lenders could provide loans to people and companies without conventional credit background.

5. **Open Banking and Personalized Financial Services (2020s)**: Artificial intelligence improves user experiences in fintech by way of chatbots and virtual assistants offering 24/7 customer service. These systems communicate with customers in natural language processing (NLP) to generate tailored financial suggestions based on actual responses to queries and personal need (Zachariadis & Ozcan, 2022). Through open banking—in which banks use APIs to communicate consumer data with different service providers— artificial intelligence has helped to create more customised financial solutions. By means of transactional and behavioural data analysis, artificial intelligence systems develop bespoke banking experiences including budget advice or personalised savings strategies. As artificial intelligence technology is progressively implemented into financial institutions, this inclination is most likely going to grow even more and raise customer satisfaction (Boukherouaa et al., 2021).

6. **AI and Blockchain Integration**: One of the most drastic financial innovations is the integration of Artificial Intelligence (AI) with blockchain technology. While blockchain provides a distributed, unchangeable ledger system that builds trust and openness, artificial intelligence gives great analytical and decision-making capability. All considered together, these technologies offer novel opportunities for security, creativity, and efficient enhancement of financial services. Among the main benefits of including artificial intelligence and blockchain technologies into fintech are enhanced security. Blockchain enabled distributed ledger guarantees open, unchangeable, tamper-resistant financial transactions. Many nodes spread over a distributed network check every transaction, so building a trust less system in which consumers are not dependent on middlemen (Nakamoto, 2008; Crosby et al., 2016). By real-time anomaly detection—that is, by means of blockchain data analysis for deviations including fraudulent transactions or anomalies—AI enhances this and reduces the risks connected to human mistake or bad behaviour taken combined, so producing more safe financial ecosystems (Saberi et al., 2019). Moreover very crucial for automating financial services are artificial intelligence and blockchain. Smart contracts, self-executing agreements with terms straight

inscribed into code possible, are made possible by blockchain technology. Working on blockchain technologies, these smart contracts automatically finish transactions depending on pre-defined criteria. Artificial intelligence greatly enhances this even more by means of contract optimisation, transaction time prediction based on market data and identification of possible contractual difficulties before they emerge. Growing scalability of more intelligent and efficient automated financial activities made feasible by this mix serves to reduce the need for human supervision. Artificial intelligence has to run effectively on enormous amounts of data and blockchain technology provides a safe, open source of financial data. Blockchain is unchangeable so accurate projections and judgements based on artificial intelligence algorithms believing in the facts they are analysing are guaranteed. Furthermore enabling speedier responses to market movements, fraud detection and compliance needs possible is AI's significantly faster processing of this data than of conventional systems. Particularly in financial services, where fast decisions could lead to significant risk reduction or cost savings, this is absolutely crucial.

Integration of artificial intelligence with blockchain in fintech still presents difficulties notwithstanding its promise. Scalability problems abound in blockchain systems and verifying transactions calls for processing capability that could be costly and slow. Conversely, artificial intelligence depends on large volumes of data processing, which can contradict the energy-efficient models blockchain aims towards. Still, continuous research and development will help to solve these issues; the future appears bright for more flawless integration of various technologies (Taherdoost, 2022). All things considered, blockchain and artificial intelligence integration is fuelling major fintech innovation. Combining the characteristics of both technologies will enable financial organisations to build more intelligent, safe and efficient systems enhancing anything from automated financial services to fraud detection. Blockchain technology has been progressively included into artificial intelligence applications recently. Especially in trade finance and cross-border payments automation, artificial intelligence advances Fintech blockchain technologies. This link assists financial transactions to become more open, effective, and safe, so promoting perfect worldwide financial operations (Garcia et al., 2023). In fields like smart contracts and distributed finance (DeFi), where AI may automate and maximise demanding financial tasks, this milestone is especially clear. Blockchain provides a safe, unchangeable ledger while artificial intelligence presents predictive analytics and decision-making ability. The two technologies are

thus complimentary. This connection has great possibility to improve financial services' transparency, security and efficiency.

These benchmarks show how artificial intelligence has always changed the financial scene, fosters innovation and generates more inclusive, safe and efficient financial institutions. As artificial intelligence develops, its influence in fintech will probably grow and provide ever more complex uses all over the financial system.

3.3 THE NATURE OF AI: CAPABILITIES AND LIMITATIONS

Artificial Intelligence (AI) has made significant strides in transforming industries by automating tasks, analyzing vast datasets, and providing intelligent decision-making capabilities. However, despite its advancements, AI remains a field with both strengths and limitations. The extent to which AI systems can perform tasks is largely determined by their underlying architectures, ranging from narrowly focused applications to highly theoretical models of general and superintelligence. While AI has demonstrated remarkable capabilities in financial services, healthcare, and automation, it is still bound by challenges such as ethical concerns, regulatory constraints, and data dependency. Understanding the capabilities and limitations of AI is crucial to ensuring its responsible and effective deployment in various sectors.

3.3.1 Types of AI: Narrow AI, General AI and Superintelligence

Based on the extent and complexity of their capabilities, Artificial Intelligence (AI) is typically classified as either narrow artificial intelligence, general artificial intelligence, or superintelligence. Every kind denotes different degrees of machine intelligence, together with varied degrees of autonomy and problem-solving power.

1. Narrow AI (Artificial Narrow Intelligence - ANI)

Narrow artificial intelligence is artificial intelligence systems meant for a particular task or a limited spectrum of tasks. These highly specialised systems run under present limits. Among these are virtual assistants (like Apple's Siri or Amazon's Alexa), facial recognition systems and recommendation engines applied by companies including Netflix and Amazon. These systems lack overall problem-solving capacity yet shine in completing specific tasks.

Often referred to as "weak AI," narrow artificial intelligence functions without general reasoning or self-awareness. Although these systems can manage difficult chores as disease diagnosis or financial transaction processing, they cannot share their knowledge

or experience outside their own field of speciality (Cao, 2021). Since almost all artificial intelligence applications nowadays fit this criteria, ANI is the most used kind of artificial intelligence.

2. General AI (Artificial General Intelligence - AGI)

General artificial intelligence is the ability of AI systems to independently carry out a wide range of tasks across several fields, with human intelligence-like capacity. At this point, general artificial intelligence is theoretical since no current system has reached the degree of cognition needed to adapt to new tasks in the manner humans do. Just like a human can, AGI systems would be able to transmit knowledge across many spheres, reason, learn from experience and apply that learning to a wide spectrum of activities (Bostrom, 2014).

Developing AGI calls for innovations in cognitive architecture, machine learning and understanding and interpretation of the subtleties of human experience. Though AGI is still far off, research in fields including neural networks and human brain emulation keeps on trying to recreate broad human cognitive ability (Rathi, 2022).

3. Superintelligence (Artificial Superintelligence - ASI)

A potential type of artificial intelligence, superintelligence would transcend human knowledge in all spheres. Such an artificial intelligence system would have cognitive skills and problem-solving capacity much above that of the brightest human brains. It could be able to grow personally, therefore its intellect increases exponentially and results in a level of knowledge and capability beyond human comprehension (Bostrom, 2014).

ASI begs questions about existential hazards, ethical consequences and control. Should artificial intelligence systems be able to outsmart and outmanoeuvre humans, they may seriously endanger human civilisation. Talks on superintelligence usually centre on the possibility for machines to grow motivations or goals contradicting human well-being (Everitt, 2018).

Ultimately, these three forms of artificial intelligence show the development of machine intelligence from specialised task performance (ANI) to a more general and flexible knowledge of the environment (AGI and ASI).

3.3.2 Capabilities of AI in Decision-Making and Data Processing

By allowing systems to examine vast databases and make judgements with little human involvement, artificial intelligence's data processing and decision-making powers have revolutionised several sectors. The ability of Artificial Intelligence (AI) to comprehend enormous volumes of structured and unstructured data, discover patterns and forecast outcomes using advanced techniques such Machine Learning (ML), Natural Language Processing (NLP) and neural networks determines much of how these fields evolve.

The fundamental capacity of artificial intelligence for data processing dictates its capacity for decision-making. While artificial intelligence can quickly analyse and assess vast amounts of data in real-time, traditional data processing techniques are constrained by their capacity to manage such volumes. Using deep learning and other algorithms, artificial intelligence systems extract insights from both structured and unstructured data (e.g., consumer comments, social media posts) and structured data (e.g., financial reports) (Huang, 2023). These systems run continuously and grow in accuracy over time by learning from fresh data inputs.

Artificial intelligence-driven data processing supports in particular the financial sector's ability to enable algorithmic trading—which automates financial transactions by examining market patterns and making trades based on predictive analytics—in particular (Garcia et al., 2023). Maintaining competitiveness in fast-paced marketplaces calls on this swift and exact management of significant volumes.

Using machine learning techniques to identify trends, provide projections and propose best actions depending on current data helps artificial intelligence shine in improving decision-making. In fields such credit risk assessment, artificial intelligence algorithms explore consumer data including alternative credit indicators to more precisely estimate default risks than conventional models (Boukherouaa et al., 2021). This ability helps lenders make better decisions so that loans could be extended to once underprivileged groups.

Artificial intelligence can also help decision-makers by providing previous data-based recommendations and stressing expected results of specific situations. By use of pattern identification and anomaly detection, artificial intelligence systems—for example—can follow millions of financial transactions and flag problematic behaviour in real-time, therefore enabling human analysts to miss (Bao et al., 2023).

One of artificial intelligence's special qualities is constant learning and adaptive capacity. By means of learning from new datasets, neural networks and other machine learning models enable artificial intelligence systems to progressively raise decision-

making accuracy. AI adjusts to changes in consumer preferences and market situations in applications such as robo-advisors to offer individualised financial advice (Cao, 2021). AI's ability in settings like stock markets or consumer behaviour where conditions often alter depends on this self-learning component.

Finally, in sectors including finance, healthcare and marketing, artificial intelligence's ability for data processing and decision-making has tremendously improved accuracy and efficiency. AI technologies are enabling companies to make more informed and timely decisions by analysing enormous amounts in real-time and always improving via machine learning.

3.3.3 Limitations of AI in Financial Applications

Though artificial intelligence (AI) has transformed the financial industry, certain issues have to be resolved if users are to fully utilise its possibilities. These limitations generally include data quality, control, ethical problems and technology constraints.

Data privacy and security characterise one of the most urgent limits of artificial intelligence in financial applications. Effective operation of artificial intelligence systems depends on a lot of personal financial data. Still, this begs serious questions regarding data leakage and consumer information abuse. The use of artificial intelligence in finance, particularly in areas like credit scoring or automated decision-making, usually includes the processing of personal data, thereby creating possible issues with compliance with privacy regulations including GDPR in Europe and analogous rules elsewhere (Ridzuan et al., 2024). Insecure artificial intelligence systems could permit hackers into financial institutions, therefore endangering not just personal data but also the stability of the financial markets.

The natural inclination in artificial intelligence systems is another restriction with major influence on financial decisions. AI models match the data they have been trained on exactly. Should historical preconceptions—including credit score or loan discrimination—show up in the training data, the AI system would disseminate and maybe intensify these prejudices. Studies on artificial intelligence algorithms used in loan approvals or investment suggestions, for example, have shown that they unfairly punish particular groups—especially underdeveloped places (Boukherouaa et al., 2021). This raises moral issues about fairness and the transparency of financial decisions derived from artificial intelligence.

One of the most regulated sectors is the financial one, hence using artificial intelligence presents fresh difficulties in guaranteeing adherence to these rules. Particularly in sectors like algorithmic trading and automated lending, financial authorities are still debating how best to control artificial intelligence systems. Lack of standardised frameworks for AI governance results in regulatory uncertainty that makes it challenging for institutions to make sure their AI models follow financial rules (Cao, 2021). Still a major challenge is making sure artificial intelligence systems are explainable so authorities may know how judgements are taken.

Many financial organisations still rely on legacy systems, which are frequently incompatible with sophisticated artificial intelligence technologies. Including artificial intelligence into these antiquated systems calls both large technological and financial commitment, which not every institution can afford. Furthermore adding to the complexity and cost of deployment is AI models' need for consistent updates and training to keep correct and relevant (IMF, 2021). Moreover, artificial intelligence systems could find it difficult to understand qualitative financial data, such market mood or geopolitical considerations, so restricting their usefulness in particular situations.

Another question is the probable over-reliance on artificial intelligence, especially in sectors like risk management or automated trading, which begs even more problems. Though it can consume data faster and more precisely than humans, artificial intelligence is not flawless. Lack of human supervision can lead to significant financial risks, particularly in circumstances when artificial intelligence algorithms are rendering significant decisions free from suitable checks and balances. The 2010 Flash Crash raised awareness of this problem when algorithmic trading drastically and severely weakened the market, therefore stressing the need of human supervision in AI-driven financial systems (Ridzuan et al., 2024).

Artificial Intelligence cannot be stressed in terms of data privacy, regulatory compliance, bias and integration challenges even if it has immense potential to transform the financial sector. Dealing with these restrictions will be essential to ensure that artificial intelligence can be properly and successfully used in financial applications.

3.3.4 AI's Impact on Employment in the Financial Industry

Artificial intelligence (AI) integration into the finance industry is fundamentally changing job trends. Particularly in fields involving repetitive work, AI-driven automation has the ability to both destroy current roles and generate new career opportunities.

Routine and manual tasks in finance including data entry, transaction processing and regulatory compliance are being automated using artificial intelligence more and more. Highly effective technologies for customer service, loan approvals and fraud detection are robotic process automation (RPA) and artificial intelligence-based chatbots. Roles including these responsibilities are thus becoming obsolete, which reduces demand for lower-skilled clerical jobs (BCG, 2018) (Bahoo, Cucculelli, Goga, et al., 2024). Although artificial intelligence might replace some occupations, it is also generating new ones requiring specific knowledge. As financial firms try to fully utilise artificial intelligence, positions including data scientists, machine learning engineers and AI ethics officers are much sought for. These positions, which call for knowledge in data analysis, algorithm design and AI governance, centre on the creation, deployment and administration of AI technology (Georgieff & Hyee, 2022). Particularly in occupations needing sophisticated digital skills, professions heavily exposed to AI are seeing rising job growth (Comunale & Manera, 2024). Many financial professionals find that artificial intelligence lets them concentrate more strategically and analytically instead of on menial, repetitious chores. With real-time processing of enormous volumes of data, artificial intelligence systems can provide insights that enable human workers make better decisions. AI can spot trends in investment portfolios, for example, freeing financial analysts to concentrate on more difficult decisions needing human judgement (BCG, 2018). This change results in a re-skilling of the workforce as staff members assume more value-added positions stressing customer interactions, creativity and problem-solving. The consequences of artificial intelligence on employment vary in many fields of finance. In investment banking, for example, AI-powered computers are replacing risk management and trading activity, hence lowering the need for human traders. On the other hand, in fields like wealth management, where trust and personal relationships are vital, artificial intelligence helps human advisers rather than replaces them totally (Bahoo, Cucculelli, Goga, et al., 2024).

Artificial intelligence's overall effect on banking industry employment is complex. Although automation might cause employment losses in some low-skilled and clerical

roles, it also generates new roles and refines attention towards key tasks. Reskilling its staff must thus be given top priority by financial institutions in order to match the changing needs of an AI-driven world.

3.4 THE FUTURE OF AI IN FINTECH

The future of Artificial Intelligence (AI) in financial technology (Fintech) is set to redefine the industry by enhancing efficiency, personalization, and decision-making. As AI continues to evolve, it is expected to drive innovation in areas such as automated risk assessment, fraud detection, and high-frequency trading. With financial institutions increasingly relying on AI-driven analytics, the sector will witness a shift towards more data-driven, real-time decision-making processes. However, alongside these advancements, the growing influence of AI will also bring ethical and regulatory considerations to the forefront, requiring a balanced approach to innovation and compliance.

3.4.1 Predictions for AI's Role in Financial Services

With the technology ready to transform multiple important sectors, artificial intelligence (AI) in the financial services sector looks to be bright. Research and present trends suggest the following main forecasts on the function of artificial intelligence in financial services: As artificial intelligence keeps automating a variety of financial tasks, operational efficiency should rise noticeably. AI systems will be more in charge of routine chores such fraud detection, regulatory compliance and transaction monitoring, hence lowering the need for human involvement. Predictive features of artificial intelligence will also enable financial organisations to automate credit scoring, risk assessment, loan underwriting and credit scoring, hence reducing errors and accelerating operations (IJCRT, 2023) (Deloitte, 2024). Highly customised financial services for consumers will be created by artificial intelligence in big part. By means of data analytics and machine learning, financial institutions will be able to provide customised goods and services depending on particular consumer behaviour and preferences. Already offering tailored investing advice, AI-driven platforms such robo-advisors will spread to other sectors including insurance and wealth management, so improving consumer pleasure and involvement in all spheres (IJCRT, 2023) (Hentzen, Hoffmann, Dolan, & Pala, 2022). Advanced data analysis using artificial intelligence will produce more informed and strategic decisions all over the financial sector. Large datasets in real-time processing and analysis by AI models provide insights that improve market projections, risk management and investment decisions. In a fast-paced, data-driven industry, this will help financial institutions keep ahead. Further

changing the way financial markets function is the predicted increase in the part artificial intelligence plays in algorithmic and high-frequency trading (El Hajj & Hammoud, 2023) (IJCRT, 2023). AI is quite good in controlling risks and preventing fraud since it can find abnormalities and trends in big datasets. AI will keep developing in future in its capacity to identify sophisticated kinds of financial fraud including cyberattacks and identity theft. By offering predictive insights that enable financial organisations to reduce possible risks before they become more severe, it will also improve risk management techniques (Deloitte, 2024) (El Hajj & Hammoud, 2023). As artificial intelligence grows more common in financial services, ethical and legal issues will take front stage. Greater governance structures will be needed for problems including algorithmic bias, openness and data privacy. Regulators are supposed to monitor AI-driven operations more closely to guarantee they follow ethical norms and legal obligations. Financial institutions will have to strike a balance between the benefits of artificial intelligence and the need of responsible and moral use (Bholat & Susskind, 2021) (Deloitte, 2024).

Artificial intelligence is poised to revolutionise financial services by improving efficiency, personalisation, decision-making, risk management and accuracy. To guarantee that the advantages of artificial intelligence be used sensibly, the sector must also handle the ethical and legal issues related to its growing acceptance.

3.5 CONCLUSION

This chapter explored the transformative role of Artificial Intelligence (AI) in financial technology (Fintech), tracing its evolution from foundational concepts to advanced financial applications. It examined AI's integration into key financial services, including fraud detection, risk management, personalized customer interactions, and algorithmic trading, demonstrating its impact on improving efficiency and accuracy. Additionally, the chapter highlighted AI's expanding role in reshaping the financial ecosystem, emphasizing its potential to drive innovation and optimize financial operations. Building on the understanding of AI's role in Fintech, the next chapter, "Chapter 4: Legal Challenges and Issues with Integration of AI in Fintech", will delve into the legal implications of AI integration. It will explore regulatory gaps, jurisdictional challenges, and ethical concerns, particularly focusing on how these impact consumer rights and financial institutions. This chapter will critically analyze how existing laws address the complexities introduced by AI in Fintech and identify key areas requiring regulatory intervention to ensure a sustainable and ethical financial environment.

CHAPTER 4

LEGAL CHALLENGES AND ISSUES WITH INTEGRATION OF AI IN FINTECH

"The real question is, when will we draft an artificial intelligence bill of rights? What will that consist of? And who will get to decide that?"**— Garry Kasparov**

4.1 INTRODUCTION TO LEGAL ISSUES IN AI AND FINTECH

The integration of Artificial Intelligence (AI) into financial systems has introduced significant advancements in efficiency, automation, and predictive analytics. However, alongside these benefits, AI-driven financial systems also present critical legal challenges that require careful consideration. Issues such as algorithmic bias, lack of transparency, data privacy concerns, and regulatory compliance complexities have become central to discussions on responsible AI deployment in Fintech. The opaque nature of AI decision-making, often referred to as the "black box" problem, raises concerns about accountability, while regulatory frameworks struggle to keep pace with rapid technological advancements. Addressing these challenges is crucial to ensuring that AI-driven financial systems operate fairly, transparently, and within the boundaries of legal and ethical principles.

4.1.1 Overview of AI's Growing Role in Financial Services and Legal Framework

Artificial Intelligence is progressively taking front stage in transforming financial services by automating chores, enhancing decision-making and improving client connections. The banking sector is seeing more of AI's influence as companies apply its abilities to boost productivity, save running costs and offer customised services. Artificial Intelligence driven solutions are changing operational processes by automating tasks including transaction processing, fraud detection and compliance monitoring. These systems can handle enormous amounts of data in real time, therefore reducing human participation and the risk of errors. This efficiency helps financial companies to maximise their operations and focus on strategic elements. Artificial intelligence also helps simplify regulatory compliance by way of significant data analysis guaranteeing adherence to legal frameworks, including anti-money laundering (AML) and Know Your Customer (KYC) protocols. (Bholat & Susskind, 2021).

Among artificial intelligence's most important impacts on the banking industry is its capacity to offer customised consumer experiences. By means of individual consumer behaviour analysis, financial history analysis *and* preference analysis, machine learning algorithms generate tailored products and services including bespoke loan offers and investment advice. AI-powered chatbots and virtual assistants have also increased customer involvement by providing real-time, 24/7 service and so improving customer happiness and loyalty. (Deloitte, n.d.) Artificial intelligence enhances risk management by means of pattern and anomaly discovery in financial transactions with predictive analytics. Artificial intelligence systems enable financial institutions detect fraud before it starts by spotting unusual conduct and declining dubious activities for more research. By assessing a larger spectrum of data points and providing more accurate assessments of an individual's creditworthiness, artificial intelligence also enhances credit scoring models (Bholat & Susskind, 2021) (Deloitte, n.d.).

Investment management and trading especially clearly show the impact of artificial intelligence. High-frequency trading systems maximise investing strategies depending on real-time market movements by running transactions in milliseconds using artificial intelligence algorithms to analyse market data. This raises financial markets' liquidity and efficiency, so providing companies a competitive advantage in their trading activities (Ostmann et al., 2021) (Ridzuan, Masri, Anshari, Fitriyani and Syafrudin, 2024).

All things considered, including artificial intelligence into financial services is improving operational efficiency, customer experiences and risk management. The function of artificial intelligence in financial services is projected to expand as it develops, bringing fresh ideas and posing significant ethical and regulatory questions. (Deloitte, n.d.) (Ridzuan, Masri, Anshari, Fitriyani and Syafrudin, 2024). Significant legal and regulatory difficulties are being generated by Artificial Intelligence (AI) fast merging into Financial Technology (Fintech). While providing great advantages in terms of efficiency and innovation, AI's transforming power also brings complexity around data privacy, algorithmic responsibility and the ethics of decision-making. Authorities all around are thus building methods to manage these issues and ensure that artificial intelligence in fintech functions under a clear legal framework. The regulatory sandbox is one of the main tools governments and regulating bodies have embraced to allow artificial intelligence and fintech innovation while safeguarding consumer protection. Originally designed by the Financial Conduct Authority (FCA) of the United Kingdom in 2016, the concept helps fintech companies test new products and services within a controlled environment free from complete regulatory constraints.

This small space ensures consumer safety and market integrity while yet letting creativity flourish. (Range & Ruof, 2020).

From Singapore to Hong Kong and certain EU members, countries all across have embraced this approach. As fintech companies create AI-driven products like risk management systems or robo-advisors, these sandboxes provide fintech companies temporary legal protection. These sandboxes' basic objective is to strike a balance between innovation and required legal control such that new artificial intelligence applications are safe and secure before total market release. (Range & Ruof, 2020) (Agharwal, 2024).

Among the main legal concerns artificial intelligence raises is data security. Large databases with sensitive personal financial data enable artificial intelligence systems in fintech to offer credit scoring, bespoke financial solutions and fraud detection. As such, the use of artificial intelligence in fintech has to abide by strict data security guidelines including EU General Data Protection Regulation (GDPR). The GDPR demands high standards for user permission, data processing and openness on how artificial intelligence systems utilise personal data. (Tallberg, Erman, Furendal, Geith, Klamberg, & Lundgren, 2023) (Omarova, 2020). Furthermore, privacy rules mandate that artificial intelligence systems include tools enabling people to contest decisions rendered by AI. Under the GDPR, for instance, people have the right to learn how their data is being used and to have justifications for automated choices. This guarantees responsibility and openness especially in high-stakes areas like credit rating and loan approvals. (Omarova, 2020)

Legal frameworks for artificial intelligence in fintech also address issues of algorithmic openness and responsibility. The "black box" feature of many artificial intelligence systems—where decision-making processes are opaque—is raising financial regulators increasing concern. Authorities such as the European Banking Authority (EBA) and the U.S. Securities and Exchange Commission (SEC) stress the need of explainability in AI-driven decisions especially in domains like trading algorithms and automated lending. Fintech firms leveraging artificial intelligence must so create interpretable models in addition to being efficient. This implies making sure that AI judgements may be justified in human-understandable terms to legislators, consumers and other stakeholders (Aggarwal, 2024).

Various countries have handled artificial intelligence in fintech using different strategies. With an eye on high-risk uses like credit scoring and investment advising

services, the forthcoming EU AI Act seeks to provide a complete framework for the use of artificial intelligence within the European Union. While federal agencies like the Federal Trade Commission (FTC) are progressively active in supervising AI-related concerns in financial services, AI regulation in the United States is patchier, with different states implementing their own rules (Omanova, 2020) The legal environment controlling artificial intelligence in fintech is still developing. It is evident that regulators are trying to combine encouraging innovation with making sure artificial intelligence runs ethically, transparently and in line with current financial rules.

4.2 LEGAL CHALLENGES IN AI-DRIVEN FINANCIAL SYSTEMS

4.2.1 AI-Powered Fraud: The Rise of Synthetic Identities

The integration of artificial intelligence (AI) into financial technology (fintech) has led to the emergence of sophisticated fraudulent activities, notably the creation of synthetic identities. Fraudsters employ advanced AI techniques to fabricate identities that closely resemble real individuals, complete with convincing backstories and digital footprints. Usually avoiding conventional fraud detection systems, these synthetic identities are subsequently opened bank accounts, applied for credit, and utilised for other financial activities. The American Bankers Association notes that these synthetic identities created by artificial intelligence participate in modest deposit making and credit opening operations, therefore complicating detection attempts (American Bankers Association, 2024). The white paper on synthetic identity fraud mitigating by the Federal Reserve underlines how greatly technology developments—including artificial intelligence and machine learning—have shaped the spread of synthetic identity theft (Federal Reserve, 2024). These technologies allow the development of quite realistic phoney identities, which makes it difficult for banks to tell real from fraudulent clients.

Moreover, the creation of synthetic identities using generative artificial intelligence poses a great difficulty to current fraud detection systems. Researchers on ResearchGate explore how generative artificial intelligence-generated synthetic identities with compelling backstories and digital footprints threaten conventional fraud detection paradigums (Balamurugan & Merlin, 2024). These AI-generated identities' sophistication calls for the financial sector to create increasingly sophisticated detection systems. Financial institutions are investigating the use of sophisticated artificial intelligence systems to improve fraud detection capacity in response to this increasing

risk. Using deep learning and natural language processing, according to a thorough research on changing fintech fraud detection with sophisticated AI algorithms, can result in more solid fraud detection systems able of spotting and stopping fraudulent transactions in real-time (Shoetan & Familoni, 2024). The emergence of synthetic identity fraud driven by artificial intelligence emphasises how constantly innovative fraud detection techniques must be. Financial institutions have to use cutting-edge AI-driven solutions to protect against these changing risks as fraudsters pick more complex AI tools.

4.2.2 Algorithmic Manipulations in High-Frequency Trading

Artificial intelligence (AI) inclusion into high-frequency trading (HFT) has brought opportunities as well as difficulties in financial markets. AI-driven algorithms offer chances for market manipulation even as they improve trade efficiency. Adversarial players can take advantage of weaknesses in these systems, therefore causing possible disturbances of the market. Adversarial assaults on machine learning models applied in HFT, for example, can control trade results, as highlighted by (Goldblum et al., 2020). These assaults cause AI models to produce erroneous predictions by means of minute modifications to input data, therefore enabling financial advantage. Moreover, the opacity of sophisticated artificial intelligence algorithms—often referred to as "black box" models—complicates the identification of such manipulative behaviour, therefore providing major difficulties for market players and authorities (Azzutti et al., 2024). Growing autonomy of artificial intelligence systems in trading calls for strong control measures to guarantee market integrity and stop exploitation.

4.2.3 Deepfake Frauds and Financial Deception

Sophisticated fraud schemes employing deepfake technology expose the banking industry to increased vulnerability. Cybercriminals are employing hyper-realistic synthetic media created with artificial intelligence—deepfakes—to fool financial institutions and their customers. 2019 had a noteworthy incident which attackers used AI-generated audio to pass for a CEO of a corporation, so persuading a subordinate to send $243,000 to a phoney account (FS-ISAC, 2024.). This episode emphasises how much deepfake technology could enable significant financial fraud. Attacks of this kind are becoming more common. According to a Deloitte analysis, 700% increase in deepfake events in the fintech industry in 2023. These attacks usually entail the production of convincing audio or video material that mimics clients or executives, therefore guiding people into approving illegal transactions. The ease with which generative artificial intelligence systems can create high-quality deepfakes has reduced

the obstacle for cybercriminals creating such deepfakes, therefore aggravating the danger landscape (Lalchand, Srinivas, Maggiore, & Henderson, 2024). Deepfake fraud has consequences beyond only instantaneous cash losses. Financial organisations are seriously at danger from them since disinformation campaigns using deepfakes can undermine customer confidence and discredit an institution. Furthermore very visible are regulatory problems; for example, interacting with or hiring people whose identities have been fabricated using deepfakes could cause legal issues and fines (FS-ISAC, 2024). These difficulties call for financial institutions to put strong detection and prevention plans into use. This covers funding technologies equipped to detect synthetic media, improving staff training to spot possible deepfake situations, and creating thorough reaction systems to lessen the effects of such frauds. Protecting against the developing threat of deepfake-enabled financial crimes calls for proactive actions.

4.2.4 Smart Contract Exploits in Blockchain Systems

Particularly with regard to smart contracts, the inclusion of artificial intelligence (AI) into blockchain-based financial systems has brought both fresh security issues and creative ideas. On blockchain systems, smart contracts—self-executing agreements with terms straight entered into code—help to enable automated transactions. But their immutability and complexity make them easy targets, particularly in cases when code flaws exist. In this regard, artificial intelligence-driven analysis has turned into a two-edged blade. One hand, by spotting possible weaknesses, artificial intelligence tools are used to improve smart contract security. AI-powered solutions, for example, may examine code structures to identify typical security weaknesses include arithmetic overflow problems and re-entrancy attacks, which together have resulted in losses above $2 billion since 2020 (AI-Driven Analysis for Smart Contract Security, 2025). By automating the auditing process, these artificial intelligence-driven instruments offer a more thorough and quick evaluation of smart contract security. Conversely, hostile players are using artificial intelligence to take advantage of these precisely weaknesses. Using artificial intelligence algorithms, attackers can methodically find and target flaws in smart contracts, therefore facilitating illegal financial transfers or contract manipulation to benefit them. The research by (Han et al., 2024) highlighted how artificial intelligence can be used to find and exploit composability flaws in decentralised finance (DeFi) systems by means of automated attack synthesis for constant product market makers (Han, Kim, Lee, & Yun, 2024). Blockchain transactions' immutable character increases the effect of such vulnerabilities since once a transaction is carried out it cannot be readily undone. This feature emphasises the great need of careful smart contract audits and the application of strong security

mechanisms before deployment. Moreover, the distributed and sometimes anonymous surroundings of blockchain systems poses great difficulties in assigning blame and tracking attackers. These difficulties call for the creation of sophisticated AI-powered security solutions right now. By use of pattern and behaviour analysis inside the blockchain ecosystem, such solutions should not only concentrate on identifying current vulnerabilities but also forecast possible attack routes. Staying ahead of hostile players who are progressively clever in their approaches also depends on encouraging cooperation between artificial intelligence researchers, blockchain builders, and cybersecurity specialists. AI creates new opportunities for exploitation even while it provides strong tools to improve the security of smart contracts in blockchain-based financial systems. To protect these systems against changing threats, a balanced approach combining proactive defence using artificial intelligence with strict security measures and teamwork is absolutely vital.

4.2.5 AI-Enhanced Phishing Attacks

Sophisticated phishing assaults driven mostly by artificial intelligence (AI) are exploding in the financial industry. Cybercriminals are using artificial intelligence to create highly tailored and convincing phishing emails, therefore making it difficult for people and businesses to separate real from fake communications. The report for annual number of cyber-attacks worldwide basically indicates the number of frauds that happens and what are the types that is happening such as Phishing Scams, Identity Theft, Personal Data Breach, etc. Among these Phishing scams are more prevalent and with the rising technology, the attacks become easier in use of these technologies. Below is the chart that represents this data from 2016-2023.

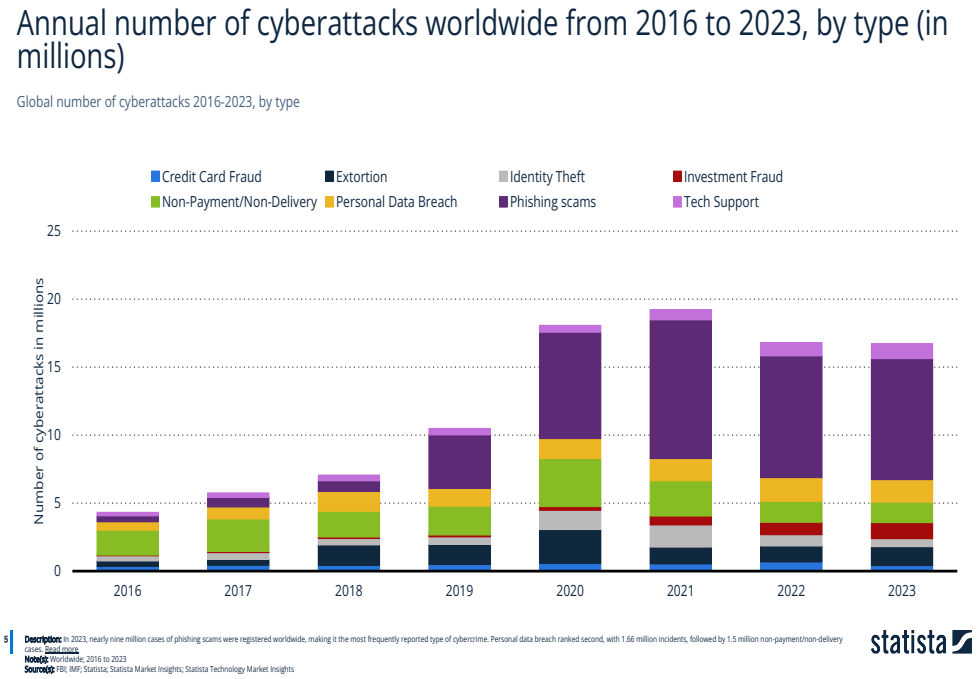

Figure 4.1: Number of Cyber Attacks from 2016-2023
Source: Statista

Generative artificial intelligence techniques let attackers examine enormous volumes of data—including public records and social media data—to create messages that quite nearly reflect actual correspondence. This personalising raises the possibility of recipients interacting with harmful content, therefore compromising sensitive data (Internet Crime Complaint Centre [IC3], 2024). A significant concern is the use of AI to overcome language barriers and cultural nuances, allowing cybercriminals to target a global audience with minimal effort. AI-generated phishing emails exhibit fewer grammatical errors and are contextually relevant, reducing traditional red flags that users rely on to identify scams. This evolution in phishing tactics has led to a notable increase in successful breaches within the financial industry. (Sharon, 2024)

The implications of AI-enhanced phishing are profound. Financial institutions face not only immediate financial losses but also long-term reputational damage. As these attacks become more sophisticated, there is an urgent need for advanced detection and prevention mechanisms. Traditional security measures are often inadequate against AI-driven threats, necessitating the adoption of AI-based defensive strategies. Implementing machine learning algorithms that can detect anomalies in communication patterns, enhancing employee training programs to recognize subtle phishing attempts, and fostering information sharing among institutions are critical steps in mitigating this growing threat (JDSupra, 2025)

The rise of AI-enhanced phishing attacks presents a significant challenge to the financial sector. Maintaining confidence in financial institutions and safeguarding private financial data depend on proactive actions including the integration of artificial intelligence in cybersecurity systems and ongoing education on developing risks.

4.2.6 Sentiment Manipulation Using AI Tools

Especially for sentiment analysis, artificial intelligence (AI) has fundamentally changed financial markets. By processing enormous volumes of textual data from news stories, social media, and financial reports, artificial intelligence systems can evaluate market sentiment and hence affect trading methods. This capacity enables quick responses to market news, thereby maybe increasing volatility (IMF, 2024). Still, the same sentiment-analysis AI techniques can be used to skew market impressions. Through automated systems, malicious actors can spread misleading or incorrect information, therefore manipulating asset values either artificially increasing or decreasing. Existing regulatory systems may not be able to identify or stop such advanced strategies (Sidley, 2024), hence this type of market manipulation presents major difficulties to them.

Moreover, the opacity of modern artificial intelligence systems makes it more difficult to find market misuse. These models' "black box" makes it challenging for authorities to grasp the decision-making processes behind trading operations, therefore impeding the discovery of manipulative actions. (Azzutti, Ringe, & Stiehl, 2024). Although sentiment analysis driven by artificial intelligence provides insightful information for market players, it also creates fresh channels of market manipulation. Dealing with these issues calls both strong legal systems and cutting-edge monitoring techniques equipped to identify and minimise market abuses driven by artificial intelligence.

4.2.7 IoT-Driven Cybercrimes in Fintech

Significant cybersecurity problems have been brought about by incorporating Internet of Things (IoT) devices into financial technology (fintech) systems. they IoT devices are vulnerable to assaults since they lack appropriate encryption and authentication systems. This weakness puts financial organisations open to possible data leaks and illegal access (Shaikh, 2024).

One such example is the Mirai botnet assault of 2018, in which attackers launched a distributed denial-of- service (DDoS) attack using compromised IoT devices, therefore upsetting internet services all throughout the eastern United States. Such events draw

attention to the possibility for IoT-driven cybercrimes to affect financial services, particularly in cases when these devices are linked inside fintech systems (High, 2020).

If financial organisations wish to lower these risks, they have to create robust security rules comprising regular software updates, strong encryption methods, and continuous IoT device monitoring. Moreover, applying AI-powered security solutions can enable better identification and prevention of illicit activities, thereby enhancing the general cybersecurity posture of fintech businesses (Sharma, 2024).

4.2.8 The "Black Box" Problem in AI Decision-Making

The "black box" problem of artificial intelligence (AI) is the difficulty of knowing how AI systems—especially advanced machine learning models like deep learning—particularly arrive at certain decisions. This lack of openness and explainability creates serious issues, particularly in industries like financial services where ethical and legal responsibilities call for clear, responsible decision-making procedures. In financial services for credit scoring, fraud detection, or automated investment decisions, artificial intelligence models are quite opaque. These models apply techniques even engineers find difficult to understand in order to manage enormous volumes of data. Mathematical calculations hide the decision-making process, producing what is sometimes known as the "black box" effect. This poses a significant challenge to guaranteeing responsibility since it is difficult to justify why the AI system made particular decisions—such as credit limit adjustment or loan denial—especially Jakubiec, Furman, et al., 2024) (2020 Wischmeyer). Many countries have laws requiring a degree of openness and explainability in decision-making, especially in regard to delicate topics like personal money. For example, the General Data Protection Regulation (GDPR) of the EU gives people the right to an explanation for automatically made decisions having a major impact on them. But the complicated character of artificial intelligence models sometimes runs counter to these legal obligations since the nuances of machine learning systems are not readily expressed in common language (Wischmeyer, 2020). (von Eschenbach, 2021). Artificial intelligence-using financial institutions struggle to satisfy legal requirements. In credit scoring, for instance, someone can ask why their application was turned down. Giving a meaningful explanation, however, calls for an awareness of how the model's variables interacted to generate the conclusion rather than merely referencing them. Given the black box character of artificial intelligence, such openness is challenging (von Eschenbach, 2021). Researchers and regulatory authorities are pushing Explainable AI (XAI) development to solve the black box issue. XAI aims to produce interpretable models in addition to ones that are accurate Proposed

to be transparent AI models are techniques like decision trees, rule-based systems, or post-hoc explanation methods such Local Interpretable Model-agnostic Explanations (LIME). These initiatives seek to close the legal demand for explainability's gap with the natural complexity of AI systems (Brożek, Furman, Jakubiec, et al., 2024). In essence, even if artificial intelligence has revolutionary possibilities in financial services, its transparency raises ethical and legal issues. Developing AI systems that are both accurate and interpretable would help one to comply with regulatory frameworks and guarantee consumer trust by means of open decision-making procedures that correspond with legal criteria. Particularly with regard to the "black box" character of many artificial intelligence (AI) models, the integration of AI into financial decision-making procedures presents major difficulties. This term describes the difficulty for stakeholders to understand and trust these results since the opacity in knowledge about how artificial intelligence systems reach particular conclusions. Within the financial industry, this lack of openness can cause problems with ethical considerations, regulatory compliance, and responsibility (Yurcan, 2022). The difficulty in articulating AI-driven decisions—such as credit score or loan approvals—makes one of the main worries The complicated algorithms involved in financial institutions sometimes make it difficult for them to offer convincing reasons for their choices. This opacity not only erodes consumer confidence but also presents difficulties for regulatory compliance as institutions have to guarantee that their procedures of decision-making are equitable and non-discriminatory (Mastercard, n.d). Furthermore, the black box challenge makes it more difficult to find prejudices in artificial intelligence systems. It becomes difficult to spot and minimise such prejudices that can result in unjust results without a comprehensive knowledge of how decisions are taken. In financial services, where biassed judgements can significantly affect people's financial situation, this is especially alarming (Bathaee, 2018). The banking sector is looking at explainable artificial intelligence (XAI) models to help with these difficulties. XAI seeks to make AI decision-making processes more open so that interested parties may know the elements affecting certain results. XAI can assist consumers develop trust by improving interpretability and guarantee that financial services driven by artificial intelligence run inside ethical and legal guidelines (Venkatraman, 2024). Although the artificial intelligence presents great advantages for financial decision-making, solving the black box issue is absolutely important. Using explainable artificial intelligence models helps to improve justice, openness, and responsibility, thereby building more confidence in financial services driven by artificial intelligence.

4.2.9 Algorithmic Bias and Fairness in AI-Driven Financial Decisions

Especially in areas like credit scoring, loan approvals, and fraud detection, artificial intelligence systems in financial services are prone to errors and prejudices that could provide unfair or discriminating outcomes. Ensuring that AI-driven financial systems operate fairly and openly depends on control of these biases and mistakes.

In artificial intelligence, bias can come from several causes including faulty algorithms, biased training data, or human misjudgement during design. An artificial intelligence model educated on past data involving biased choices against a given demographic group, for example, might thereby spread that bias. In industries like credit scoring or hiring, where biased decisions can have significant social consequences, this is particularly concerning (Ferrara, 2024) (Balayn, Lofi, & Houben, 2021).

Below is the chart that represents the AI issues companies are not addressing worldwide and not reducing unintended bias has more % among all.

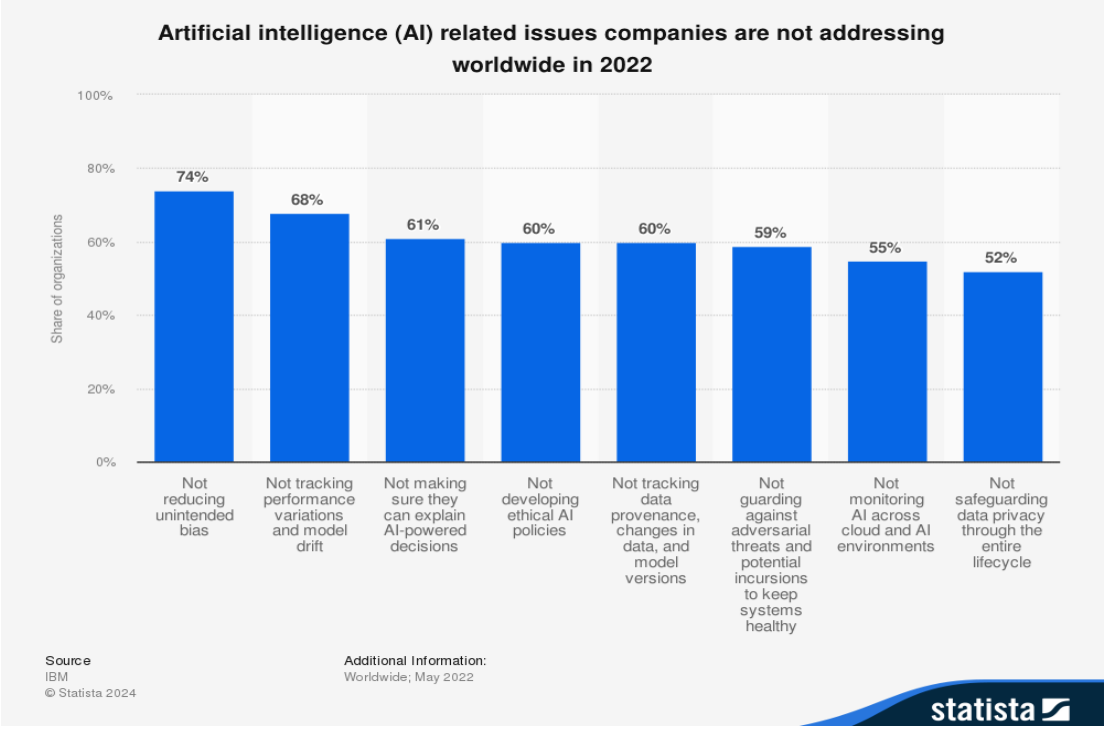

Figure 4.2: AI Related Issues Worldwide

Source: Statista

One of the key strategies is raising the quality and objectivity of data before it enters artificial intelligence algorithms. This means ensuring that various and representative datasets are applied and removing or lowering biased data. The system can be less prone to discriminate depending on sensitive factors like ethnicity, gender, or socioeconomic

level by balancing datasets among several demographic groups. (McKinsey & Company, 2019).

AI models can also have post-processing methods used to fix any unjust outputs. For instance, counterfactual fairness guarantees that, even if sensitive factors like race were changed, the conclusion of the system stays the same. This guarantees that groups under protection are not being unfairly singled out (McKinsey & Company, 2019). Managing mistakes in artificial intelligence systems depends on addressing the "black box" challenge. By means of transparent AI models and understandable decision-making processes, one can help in the identification of sources of bias or mistakes. Explainable AI (XAI) solutions help developers and authorities to see unjust results by letting them know how an artificial intelligence system got at a given conclusion (McKinsey & Company, 2019) (Abrams, 2024). Regular audits and monitoring of AI systems should help to find flaws and prejudices even after they are implemented. Before and throughout the implementation of artificial intelligence systems, financial institutions can conduct fairness effect studies to guarantee they run in line with justice requirements. Through constant reviews, organisations can stop any unjust decisions from being carried on over time (Balayn, Lofi, & Houben, 2021). Human supervision is still absolutely vital even if artificial intelligence can automate and improve decision-making. Particularly when those judgements impact disadvantaged groups, humans have to be involved in examining and intervening in choices that artificial intelligence systems make. Regulatory authorities are stressing more and more the requirement of a human-in---the-loop strategy to guarantee responsible and ethical behaviour of artificial intelligence systems (McKinsey & Company, 2019). Particularly in credit scoring, the inclusion of artificial intelligence (AI) into financial decision-making has resulted in major advantages including efficiency and the capacity to handle big data. AI systems do, however, also seriously question fairness, prejudice and algorithmic bias. Especially in sensitive fields like loan approvals and credit assessments, these prejudices can reinforce and even aggravate already existing social imbalances. Often resulting from biased datasets and poor model development, algorithmic bias in artificial intelligence systems is usually educated on historical data, AI models will probably repeat and propagate prior discriminatory acts if this data indicates such patterns. Credit scoring systems, for instance, may employ information reflecting discriminatory lending habits that deny access to credit to some racial or socioeconomic groups. This leads to unjust loan decisions depending on region, gender, or ethnicity, therefore aggravating financial inequalities (Bono, Croxson, & Giles, 2021) (Garcia, Garcia, & Rigobon, 2024). Furthermore, prejudices might surface throughout data collecting and processing

as well as during other phases of artificial intelligence development. AI systems can generate erroneous or unjust results in situations when data is under-represented of some demographic groups or skewed. If their data is misrepresented or under-represented in the datasets used to train AI systems, for example, minority groups may be more likely to be excluded from credit markets (Bajracharya, Khakurel, Harvey, & Rawat, 2023).

Discrimination in credit rating might show up in several ways. “Third-degree price discrimination,” in which varying loan conditions are provided depending on group factors like ethnicity, age, or socioeconomic level, is possible for artificial intelligence systems. While some pricing discrimination tactics are lawful and well-liked (e.g., elder discounts), in many countries employing race or locality to set credit terms is deemed discriminatory and illegal (Garcia, Garcia, & Rigobon, 2024). Unchecked, artificial intelligence algorithms can amplify such prejudices by methodically excluding minority groups from judgements based on biased past data. Many machine learning models’ “black box” character makes ensuring fairness in AI-driven financial choices difficult. Many times lacking transparency, these models make it challenging for financial institutions and authorities to completely grasp or justify the process of decision-making. Because stakeholders could not know how or why a given choice was taken, this opacity hinders attempts to find and fix biases (Bono, Croxson, & Giles, 2021). Furthermore, difficult is balancing algorithmic accuracy with fairness; attempts to eliminate bias from AI models often result in worse predicted accuracy. Regulators and financial organisations have to use a multifarious strategy to solve these problems. leveraging justice-aware algorithms that actively reduce prejudice during the decision-making process, routinely auditing AI systems and leveraging transparency tools to make AI-driven choices more understandable (Bajracharya, Khakurel, Harvey, & Rawat, 2023) Furthermore, including varied and representative datasets helps to reduce bias so that AI models take into account a wider spectrum of events and actions while deciding creditworthiness. Basically, even if artificial intelligence delivers more efficient and data-driven solutions that could totally change financial services, it raises serious questions about justice and prejudice. Dealing with these problems requires continual efforts by authorities and business players to ensure that artificial intelligence systems work fairly and ethically. Since they require vast amounts of personal and financial data to run at their optimum, artificial intelligence systems in financial services create problems with the handling of both. Inappropriately regulated artificial intelligence systems run the risk of revealing private information to unethical profiling,

leaks, or use. Many times, data is gathered, handled and distributed over multiple platforms, raising unauthorised access or data breaches risk.

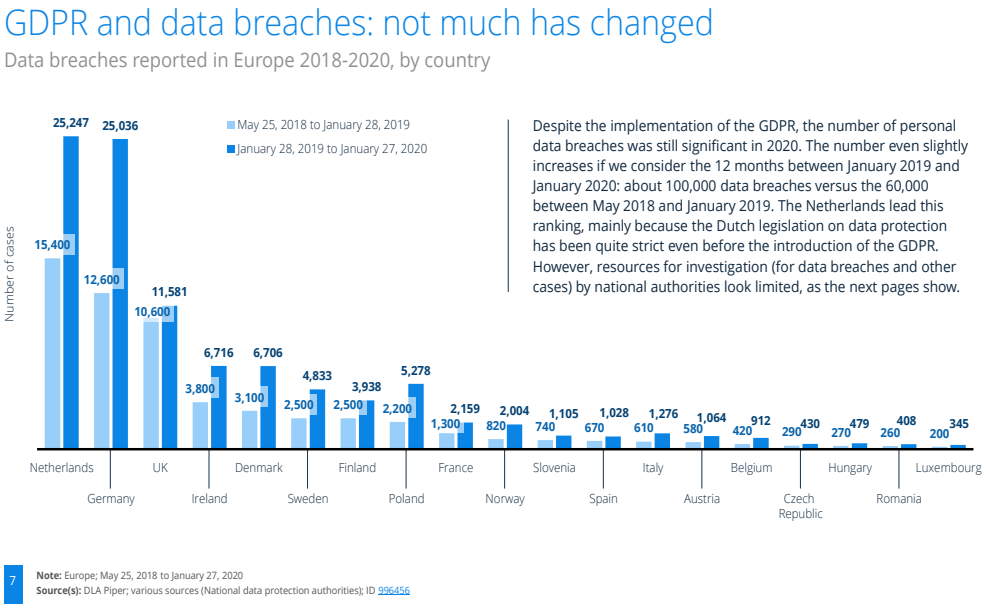

Figure 4.3: Data Breaches reported from 2018-2020
Source: Statista

One of the main challenges is keeping data security throughout operations powered by artificial intelligence. Implementing strict data governance policies encompassing anonymisation, encryption and regular security assessments to safeguard personal data means that financial organisations have to obey GDPR. Using artificial intelligence also means implementing these principles while balancing the demand for perfect user experiences and great computational performance. (Peck Pinheiro & Batista Battaglini, 2022).

4.3 REGULATORY CHALLENGES IN AI-FINTECH INTEGRATION

As Artificial Intelligence (AI) continues to transform financial technology (Fintech), regulatory challenges have emerged as a crucial area of concern. AI-driven financial systems must navigate complex legal landscapes, including compliance with existing laws, cross-border regulatory conflicts, and liability concerns in automated decision-making. The rapid evolution of AI outpaces traditional regulatory frameworks, raising questions about algorithmic accountability, data security, and transparency. Addressing

these challenges requires a dynamic regulatory approach that balances innovation with legal safeguards, ensuring that AI operates within ethical and lawful boundaries while fostering financial stability and consumer trust.

4.3.1 Compliance with Existing Laws: AI Disruption of Current Financial Regulations such as AML and KYC Protocols

Particularly in areas like Anti-Money Laundering (AML) and Know Your Customer (KYC) procedures, the incorporation of Artificial Intelligence (AI) into financial systems has revolutionised how institutions follow standards. Artificial intelligence calls into doubt the present legal systems built for human operations even if it provides until unheard-of accuracy and efficiency.

Artificial intelligence dramatically increases the effectiveness of AML compliance by automating the detecting and reporting of questionable activities. Conventional AML systems rely on human discretion and predefined rules that could lead to errors and delays. Particularly Artificial Intelligence (AI) enabled by Machine Learning (ML) permits real-time transaction monitoring and anomaly and unusual pattern recognition that might indicate money laundering. For example, AI-driven systems can employ behavioural analytics to create consumer profiles and handle enormous volumes of transactional data, therefore enabling more precisely identification of questionable activities. By allowing financial institutions to follow AML rules as those established by the Financial Action Task Force (FATF), this automation helps to improve detection rates and lower false positives. (Pavlidis, 2023). But artificial intelligence's automation in AML raises legal questions as well, especially with relation to decision-making's openness and possible bias. AI algorithms might not always offer clear explanations for declining transactions as suspicious, which runs against regulatory requirements for openness in many nations (Pavlidis, 2023) (Financial Crime Agency, 2024).

Historically labour-intensive and time-consuming, Know Your Customer (KYC) procedures involve hand document and customer identity verification. By bringing automation that greatly accelerates the client onboarding process, artificial intelligence disturbs this. Real-time identity verification made feasible by technologies such biometric verification, optical character recognition (OCR) and facial identification helps to lower human error and delays (Lucinity, 2024). Through "perpetual KYC," which lets customer profiles be real-time updated depending on continuous

transactions, artificial intelligence also enables constant KYC. This dynamic monitoring guarantees that institutions remain current on the risk profiles of their clients and helps them to comply with changing KYC rules.

Nonetheless, artificial intelligence in KYC has to go by data privacy rules such as the General Data Protection Regulation (GDPR), which upholds openness and grants people their right to know how their data is handled. The difficulty for financial institutions is juggling the speed and efficiency of artificial intelligence with these regulatory constraints such that AI systems do not violate privacy or fail to offer clear explanations for automated choices (American Bankers Association, 2024). (Economic Crime Academy, 2024)

By providing real-time monitoring, enhancing accuracy and lowering of manual labour, artificial intelligence (AI) has the ability to transform compliance with AML and KYC rules. Financial institutions must so carefully negotiate the legal problems presented by the opacity of artificial intelligence and make sure these systems follow current data protection and openness rules.

4.3.2 Governing AI in Cross-Border Financial Transactions: Addressing Jurisdictional Issues

Different national regulatory regimes in Artificial Intelligence (AI) applied in cross-border financial transactions generate significant jurisdictional challenges. Financial institutions depend more and more on artificial intelligence systems for duties including fraud detection, real-time risk analysis, client validation—all of which involve the transfer of huge amounts of personal and financial data across borders. Particularly in data security and compliance, the jurisdictional complexity results from these interactions among several nations with various legal responsibilities.

Following data security policies that vary greatly among countries is one of the primary difficulties in cross-border artificial intelligence-driven financial transactions. For instance, the European Union's General Data Protection Regulation (GDPR) establishes rigorous rules on the handling and dissemination of personal data even outside of its borders. Artificial intelligence-using financial companies have to ensure sure any data crossing borders complies with GDPR regulations, including ensuring suitable data protection and obtaining unambiguous permission from individuals when handling their data outside the EU. (Generis Global, 2024).

Other countries, including the United States, have their own data protection rules, such the California Consumer Privacy Act (CCPA), which presents still another challenge for foreign banks. Artificial intelligence systems negotiating contradictory legal regulations across many countries find challenges from this variety of legal rules. (Generis Globally, 2024) (Cross-Border Data Forum, 2024).

Some countries, including China and Russia, have embraced data localisation policies, which demand data to be retained inside national borders. For financial companies using artificial intelligence, this is a challenge since these systems usually run successfully depending on centralised data processing. Maintaining the operational benefits of artificial intelligence across borders while ensuring compliance with such localisation standards is difficult. Financial companies could have to construct duplicate data infrastructures or localised artificial intelligence models, which can be costly and challenging. (Generis Global, 2024) (Cross-Border Data Forum, 2024).

Still another challenge is the fragmentation of rules on artificial intelligence's legal obligation. Regarding artificial intelligence liability, national laws vary. Some sectors lack a clear legal framework defining how artificial intelligence-driven decisions in financial transactions should be handled in cases of disagreements or blunders. This lack of legislative harmonisation increases the legal risks associated with artificial intelligence since financial firms can be sued in numerous nations with various liability policies. Laws enforced differently between countries make it challenging for financial institutions to use standard artificial intelligence systems across borders. (Generis Global 2024; Cross-Border Data Forum 2024)

Several strategies allow financial organisations to negotiate the jurisdictional complexity:
To ensure local regulatory compliance, institutions should learn about the locations of data storage and handling.

- Cross-border agreements: Data transfers agreements—mostly those approved by the EU for non-EU countries—can help to enable legal data flows.
- Institutions could have to employ localised versions of their AI systems to avoid non-compliance in locations with stringent localisation laws. (Generis Global, 2024) (Cross-Border Data Forum, 2024)

AI-driven financial systems encounter significant jurisdictional challenges when operating across borders due of varied rules on data protection, localisation and legal

liability. Using the benefits of artificial intelligence in global financial markets, institutions must assure compliance using tailored and flexible strategies.

4.3.3 Liability and Accountability in AI Decision-Making: Legal Dilemmas in Financial Systems

Growing Artificial Intelligence (AI) presence in financial systems raises important legal questions of responsibility and accountability. Whether direct human involvement is present or not, AI-driven decisions—whether in loan approvals, investing strategies, or fraud detection—often make it difficult to assign culpability when these decisions lead mistakes or losses. This creates an interesting conundrum inside the financial institutions' legal structure.

1. Autonomy vs. Human Oversight

One of main difficulties is the degree of autonomy artificial intelligence systems hold in processes of decision-making. Usually the financial institution or human operators bear liability; but, it becomes more challenging to allocate when an artificial intelligence system renders autonomous decisions resulting in financial loss. This is especially challenging in cases when artificial intelligence chooses autonomous behaviour against social conventions. Financial institutions have responsibilities for ensuring that decisions driven by artificial intelligence obey current rules and standards even though their efficiency depends on artificial intelligence. (Giuffrida, 2019)

2. The "Black Box" Problem

Further complicating responsibility is the "black box" problem of artificial intelligence's opaque decision-making process. Especially machine learning models, artificial intelligence systems base decisions on complex data patterns often difficult for humans to grasp. This opacity causes legal issues since financial companies find it challenging to support the decision an artificial intelligence system made. Customers affected by these decisions, including those denied a loan, could find it challenging to contest AI-based conclusions without knowing exactly the decision-making process involved. Giuffrida, 2019 (Perdana, Wang and Arifin, 2024)

3. Legal Frameworks and Liability Models

Not yet fit to manage the complexity of AI-driven decisions are current legal systems. One potential solution is the adoption of strict liability models, in which financial

companies are totally responsible for the activities of their artificial intelligence systems independent of their intention or understanding of the decision-making process. While this would simplify assigning responsibility, it might also give financial institutions great legal weight (Giuffrida, 2019). Another approach is shared liability, in which case the creators of artificial intelligence technology and the financial institutions share responsibility for any losses or errors caused by AI decisions.

As artificial intelligence gets more firmly rooted into financial institutions, clearer legal frameworks around liability and duty becomes very vital. Artificial intelligence solutions must be dependable, transparent and legal complying for financial companies as well. At the same time, authorities have to draft laws that especially address the unique challenges posed by artificial intelligence so that responsibility for decisions taken under its impact is exactly defined.

4.4 INTELLECTUAL PROPERTY (IP) CONCERNS WITH AI IN FINTECH

The integration of Artificial Intelligence (AI) into financial technology (Fintech) has raised complex intellectual property (IP) concerns, particularly regarding ownership and patentability of AI-generated innovations. Traditional IP frameworks were designed to protect human creativity, leaving legal ambiguities about whether AI-generated content and algorithms can be copyrighted or patented. Courts and regulatory bodies worldwide are grappling with defining ownership rights and determining whether AI can be considered an inventor. As AI continues to autonomously generate financial models, trading strategies, and risk assessment tools, the need for updated legal frameworks to address these challenges becomes increasingly urgent.

4.4.1 Ownership of AI-Generated Content: Intellectual Property Issues

Particularly in the financial technology (fintech) sector, the use of artificial intelligence (AI) in content production begs challenging intellectual property (IP) ownership legal questions. Based on the idea of human creativity, traditional IP rules do not readily allow decisions or content produced by artificial intelligence. This leaves questions about who has rights to AI-generated models, content and choices. Most governments extend copyright protection solely to works produced by humans. The U.S. Copyright Act mandates that authorship underlines natural beings. In many nations, the Berne Convention—which controls copyright law—also states that copyright is reserved for human creators who actively participate in their works. Determining who owns the copyright becomes difficult, nevertheless, when an artificial intelligence generates content—such as in credit risk modelling or automated financial analysis. Should it be

the user entering data, the entity owning the AI, or the person building it? This uncertainty complicates IP protection in finance and other industries where artificial intelligence systems produce valuable outputs free from direct human interaction. (Gaffar & Albarashdi, 2024)

Ownership in artificial intelligence-generated information has been under scrutiny in a few recent judicial rulings. For instance, the U.S. courts ruling on the Naruto v. Slater case concluded that copyrights cannot be owned by animals, hence by extension by non-human entities like artificial intelligence. The U.S. Patent Office also denied a patent application for inventions created by an artificial intelligence system, therefore verifying that only human creators are covered by U.S. law (Gaffar & Albarashdi, 2024). These choices highlight the tension existing between present legal frameworks and the growing ability of artificial intelligence to produce content on its own.

Some academics suggest building a fresh legal structure especially for material produced by artificial intelligence. Introducing a sui generis system of rights for AI-generated works could be one possible solution, therefore giving ownership to the entity who owns or manages the AI instead of the AI itself. Others propose that the individual who supplies the creative ideas or guidelines for the output of the AI system could be responsible for ownership rights (Gaffar & Albarashdi, 2024).

All things considered, modern IP systems are not quite able to handle the issues raised by finance material created by artificial intelligence. As artificial intelligence keeps generating significant outputs autonomously to manage responsibility and ownership concerns, updated legal frameworks are becoming more and more essential.

4.4.2 Patent Law and AI Algorithms: Legal Implications for Patenting AI Innovations in Fintech

Especially with regard to the patentability of AI-generated concepts, the rising use of artificial intelligence in fintech raises serious legal questions. While patent law has always been meant to protect human-created ideas, AI's ability to independently generate models, algorithms and approaches calls into doubt this paradigm.

Particularly in fintech, AI-driven solutions can feature algorithms and machine learning models processing vast datasets. Because they lack a technical character, algorithms and mathematical techniques are often not regarded as patentable under existing patent law. For example, the European Patent Office (EPO) does not grant patents for abstract computational models or processes unless they are used in a practical, technical manner,

like in a particular industrial process or equipment (Aguilar, 2023). For fintech businesses trying to patent unique AI algorithms applied for credit scoring, automated trading, or risk management, this restriction presents difficulties. Furthermore, AI innovations have to satisfy the complete disclosure criteria for patents, so an invention has to be sufficiently detailed for someone working in the field to copy it. But the intricacy of AI models—especially deep learning networks—makes it challenging to meet this need since these models typically develop autonomously and are not easily understandable even by their designers (Brookings, 2022). Deciding who qualifies as the "inventor" of an AI-generated invention is among the most divisive questions in artificial intelligence. Under present patent rules in the United States, the United Kingdom and the EU, only humans can be named inventors. High-profile decisions as Thaler v. Vidal, where the U.S. courts decided that artificial intelligence cannot be credited as an inventor even if it independently produced the innovation, underline this again (Brookings, 2022). These decisions beg problems regarding the status of innovations produced totally by artificial intelligence systems without direct human participation. For financial companies dependent on artificial intelligence to create fresh algorithms or solutions, this creates a major conundrum. Should the programmer of AI-generated innovations credit the AI, its user, or the company owning the AI system? These unresolved issues hamper the patenting process for fintech companies and emphasise the need of revised legal frameworks able to fit AI's increasing importance in innovation (Merritt, 2023).

Regarding the issue of artificial intelligence patentability, different countries are doing things differently. While the U.S., EU and U.K. patent office's demand human inventiveness, nations like South Africa have let artificial intelligence be recognised as an inventor in a limited context. For fintech companies with worldwide operations, these different criteria cause uncertainty since the patentability of AI-generated inventions could vary depending on the jurisdiction (Brookings, 2022).

It is complicated and several legal ramifications are discovered for patenting AI in fintech. Although present patent rules are not suited to address the special difficulties presented by artificial intelligence, continuous legal discussions and court decisions will probably help to define intellectual property rights in this field.

4.5 CONTRACTUAL ISSUES AND AI-ENABLED FINANCIAL AGREEMENTS

The rise of Artificial Intelligence (AI) and blockchain technology has significantly altered the landscape of financial agreements, introducing new challenges in legal enforceability, consent, and regulatory compliance. Smart contracts, powered by blockchain, offer automation and efficiency but pose jurisdictional complexities and difficulties in interpretation. Similarly, AI-driven financial agreements raise concerns regarding consent and accountability, as decisions may be made without direct human intervention. As these technologies continue to reshape financial transactions, ensuring legal clarity, adaptability, and robust dispute resolution mechanisms will be essential for their widespread and secure adoption.

4.5.1 Smart Contracts and Legal Enforceability: Legal Issues Around Blockchain-Based Smart Contracts

Operating on blockchain technology, smart contracts have changed the way financial agreements are generated and carried out. These agreements are self-executing, with the agreement terms expressed straight into code. Although smart contracts have many benefits—such as transparency and automation—their legal enforceability creates various difficulties because of variations in how governments view and control them.

In some countries, including the U.S., U.K. and portions of the European Union, where legislative measures have been taken to offer legal certainty, smart contracts are commonly acknowledged. States such as Arizona and Nevada in the United States have changed their electronic transaction rules, for instance, to specifically acknowledge smart contracts as legally binding. Likewise in England and Wales, the UK Jurisdiction Taskforce has confirmed that under common law smart contracts can have the same legal standing as regular contracts (Levi & Lipton, 2018) (Ma, 2023)

Many countries, meanwhile, lack clear legal foundations for smart contracts, which creates confusion. Like those in Europe, some civil law nations may rely on whether the agreement satisfies conventional criteria for contract formation, such consent, consideration and legal capacity, therefore determining the enforceability of smart contracts. Furthermore, the immutability of blockchain can affect matters like contract amendment since smart contracts now find it difficult to fit flexible contractual terms that traditional legal systems usually depend on being renegotiated (Ma, 2023)

Smart contracts are fundamentally problematic for non-technical parties or judges to understand as they are written in code. Courts can interpret vague terms in conventional contracts; in smart contracts, the code runs automatically without opportunity for

interpretation. This could cause conflicts, particularly in cases of a programming error or unanticipated events influencing the performance of the contract (Levi & Lipton, 2018) (Herian, 2019)

Moreover, smart contract dispute resolution systems still need work. In circumstances of cross-border transactions, problems may develop over whose legal system or jurisdiction applies since these contracts sometimes lack built-in clauses for how conflicts should be resolved. This is especially difficult when the relevant parties come from nations with different laws and recognition of smart contracts (Herian, 2019)

Particularly in cross-border transactions, the worldwide character of blockchain makes it difficult to ascertain which laws apply to smart contracts. While some nations lag behind or have conflicting laws, others—including the United States, the United Kingdom and the EU—are making progress in legal recognition. Businesses implementing smart contracts in international transactions where the legality and execution of agreements may be questioned in courts unfamiliar with or hostile of blockchain technology find difficulties due to the lack of worldwide uniformity (Levi & Lipton, 2018) (Herian, 2019)

In essence, smart contracts provide security and efficiency; their legal enforceability varies greatly depending on the jurisdiction and reflects major differences in recognition, interpretation and dispute resolution systems. Legal systems will have to change as blockchain technology develops to make sure smart contracts may be efficiently included into current legal systems.

4.5.2 Automated Financial Agreements: Challenges Related to AI Execution, Consent and Enforceability

Using artificial intelligence to automate financial agreements poses serious legal questions, especially with regard to consent and enforceability. Legal systems have to deal with how to guarantee the legitimacy of agreements created without direct human supervision as artificial intelligence systems progressively occupy positions in drafting, negotiating and implementing contracts.

Consent is a big legal difficulty in computerised financial agreements. According to conventional contract law, parties should freely enter into agreements knowing exactly the terms. But often without explicit human engagement at the point of execution, AI-driven systems run agreements based on pre-programmed rules and inputs. This begs issues about whether the parties really agreed to the parameters of the agreement,

particularly if the artificial intelligence changes them depending on unanticipated events or learns from past transactions to make independent decisions. Since the legal definition of consent presupposes human interaction, courts could find it difficult to ascertain if consent was provided in such circumstances with validity.

Under the General Data Protection Regulation (GDPR), for instance, Article 22 guarantees people their right not to be subjected to choices based simply on automated processing, therefore greatly affecting them unless they have given express agreement. When artificial intelligence independently implements financial agreements without human supervision, this need generates a legal dispute and begs issues of whether valid permission has been acquired in the lack of human decision-making. (Foley & Lardner LLP, 2023)

Jurisdictions' enforceability of AI-driven financial agreements differs. Legal acceptance of contracts carried out by artificial intelligence systems is still developing in many nations, which results in variations in enforcement criteria. While some governments are more welcoming of artificial intelligence's involvement in contract creation and execution, others could want human supervision in both areas. For example, certain states—including Arizona and Nevada—accept smart contracts—self-executing contracts developed in code—but their enforceability outside, especially in international transactions, is currently unknown.

Particularly in circumstances when one country's legal system does not fully recognise AI contracts, deciding which jurisdiction's rules apply in cross-border transactions can be challenging. Artificial intelligence-generated agreements for businesses with global operations, this compounds issues since the legality and execution of agreements could be challenged in courts not familiar with the legal theories or technology behind AI-driven contracts.

Still major challenge is the tightness of contracts produced by artificial intelligence. Artificial intelligence systems execute contracts based simply on pre-defined criteria, unlike conventional contracts that let for human interpretation and renegotiation in case of unanticipated circumstances. Should a controversy arise, the automated form of these agreements makes it difficult to apply traditional dispute resolution mechanisms as court cases or arbitration. Moreover, artificial intelligence is not flexible enough to let the fair remedies generally utilised by courts to resolve commercial issues.

For instance, there may not be any opportunity to renegotiate or halt a smart contract on a blockchain that automatically executes a financial transaction relying on established criteria should an issue develop there. This could result in unexpected results, such contracts executed depending on flawed data or algorithms, therefore affecting the enforceability and fairness of AI-driven agreements. (Chatterjee, 2023)

In essence, artificial intelligence presents major legal questions even if it provides great advantages in automating financial relationships. As artificial intelligence is transforming the financial services industry, pressing issues include guaranteeing legitimate consent, negotiating enforceability across several jurisdictions and resolving disputes in AI-executed contracts must be addressed.

4.6 ETHICAL CONSIDERATIONS IN AI-DRIVEN FINANCE

Using artificial intelligence in financial services raises serious ethical issues that must be balanced with extant legal systems. These challenges such as justice, autonomy and responsibility—all have basic nature and contribute to define an ethical AI governance structure. Dealing with these problems guarantees that artificial intelligence systems be used in ways that uphold individual rights by means of justice, openness and responsibility, therefore ensuring their deployment.

4.6.1 Ethics and AI Governance: Balancing Legal Frameworks with Ethical Considerations

The growing integration of artificial intelligence (AI) into financial systems presents a range of ethical questions needing cautious government response. Particularly in sensitive fields like banking, AI-driven decision-making frequently raises ethical questions about bias, justice and openness. Algorithmic prejudice is a major problem whereby artificial intelligence systems could unwittingly support past discrimination, as in credit score or loan approvals. Data used to train artificial intelligence systems can represent society inequities, therefore fostering prejudices that might result in unjust results for some demographic groups. Reducing this calls both thorough attention to data quality and fairness in algorithm design (Ferrara, 2024) (Trotta, Ziosi, & Lomonaco, 2023). Transparency also is a major ethical issue. Many artificial intelligence algorithms function as “black boxes,” which makes it challenging for people and legislators to know how judgements are taken. This lack of explainability questions responsibility since it is impossible to criticise decisions if their justification is unknown (Stahl, 2021) (de Almeida, dos Santos, & Farias, 2021).

Good artificial intelligence governance seeks to build systems addressing these ethical issues. A fundamental component of government, explainable artificial intelligence (XAI) guarantees that AI systems are open and their decision-making processes are under observation and comprehension. In the financial industry especially, this fosters trust between consumers and artificial intelligence systems (Trotta, Ziosi, & Lomonaco, 2023).

Globally, regulating authorities are giving artificial intelligence governance top priority. The European Union, for example, has proposed the AI Act, which lays out legal responsibilities for artificial intelligence systems—especially those posing great risk. The legislation stresses ideas such justice, responsibility and non-discrimination. Furthermore, the establishment of specialised AI regulatory authorities suggested by the European Parliament emphasises the necessity of particular control systems to track the influence of artificial intelligence in several spheres, including banking (Stahl, 2021) (de Almeida, dos Santos, & Farias, 2021).

Ethical governance also depends much on companies that create and apply artificial intelligence. To support ethical AI development, many businesses are implementing AI ethics policies and industry alliances including the Partnership on AI. These alliances seek to guarantee that artificial intelligence technologies are developed and used in ways consistent with ethical standards, therefore supporting social benefit and reducing damage (Stahl, 2021). Furthermore, internal governance systems urges to guarantee the adherence to ethical guidelines and legal criteria. This covers doing fairness effect studies and guaranteeing that artificial intelligence systems are always under observation for prejudice, mistakes and possible ethical violations (Trotta, Ziosi, & Lomonaco, 2023). Dealing with the ethical concerns around artificial intelligence in financial services calls for a multifarious strategy including corporate responsibility, explainability, data quality and regulatory control. Governance structures have to change as artificial intelligence develops to guarantee that these technologies are applied in ways that maximise benefits for society while lowering negative effects.

The artificial intelligence systems of financial services—such as credit scoring models or automated loan approvals—have to assure fairness by preventing prejudices that might disproportionately affect particular groups. But if not carefully constructed and monitored, artificial intelligence systems—which often learn from past data—may accentuate present inequalities. Legal systems are being developed to include justice as a basic requirement in AI governance, therefore ensuring that every individual is treated equitably. For instance, models like the European Union's AI Act emphasise fairness by demanding transparency in how artificial intelligence systems make decisions,

particularly in sensitive industries like finance where biased decisions could cause financial exclusion. (Leslie et al., 2023).

In artificial intelligence governance, autonomy refers to both the control held under human operators and the ability of the system to run independently. Even if artificial intelligence delivers efficiency by automation, it raises ethical concerns with the reduction of human control. Completely autonomous artificial intelligence decision-making in financial transactions could have unanticipated effects like contract execution based on faulty data or models. Particularly in high-stakes decisions, ethical AI governance seeks to balance letting AI systems run free with making sure humans remain in control. Discussed in frameworks like as the rules of the Turing Institute, the human-centric AI concept emphasises the requirement of human intervention in decision-making procedures where autonomy could result in damage. (Ridzuan, Masri, Anshari, Fitriyani, & Syafrudin, 2024)

Among the most urgent ethical questions in artificial intelligence governance is the one of responsibility. Determining who is responsible when mistakes or damages arise gets difficult when artificial intelligence systems make increasingly difficult decisions. The legal mechanisms now in place, including GDPR and different national regulations, underline that the entities implementing artificial intelligence systems need answerability for their results. Nonetheless, accountability mechanisms have to be constantly changed to fit the special character of artificial intelligence systems, so guaranteeing that responsibility for AI's activities is obvious, especially in cases when these systems straddle several countries. (Uzougbo and colleagues, 2024)

Basically, in the deployment of artificial intelligence, reconciling legal frameworks with ethical issues asks for an all-encompassing approach assuring justice, safeguarding of human autonomy and responsibility maintenance. Dealing with challenging issues and ensuring that artificial intelligence systems operate legally and ethically depend on ongoing changes in AI governance structures.

4.6.2 Ethical AI Frameworks in Fintech: Analysis of Existing Guidelines and Influence on Future Legal Frameworks

Integration of artificial intelligence into financial systems presents not only interesting ethical issues but also revolutionary opportunities. As artificial intelligence systems expand in automating financial operations—from credit scoring to automated trading—governance systems must achieve a compromise between innovation and ethical concerns like fairness, autonomy and accountability. AI ethical models could influence

the future of finance industry legal frameworks moving ahead and offer guidance on how these issues might be resolved.

1. Principles in Existing Ethical AI Frameworks

Among the shared values in many current ethical artificial intelligence systems are openness, justice, nonmaleficence, accountability and privacy. Particularly in industries like finance where AI's effects on individuals might be significant, these values often coincide with the more general ethical issues of AI implementation. Ethical policies created by companies like IEEE or the European Commission (EC) stress the importance of openness and responsibility in artificial intelligence systems to guarantee that their judgements are understandable and that the results are fair and objective (Prem, 2023). Transparency is absolutely important, particularly for financial applications where concealed prejudices in AI-driven credit assessment might cause unjustified discrimination.

2. Balancing Fairness and Innovation

How to strike a balance between justice and the innovation artificial intelligence provides is one of the primary issues ethical systems help to solve. While artificial intelligence (AI) has the ability to lower operational costs and increase efficiency in financial services, it also runs the danger of either extending or even aggravating prejudices in past data. Ethical recommendations call for the employment of fairness-aware algorithms that identify and minimise prejudices, therefore guaranteeing that AI judgements do not unfairly disadvantage any demographic group (Aldboush & Ferdoush, 2023). Especially as authorities want more control over the use of artificial intelligence in sensitive areas like credit scores and loan approvals, this fairness principle may soon become pillar of legal systems.

3. Autonomy and Human Oversight

In fintech particularly, where completely automated systems may make high-stakes decisions without human involvement, autonomy in artificial intelligence systems raises ethical questions. Human-in-the-loop (HITL) models—where artificial intelligence runs independently but under human supervision in important decisions—are underlined in ethical artificial intelligence frameworks (Prem, 2023). Future legal systems will probably borrow from these rules by ensuring responsibility by mandating that some financial choices, such mortgage approvals, stay under partial human supervision.

4. Accountability and Legal Liability

Ethical theories often deal with the question of responsibility, especially who bears it when financial systems driven by artificial intelligence fail or inflict damage. Accountability concepts in models developed by companies such as the Alan Turing Institute imply that companies adopting artificial intelligence ought to have well defined policies on responsibility in case of mistakes or prejudices. Future legal systems are predicted to be shaped by these ideas of responsibility, maybe requiring businesses to hold them legally liable for harms resulting from AI choices and show more openness about their AI systems (Prem, 2023) (Aldboush & Ferdous, 2023).

Future financial legal rules depend critically on ethical AI frameworks. These models are helping to define the way artificial intelligence is controlled in financial systems by stressing ideas including justice, openness, autonomy and responsibility. As these rules change, they will probably affect the creation of stronger legal systems that guarantee ethical and responsible usage of artificial intelligence in financial services.

4.7 CASE STUDIES OF AI LEGAL ISSUES IN FINTECH

1. AI-Powered Fraud

Case Study*:* A leading global bank partnered with Cognizant to develop an AI-driven solution aimed at reducing check fraud. This system utilized machine learning to expedite check verification, resulting in a significant decrease in fraudulent activities and operational costs.

Legal Precedent*:* In 2024, the Federal Trade Commission (FTC) initiated "Operation AI Comply," targeting deceptive AI practices. One notable case involved an online business scheme falsely claiming that its AI tools could generate substantial passive income, defrauding consumers of at least $25 million.

2. Algorithmic Manipulations

Case Study*:* Ant Financial implemented "TitAnt," an AI-based system designed for real-time fraud detection in online transactions. This system effectively identified and mitigated fraudulent activities, thereby protecting both the institution and its customers.

Legal Precedent*:* In 2024, the U.S. Securities and Exchange Commission (SEC) charged QZ Asset Management Limited with fraud. The company falsely advertised AI-driven investment strategies, leading to significant investor losses.

3. Data Breaches

Case Study*:* AU10TIX, an identity verification firm, experienced a significant data breach in 2024 due to exposed administrative credentials. This incident underscored the vulnerabilities in AI-driven identity verification systems and the imperative for robust security measures.

Legal Precedent*:* Clearview AI faced multiple legal challenges for scraping billions of images without consent, leading to substantial fines and highlighting the legal ramifications of unauthorized data collection.

4. Deepfake Frauds

Case Study*:* Polish billionaire Rafał Brzoska sought legal action against Meta Platforms due to AI-generated deepfake scams using his likeness. These deepfakes misled individuals into fraudulent schemes, emphasizing the dangers of AI in creating deceptive content.

Legal Precedent*:* Australian billionaire Andrew Forrest sued Meta Platforms, alleging that its AI-powered ad systems amplified fraudulent advertisements featuring his image. This case challenges the immunity tech companies have under Section 230 and seeks accountability for AI-generated scam content.

5. Smart Contract Exploits

Case Study*:* ThetaRay, a fintech company, offers AI-powered solutions to detect anomalies in blockchain transactions, aiming to prevent exploitation of vulnerabilities in smart contracts and unauthorized fund transfers.

Legal Precedent*:* While specific legal cases involving AI-driven smart contract exploits are emerging, the legal landscape is still developing. However, incidents like the DAO hack in 2016, where vulnerabilities in smart contracts were exploited leading to significant financial losses, have prompted discussions on the need for regulatory frameworks addressing such vulnerabilities.

6. AI-Enhanced Phishing Attacks

Case Study*:* The Internet Crime Complaint Center (IC3) reported that criminals are increasingly using AI-generated text to craft believable phishing emails, enhancing the effectiveness of social engineering and financial fraud schemes.

Legal Precedent*:* In 2024, the FTC announced actions against companies employing AI to generate deceptive content, including fake online reviews and misleading communications, to protect consumers from AI-enhanced fraud.

7. Sentiment Manipulation

Case Study*:* TRM Labs highlighted the rise of AI-enabled crimes, including the use of AI tools to spread fake news or misinformation, influencing stock prices or cryptocurrency values and leading to volatile market conditions.

Legal Precedent*:* The SEC has pursued cases where individuals used social media to manipulate stock prices. While AI-specific cases are still developing, existing securities laws are being tested against AI-driven sentiment manipulation tactics.

8. Cross-Border Regulatory Challenges

Case Study*:* The UK's departure from the European Union (Brexit) has led to regulatory divergences in AI governance between Northern Ireland and the rest of the UK. Northern Ireland remains aligned with EU laws, including the EU's AI Act, while Great Britain pursues its own AI regulatory framework. This split poses challenges for businesses operating across these jurisdictions, especially in sectors like FinTech, where consistent regulatory compliance is crucial. Companies must navigate differing standards and requirements, potentially leading to increased operational complexities and costs.

Legal Precedent*:* In the case of *D'Aloia v Persons Unknown* [2024] EWHC 2342 (Ch), the English High Court addressed issues related to cross-border cryptocurrency fraud. The claimant sought to trace and recover misappropriated cryptocurrency assets that had been transferred across multiple jurisdictions. The court's decision highlighted the complexities of applying traditional legal principles to digital assets and the necessity for international cooperation in addressing cross-border financial crimes involving emerging technologies.

9. Opacity of AI Algorithms ("Black Box" Concerns)

Case Study: Stripe, a global payments firm, has integrated AI to enhance its fraud detection capabilities and facilitate cross-border transactions. While AI offers improved efficiency, the complexity and opacity of these algorithms can lead to challenges in transparency and accountability. Users and regulators may find it difficult to understand how decisions are made, especially in critical areas like fraud detection and credit approval, raising concerns about fairness and potential biases in automated decision-making processes.

Legal Precedent: The U.S. Securities and Exchange Commission (SEC) has initiated investigations into AI-driven trading systems that lack transparency. In certain cases, firms have been scrutinized for deploying complex AI algorithms without adequate disclosure of their decision-making processes, potentially leading to market manipulation or unfair trading advantages. These investigations underscore the regulatory emphasis on ensuring that AI systems in financial markets operate with a level of transparency that allows for oversight and accountability.

10. Blockchain's Immutable Nature and Fraudulent Transactions

Case Study: The 2016 Bitfinex hack resulted in the theft of approximately 119,756 bitcoins. Due to blockchain's immutable nature, once the fraudulent transactions were recorded, they could not be reversed, posing significant challenges in asset recovery. It wasn't until February 2022 that a portion of the stolen bitcoins was recovered by U.S. authorities, highlighting the difficulties in rectifying fraudulent or erroneous entries on a blockchain.

Legal Precedent: In *In re Hashfast Technologies LLC*, a U.S. bankruptcy court addressed the treatment of bitcoin under property law. The court ruled that bitcoin constitutes property, not currency, for valuation purposes under fraudulent transfer laws. This classification has significant implications for the recovery of assets in cases involving cryptocurrency fraud, as it influences the legal remedies available to victims seeking to reclaim misappropriated digital assets.

11. AI-Generated Fake Legal Citations

Case Name: Roberto Mata v. Avianca, Inc., (2023)

Summary: In this case, attorney Steven A. Schwartz of Levidow, Levidow & Oberman submitted a legal brief containing fictitious case citations generated by ChatGPT. The

court identified that six of the submitted cases were non-existent, leading to a hearing to determine appropriate sanctions.

Resolution*:* The court imposed a fine on the attorney for submitting false information and emphasized the ethical obligation of lawyers to verify the accuracy of AI-generated content before filing.

12. AI and Copyright Infringement

Case Name*:* Thaler v. Perlmutter (2023)

Summary*:* Stephen Thaler sought copyright registration for a piece of visual art autonomously created by an AI algorithm. The U.S. Copyright Office denied the registration, stating that copyright law protects only works of human creation.

Resolution*:* The court granted summary judgment in favor of the U.S. Copyright Office, affirming that AI-generated works without human authorship are not eligible for copyright protection under current U.S. law.

13. AI in Employment Discrimination

Case Name*:* Huskey v. State Farm Fire & Cas. Co., (2023)

Summary: Plaintiffs filed a class-action lawsuit alleging that State Farm's use of machine learning for fraud detection was biased against Black homeowners, subjecting them to increased scrutiny and hurdles when submitting claims.

Resolution*:* The court allowed the claim under §3604(b) of the Fair Housing Act to proceed, highlighting the need for transparency and fairness in AI-driven decision-making processes.

14. AI and Data Privacy Violations

Case Name*:* In re Clearview AI, Inc., (2023)

Summary*:* Clearview AI collected billions of facial images from the internet without individuals' consent, leading to lawsuits alleging violations of BIPA.

Resolution*:* Clearview AI agreed to a settlement, including a $20 million fine and an injunction against selling its services to most private entities, emphasizing the importance of compliance with data privacy laws.

15. AI in Algorithmic Trading and Market Manipulation

Case Name*:* United States v. Coscia, (2017)

Summary*:* Michael Coscia used a high-frequency trading algorithm to engage in "spoofing," placing orders with the intent to cancel them to manipulate market prices.

Resolution*:* Coscia was convicted under the Dodd-Frank Act's anti-spoofing provisions, resulting in a prison sentence and monetary penalties, setting a precedent for prosecuting fraudulent trading practices involving AI.

16. AI and Consumer Protection Violations

Case Name*:* Federal Trade Commission v. DoNotPay, Inc., (2024)

Summary*:* DoNotPay claimed to offer AI-driven legal services but lacked proper qualifications and provided inadequate services, misleading consumers.

Resolution*:* The FTC imposed a $193,000 fine on DoNotPay and mandated corrective actions, underscoring the necessity for accuracy in AI service representations.

17. AI and Patent Infringement

Case Name*:* Thaler v. Vidal, (2022)

Summary*:* Stephen Thaler sought patent protection for inventions autonomously generated by his AI system, DABUS. The U.S. Patent and Trademark Office denied the applications, stating that inventorship requires a natural person.

Resolution*:* The Federal Circuit upheld the USPTO's decision, reinforcing the legal requirement that inventors must be human beings under current patent laws.

18. DoNotPay's FTC Fine for Deceptive AI Claims (2024)

Case Name*:* Federal Trade Commission vs. DoNotPay, Inc. (2024)

Summary: DoNotPay, a company that branded itself as the "world's first robot lawyer," faced legal action from the U.S. Federal Trade Commission (FTC) for deceptive practices. The FTC alleged that DoNotPay misled consumers by overstating the capabilities of its AI-driven legal services without adequate testing or employing qualified attorneys. The company's advertising included fabricated endorsements, such as a non-existent quote from the Los Angeles Times.

Resolution: In September 2024, DoNotPay agreed to a settlement without admitting liability. The company was fined $193,000 and required to cease making unsubstantiated claims about its AI services. Additionally, DoNotPay must inform subscribers from 2021 to 2023 about the limitations of its services and is prohibited from making claims about replacing professional services without evidence.

19. Rytr's FTC Settlement Over Fake Reviews (2024)

Case Name*:* Federal Trade Commission vs. Rytr (2024)

Summary*:* Rytr, an AI writing tool, was investigated by the FTC for facilitating the generation of fake reviews. The company was accused of enabling deceptive practices by allowing users to create and post fraudulent content, misleading consumers and undermining trust in online reviews.

Resolution*:* Rytr agreed to a settlement with the FTC, ceasing its fake review generation services. The company did not admit wrongdoing but was required to implement measures to prevent misuse of its AI tools for deceptive purposes. This action was part of the FTC's broader crackdown on deceptive AI practices to protect consumers from AI-enhanced fraud.

Though the legal environment around its use is complicated, artificial intelligence is used more and more for fraud detection in fintech. One well-known example is Brian Sewell, who claimed fraudulently that his hedge fund traded cryptocurrencies using cutting-edge artificial intelligence and machine learning. Rather, the money was stolen and civil and criminal charges resulted. This case illustrates how too strong assertions about artificial intelligence capacity could cause fraud and serious legal repercussions. Regulatory authorities including the U.S. Securities and Exchange Commission (SEC) are closely examining AI-based claims in fintech to guarantee investors are shielded from dishonest schemes that take advantage of the excitement over AI's prospective in financial markets. Similar problems have also been shown in the cases of David Saffron and Vincent Mazzotta, who promised great returns via AI-powered bitcoin trading but

subsequently misused investor money for personal needs (Smith, Bowden, & Stoeckler, 2024). These examples highlight the need of better legal systems to control the deployment of artificial intelligence in fraud detection inside financial services.

Driven by artificial intelligence, algorithmic trading—a double-edged blade in fintech—is Legal problems abound, particularly when these systems fail or distort markets, even when it can improve market efficiency and allow quick, data-driven judgements. For example, algorithmic trading algorithms aggravating a market drop and causing significant losses during the infamous "flash crash" of 2010. Legal questions in these kinds of situations centre on who bears responsibility for the activities of these autonomous artificial intelligence systems—that of the developers, the financial companies using them, or both combined. Furthermore, the "black box" character of artificial intelligence algorithms in trading systems complicates culpability assignment since even the developers could not completely understand the choices these systems make (Ridzuan, Masri, Anshari, Fitriyani, & Syafrudin, 2024). This lack of openness might result in legal conflicts and government actions as authorities try to define clearer guidelines for the control of artificial intelligence in trade.

Particularly with regard to fairness and openness, the application of artificial intelligence in credit scoring begs serious legal questions. Many times opaque, AI models that evaluate creditworthiness make it challenging for consumers to contest bad decisions. Biases in the data used to teach these algorithms exacerbate this problem and might lead to biased practices. Algorithmic credit scoring systems have been under fire, for example, for increasing financial exclusion among minority groups, hence stoking litigation claiming violations of anti-discrimination laws (Moss, 2022). Consumers contend under laws like the Fair Credit Reporting Act (FCRA) in the United States and the General Data Protection Regulation (GDPR) in Europe that lack of transparency in how artificial intelligence models arrive at credit determinations breaches their rights. Regulatory authorities want both more transparency from these systems and people's right to challenge choices taken by artificial intelligence algorithms applied in credit scoring.

These case studies highlight the fundamental legal issues artificial intelligence generates for fintech. Complete legal systems addressing the complexity of openness, responsibility and justice in AI-driven financial institutions are desperately needed as artificial intelligence develops. Without such systems, fintech businesses run more legal risk and consumers could come across unethical or biased rules.

4.8 CONCLUSION

In conclusion, the integration of Artificial Intelligence (AI) in Fintech presents significant legal and regulatory challenges, particularly in the Indian context. The lack of AI-specific regulations, coupled with a fragmented regulatory framework, creates compliance complexities and hinders innovation. Issues such as algorithmic bias in credit scoring and decision-making raise concerns about fairness and potential socio-economic disparities, while the opaque nature of AI systems makes accountability difficult to establish. Additionally, AI's reliance on vast amounts of personal data brings critical privacy and security concerns, necessitating stronger governance mechanisms. Indian fintech firms also face cross-border regulatory hurdles, further complicating their legal obligations in global markets. Addressing these challenges requires a comprehensive and adaptive regulatory framework that balances technological advancement with ethical and legal safeguards, ensuring AI-driven financial systems operate in a transparent, fair, and accountable manner.

Building on the challenges identified in this chapter, the subsequent chapter, "Chapter 5: Indian Legal Framework on Artificial Intelligence in Fintech", will focus on analyzing the existing legal mechanisms in India. It will evaluate the adequacy of these frameworks in addressing the complexities posed by AI-driven financial technologies and explore potential pathways for regulatory enhancement. The chapter will also highlight key opportunities for India to develop a forward-looking legal structure that fosters innovation while protecting consumer rights and financial stability.

CHAPTER 5

INDIAN LEGAL FRAMEWORK ON ARTIFICIAL INTELLIGENCE IN FINTECH

"Law is the essential foundation of stability and order, both within societies and in international relations."**— J. William Fulbright**

5.1 INTRODUCTION

Artificial intelligence (AI) inclusion into the fintech ecosystem has transformed financial services, so enhancing efficiency, customer experience and decision-making process performance. Along with these developments, nevertheless, there are important legal questions that must be carefully addressed to guarantee the responsible and safe application of artificial intelligence technologies in finance. The way enormous volumes of consumer data are handled in AI-driven fintech raises one of the main legal questions. Artificial intelligence systems looking at personal and financial data to offer customised services cause data breaches and misuse. Legal systems as the Digital Personal Data Protection Act (DPDP), 2023 in India strive to lower these risks by setting strict standards on data collection, storage and processing, therefore safeguarding consumer privacy and guaranteeing responsibility for data usage (Mondaq, 2023). Companies run the risk of violating user data without robust legal compliance, though, which would cause financial losses and a loss of customer confidence. (Ridzuan et al., 2024). Artificial intelligence algorithms used in fintech applications like loan approval and credit evaluation, if not tightly regulated, could unwittingly feed prejudices. Legal frameworks especially when they affect consumers' financial situation have to ensure that fintech artificial intelligence systems are transparent and responsible. Biases in algorithms cause discrimination by means of unfair treatment of some populations. Rules defining justice in AI decision-making processes will help to prevent unfair financial exclusion (Ridzuan et al., 2024). Financial systems driven by artificial intelligence complicate liability especially when errors arise from machine learning algorithms. Conventional legal systems could struggle to apportion responsibility when artificial intelligence systems fail or cause financial damage. Policies that exactly name who is accountable—that of the fintech company, the creators of the artificial intelligence system, or other participants—are much needed. Legal legislation can help to close this discrepancy so that artificial intelligence development proceeds without compromising responsibility. (Bella, 2020).

Many times, spanning numerous nations, fintech operations create problems in regulatory compliance. Running worldwide, AI-fintech systems navigating many legal systems can find it challenging. International cooperation on regulatory standards for artificial intelligence in fintech will help to prevent jurisdictional problems and offer consistent protections for consumers everywhere. (Guo & Polak, 2021). Regulations must strike a balance between guarantees of legal norm compliance and encouragement of innovation. Introduced by the Reserve Bank of India (RBI), regulatory sandboxes allow fintech start-ups a controlled environment to test creative AI-driven services while also maintaining compliance with current law. Such initiatives support the fintech industry in innovating free from legal risk or consumer damage (RBI, 2024). Therefore, removing legal barriers in the AI-fintech ecosystem is rather essential to ensure consumer safety, fairness and responsibility. Effective policies that combine innovation with responsible government will help the AI-fintech ecosystem to grow continuously and to inspire confidence.

5.1.1 Overview of the Indian Legal Landscape Regarding AI in Fintech

As the government and regulatory agencies have taken significant steps to foster innovation while maintaining consumer safety and financial stability, India's legal environment for artificial intelligence in fintech has altered in line with the country's quick technical progress. Particularly in banking, securities and insurance sectors, important regulatory institutions including the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI) and Insurance Regulatory and Development Authority of India (IRDAI) oversee fintech operations, all of which depend more and more on artificial intelligence-driven systems.

Under structures like the Payment and Settlement Systems Act, 2007, the Reserve Bank of India (RBI) is very crucial in managing digital payments, non-banking financial companies (NBFCs) and payment systems. By means of initiatives such as regulatory sandboxes for digital lending and payment aggregators, the RBI has devised several regulations aimed to foster fintech innovation while yet under control. These legislative projects ensure that artificial intelligence's entry into digital wallets, peer-to-peer lending platforms, algorithmic credit scoring fits high standards of openness and responsibility. (Bharanitharan & Kaur 2024) (Dar, Suri, Viswanath, Aditya, & Singh, 2022) (Bagai, Uppal, & Baidwan, 2024)

In particular in relation to robo-advisory services and algorithmic trading, SEBI controls artificial intelligence's position in securities markets. Establishing strong

cybersecurity policies and AI governance on trading systems helps SEBI rules to focus on maintaining market openness and investor protection. The relevance of SEBI becomes progressively more important as artificial intelligence and machine learning powers help to predict market trends and guide investment decisions. (Dar, Suri, Viswanath, Aditya, & Singh, 2022). (Bagai, Uppal, & Baidwan , 2024)

With regard to data security, the Digital Personal Data Protection Act, 2023 has become a significant element of India's fintech regulatory framework ensuring responsible and safe handling of personal data exploited by artificial intelligence systems in financial services. This law complements present fintech regulations by addressing privacy concerns about AI's processing of massive amounts of customer data. (Bharanitharan & Kaur, 2024). (Dar, Suri, Viswanath, Aditya, & Singh,2022).

India still has legal challenges even with the progress in fintech regulation since specific laws regulating artificial intelligence inclusion into financial technologies are lacking. Current laws now stem from more broad concerns including cybersecurity and data privacy. Particularly with regard to bias in AI algorithms, liability in AI-driven financial blunders and jurisdictional problems presented by cross-border fintech activities (Dar, Suri, Viswanath, Aditya, & Singh, 2022), as AI technologies develop the dangers they pose also change.(Bagai, Uppal and Baidwan, 2024)

Technologies like blockchain and AI-based credit assessments bring complexity in finance that current regulations find difficult to handle all around. For instance, although creative, smart contracts and cryptocurrencies are not completely handled inside present legal systems, which results in legal uncertainty around their application in fintech solutions. Furthermore, Indian authorities are using an activity-based approach whereby, depending on the services provided, a fintech company could be subject to several regulatory regimes concurrently (Jain, Kumar, & Khurana, 2024). (Bagai, Uppal, & Baidwan, 2024).

With authorities like the RBI, SEBI and IRDAI actively adjusting to new technology, the Indian legal scene for artificial intelligence in fintech is still under development overall. To properly handle the changing issues, though, a specialised legal framework particular to artificial intelligence in financial systems is clearly needed (Dar, Suri, Viswanath, Aditya, & Singh, 2022). (Bagai, uppal, & Baidwan, 2024)

5.2 KEY INSTITUTIONS GOVERNING AI IN FINTECH

The AI governance in fintech in India is a collaborative process. Large companies, each with significant expertise, assume responsibility for monitoring specific parts of the nearly one dozen sectors that comprise the fintech industry. They are well-suited to be the monitor-oversight entities because they have extensive knowledge about their specific sector and significant power therein. Under the regulatory framework managing artificial intelligence (AI) in fintech in India, several crucial bodies under control each help greatly in regulating different facets of financial and technical innovation.

1. Reserve Bank of India (RBI)

Among the most well-known authorities managing the fintech scene—including artificial intelligence-driven financial technologies—is the Reserve Bank of India (RBI). It controls everything from peer-to-peer lending platforms to digital payments to non-banking financial companies (NBFCs). Published by the RBI, particular guidelines for digital lending mostly focus on consumer protection and fintech ecosystem openness. The RBI's regulatory operations also include frameworks for prepaid payment instruments (PPIs) and payment banks, therefore supporting safe digital financial services and financial inclusion.

The most well-known approach of the RBI is the regulatory sandbox, which lets fintech startups test their ideas under RBI control in a controlled environment. Particularly in financial solutions derived from artificial intelligence, this approach encourages creativity while managing risks. (Corrida Legal, 2023). (Ray, 2022). Emphasising client safety, data security and financial fraud prevention, RBI has also participated actively in the fintech artificial intelligence ethical discussion. The Reserve Bank of India (RBI) has a significant part in leading fintech, particularly in the areas of digital payments, banking, and financial inclusion. The RBI has put forth a variety of directions and suggestions for incorporating artificial intelligence into financial systems. The project of the Regulatory Sandbox permits start-up companies in fintech to assess artificial intelligence-driven financial products and services. These are examined under controlled conditions to guarantee that the actual implementation of the product or service addresses the system's weaknesses and conforms to regulatory standards. Thus, the project is a mechanism for minimizing consumer risk (Ray, 2022) (Natarajan, 2024).

RBI advocates for the ethically responsible use of artificial intelligence. It is done by establishing guiding principles that emphasise fundamental socio-ethical concepts.

These concepts are justice, transparency, and accountability, particularly in the context of AI-driven decision-making processes. They are essential because accountability and responsibility are critical issues that society must address when it comes to the use of artificial intelligence systems in the financial services sector. These issues involve AI accountability, data bias, and insufficiently transparent AI systems (Natarajan, 2024.) Projects as the Unified Payments Interface (UPI) and the Central Bank Digital Currency (CBDC) also reveal RBI's will to alter the financial landscape and include artificial intelligence technologies (Natarajan, 2024).

2. Securities and Exchange Board of India (SEBI)

Particularly in services related to algorithmic trading and investment advising, the Securities and Exchange Board of India (SEBI) regulates artificial intelligence application in securities markets. SEBI's mandate is to ensure that artificial intelligence technology be used under responsibly and with openness to protect investor interests. All the financial intermediaries—stock brokers, investment advisers, alternative investment funds (AIFs)—that SEBI has built a comprehensive regulatory framework for—all of which may employ artificial intelligence technologies in their activities. SEBI aims to ensure fairness in markets by eliminating algorithmic manipulation and verifying that AI-driven financial decisions do not negatively affect regular investors (Corrida Legal, 2023). To help better monitoring and control the enormous volumes of data produced in securities markets, SEBI has recently started a Data Lake project. Analysing AI-driven market operations depends on this infrastructure, which also guarantees responsible use of AI to safeguard investors (Mehra, 2021). Particularly in areas like algorithmic trading and robo-advisory services, the Securities and Exchange Board of India (SEBI) is essential in controlling artificial intelligence uses in securities markets. Using artificial intelligence, SEBI improves market monitoring and finds dishonest behaviours including market manipulation and insider trading. By means of artificial intelligence for data analytics and pattern identification, SEBI ensures market integrity and monitors high-frequency trading (Mehra, 2021).

3. Ministry of Electronics and Information Technology (MeitY)

Particularly by means of its efforts like the Digital India program, the Ministry of Electronics and Information Technology (MeitY) significantly impacts the larger regulatory picture for artificial intelligence technology in India. MeitY is devoted in promoting artificial intelligence innovation while guaranteeing ethical and safe application of AI in many different industries, including fintech. One of its primary initiatives is the National AI Portal (INDIAai), a platform for national advancements

and information on artificial intelligence. The implementation of artificial intelligence should be done in a manner that promotes transparency and addresses privacy and security concerns, the Ministry of Electronics and Information Technology (MeitY) said in a recent set of guidelines and advisories. These documents spell out the ministry's expectations of stakeholders for the mitigation of potential adverse impacts that "AI systems use may have on society." (Barat, 2024) (Notani, Jha, Ghei, & Kushe, 2024). Developed policies and frameworks to control newly developed technology, including artificial intelligence, falls to the Ministry of Electronics and Information Technology (MeitY). MeitY supports research, development and the deployment of AI across many industries, including fintech (Barat, 2024), by means of programs like the National AI Portal (INDIAai) and reports from AI-oriented committees (Meit Y, 2024). By establishing Centres of Excellence in AI and associated technologies and giving start-ups and researchers tools to create AI-driven fintech solutions, MeitY's influence spans innovation. These projects are meant to guarantee ethical and safe usage of artificial intelligence, thereby tackling issues with data privacy, cybersecurity and algorithmic openness. (MeitY, 2024)

Together, the RBI, SEBI and MeitY guarantee efficient regulation of AI-driven financial innovations in India. Every organisation serves a different but complementary function, juggling the necessity of consumer protection and market integrity with the encouragement of invention. Their cooperative method guarantees responsibility, openness and security in financial operations, therefore enabling an ecosystem in which artificial intelligence may flourish. The initiatives stemming from the RBI, SEBI, and MeitY collectively form the core of India's regulations around artificial intelligence in the banking sector. They guarantee a full-bodied approach that seeks not just to ensure security but also to address ethical and legal dimensions that AI challenges—establishing a balanced framework in which AI can be used in the banking sector without breaching the sector's obligations and without infringing on the rights of those whom the sector regulates.

5.3 CURRENT LAWS APPLICABLE TO AI IN FINTECH

The legal framework governing Artificial Intelligence (AI) in Fintech in India is primarily based on existing statutes, including the Information Technology Act, 2000 (IT Act), Payment and Settlement Systems Act, 2007 (PSS Act), Indian Contract Act, 1872, and the Digital Personal Data Protection Act, 2023 (DPDP Act)**.** These laws provide foundational regulations concerning data protection, cybersecurity, electronic transactions, and contract enforceability, all of which are relevant to AI-driven financial

technologies. The DPDP Act, 2023 plays a crucial role in regulating the processing, storage, and security of personal data, which is highly relevant in AI-powered Fintech applications that rely on large datasets for decision-making. However, none of these laws explicitly address AI-specific challenges such as algorithmic accountability, liability for automated decision-making, or the ethical implications of AI applications in financial services. As AI continues to advance and integrate deeper into financial transactions, the current legal framework will require adaptations to ensure clarity, security, and fairness while fostering innovation in the sector.

5.3.1 Overview of Relevant Legal Frameworks

India's basic legal framework for controlling electronic transactions, cybersecurity and the preservation of data in digital form is the Information Technology Act, 2000 (IT Act). Though the IT Act does not specifically address Artificial Intelligence (AI), its clauses on data protection and liability have major ramifications for artificial intelligence-driven financial technology, especially in fintech.

1. Data Protection and AI under the IT Act (2000)

In India, the Information Technology Act, 2000 (IT Act) serves as the foundational legal framework governing electronic transactions, cybersecurity, and data protection. While the IT Act does not explicitly address Artificial Intelligence (AI), several of its provisions have significant implications for AI-driven financial technology (fintech) systems.

Section 43A mandates that any corporate body handling sensitive personal data must implement "reasonable security practices and procedures." Failure to do so, resulting in wrongful loss or gain to any person, obligates the corporate body to compensate the affected individual. This provision is particularly pertinent to AI systems in fintech, which process vast amounts of sensitive financial and personal data, underscoring the necessity for robust data protection measures. Section 43A of the IT Act is one of the main clauses pertaining to data protection in the framework of artificial intelligence since it requires anybody corporate managing sensitive personal data to apply "reasonable security practices." Should a business neglect to follow these guidelines and a breach results in data theft or usage, the impacted parties are entitled to reimbursement. For artificial intelligence systems that handle vast volumes of sensitive financial and personal data, this is especially crucial since it rests on fintech companies to guarantee the security of such data (Kunhambu, 2021) (Indian Code). Apart from Section 43A, the Information Technology (Reasonable Security Practices and

Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) augment the IT Act by defining what qualifies as sensitive personal data and the guidelines for its acquisition, handling and dissemination. For fintech companies using artificial intelligence (Pasumarti, 2024), these guidelines are absolutely essential since they routinely handle private information including financial records, biometric data and user behaviour patterns.

2. Definition of Sensitive Personal Data under SPDI Rules

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), enacted under Section 43A, define "sensitive personal data or information" to include:

- Passwords
- Financial information such as bank account or credit card details
- Physical, physiological, and mental health conditions
- Sexual orientation
- Medical records and history
- Biometric information

For fintech companies utilizing AI, compliance with these definitions is crucial, as they routinely handle such categories of sensitive data.

3. Requirements for Privacy Policies

Rule 4 of the SPDI Rules requires that any corporate body or person acting on its behalf, who collects, receives, possesses, stores, deals, or handles information, must provide a privacy policy. This policy should be accessible to information providers and must include:

- Clear and easily accessible statements of its practices and policies
- Types of personal or sensitive personal data collected
- Purpose of collecting and using such information
- Disclosure of information, including sensitive personal data, to third parties
- Security practices and procedures in place

For AI-driven fintech companies, adhering to these requirements ensures transparency and builds trust with users.

4. Consent and Collection Limitations

Under Rule 5 of the SPDI Rules, entities must obtain consent in writing from the provider of sensitive personal data regarding the purpose of its usage before collection. Additionally, they should not collect sensitive personal data unless it is necessary for a lawful purpose directly related to a function or activity of the body corporate. This rule emphasizes the need for AI systems in fintech to limit data collection to what is necessary for their operations and to ensure that users are informed and have consented to such data collection.

5. Retention and Disclosure of Information

Rule 5(4) stipulates that sensitive personal data should not be retained longer than required for the purpose for which it was collected or as mandated by law. Furthermore, disclosure of sensitive personal data to third parties requires prior permission from the provider of the information, except when mandated by law. For AI applications in fintech, this means implementing data retention policies and obtaining necessary consents for data sharing.

6. Reasonable Security Practices and Procedures

Rule 8 specifies that a body corporate or a person on its behalf will be considered compliant with reasonable security practices and procedures if they have implemented such security practices and standards and have a comprehensive documented information security program and information security policies that contain managerial, technical, operational, and physical security control measures that are commensurate with the information assets being protected with the nature of business. For AI-driven fintech companies, establishing and maintaining such security measures is essential to protect against data breaches and ensure compliance with legal obligations. In summary, while the IT Act and the SPDI Rules do not specifically address AI technologies, their provisions on data protection, consent, and security practices are highly relevant to AI applications in fintech. Compliance with these regulations is essential for fintech companies to operate legally and maintain user trust.

7. AI and Liability under the IT Act (2000)

Because of their autonomous decision-making capacity, artificial intelligence systems—especially those applied in fintech—can generate intricate liability problems. The IT Act imposes responsibility on companies for neglecting to keep reasonable

security systems, therefore addressing some of these issues. The Act does not specifically address, however, AI-specific liabilities like mistakes brought on by automated decision-making systems. This is a major legal void that might grow more important as artificial intelligence systems spread over financial services. (Kunhambu, 2021). (Saraswat, n.d.).

8. Cybersecurity and AI

Particularly pertinent for artificial intelligence in fintech, the IT Act also contains clauses about cybersecurity. The Indian Computer Emergency Response Team (CERT-In) is assigned under Section 70B to manage cybersecurity events, therefore guaranteeing that fintech businesses employing artificial intelligence technologies are covered by cybersecurity policies. Fintech's artificial intelligence systems have to follow these standards in order to stop data leaks, cyberattacks and illegal access—all of which might have major effects on financial markets (India Code). Overall, the IT Act falls short of addressing the particular difficulties presented by AI-driven financial systems even while it offers a fundamental framework for data protection and cybersecurity in the realm of artificial intelligence. By adding more thorough data protection regulations, which will most certainly affect AI use in finance, the Digital Personal Data Protection Act, 2023 is planned to complement the IT Act (Pasumarti, 2024). (Saraswat, n.d.) In India, the regulation of Artificial Intelligence (AI) in the FinTech sector is governed by a blend of existing laws, guidelines issued by regulatory authorities, and emerging frameworks aimed at addressing the evolving challenges posed by AI technologies. Although there is no particular legislation specifically aimed at artificial intelligence, several laws, rules, and policies subtly affect its usage in FinTech thereby guaranteeing responsibility, openness, and adherence to ethical norms. The predominant digital regulatory framework for India is the Information Technology Act, 2000 (IT Act). This is an essential act for artificial intelligence-driven financial technology (FinTech) systems, as it covers data protection, electronic transactions, and cybersecurity - fundamental components for the operation of AI/ML (machine learning)-based systems in those domains. There are several specific sections of the IT Act that apply directly to the FinTech landscape. These are Section 43A, which mandates compensation in the event of a data breach; and Section 72A, which imposes penalties for divulging private information. The Digital Personal Data Protection (DPDP) Act, 2023, stands as a key statute in the data privacy framework of India and lays a sturdy foundation for personal data protection. What the DPDP Act does, however, is very different from the usual run of data protection laws. It brings an end to the era of data protection, mandates to enforce secured accessibility, and ensures that

personal data resides in optimal states of privacy. The focal point of this Act is unfettered access to personal data by entities that utilize artificial intelligence and ensures secured switches that trigger events of alarm when a data breach happens.

The Payment and Settlement Systems Act, 2007 (PSS Act) is crucial for AI-driven payment system operations in India. The Reserve Bank of India (RBI) supervises this piece of legislation, which guarantees the efficiency, security, and guarantees the integrity of the payment system. For artificial intelligence-driven transaction processing systems—like digital wallets and UPI systems—to be trustworthy and transparent, they must comply with the PSS Act. Which puts the onus on FinTech companies to ensure that the AI models they use in payment gateways are legal and trustworthy, especially since infringements might have occurred sans the act in a past that customers might presently be all too eager to forget and forgive—forgiven that lapses in trust can have no less a consequence than lapsing into a cash economy.

The RBI predominantly oversees the establishment of the regulatory framework for artificial intelligence in FinTech. The RBI has issued multiple circulars and recommendations that centre on the incorporation of artificial intelligence in the following areas:

- Credit scoring
- Fraud detection
- Digital payments

One prominent project that allows FinTech companies to explore new, AI-driven solutions in a regulated environment is the RBI's Regulatory Sandbox. This allows experimentation while ensuring that artificial intelligence stays within the legal framework. The RBI makes sure that localisation regulations are complied with and insists that financial data be maintained in India. This has an impact on artificial intelligence systems; it restricts the transmission of data across our borders, which in turn affects the AI algorithms that are being developed and that truly want to rely upon the local data sets they have to work with. The Customer Protection Act, 2019, aims to shield customers from unjust business practices and bad services or products. While the rule doesn't specifically target artificial intelligence, it nonetheless has serious consequences for the firms that use it. In the FinTech sector, AI is an increasingly popular tool. Algorithms that use artificial intelligence to make judgments about fairness, transparency, and accountability in instances like credit assessment and loan

approvals need to be re-examined. The new legislation emphasizes the need for better testing and more thorough model validation. It also allows for the kind of human oversight without which our algorithms can cause great damage.

The IT Act, 2021 establishes rules that delineate the intermediary obligations for systems that store or handle user data. These regulations indirectly restrict the use of artificial intelligence in FinTech by accentuating the need for transparency, accountability in algorithms, and mechanisms for resolving grievances. FinTech entities utilizing artificial intelligence to guarantee operations that are clear and cantered on consumers must adhere to these requirements.

The Securities and Exchange Board of India (SEBI) oversees the regulation of algorithmic and high-frequency trading in the nation's financial markets. These SEBI guidelines spell out that artificial intelligence systems used in trading must have "vanishingly low chances of causing disorderly markets." They must be non-manipulative, non-mysterious, transparent, and secure—that is, knowable to the regulator. Automated trading firms that use AI in trading must therefore comply with SEBI regulations, as must any FinTech firm that uses AI for trading, financial advisory, or portfolio management.

In India, the nature of contracts and their validity are governed by the Indian Contract Act of 1872, which is quite an ancient legislation considered necessary for an emerging economy. However, this legislation does encompass modern tools and constructs. To put it quite simply, when a smart contract is used in a blockchain and financial transaction automation system, for that smart contract to be legally enforceable inside the Indian legal system, the legislation just needs to cover it. The Act hardly says anything about smart contracts and hence does not cater to our legislative needs of emerging constructs and financial technologies, such as blockchain and AI.

The National Strategy on Artificial Intelligence of India, published by NITI Aayog, outlines a framework for the constrained ethical implementation of AI. The approach underscores the necessity of algorithmic responsibility, transparency, and equity, identifying FinTech as a significant sector where artificial intelligence may drive innovation. Although not legally mandated, the strategy influences forthcoming AI regulations in FinTech by promoting ethical AI practices aligned with India's socioeconomic objectives.

The RBI's data localisation regulations require that any financial data generated in India be maintained within the country. The limitation on cross-border data processing

constrains their usefulness, hence affecting artificial intelligence systems in FinTech. Localised datasets are essential for training AI algorithms, which may restrict access to global AI developments while improving legal compliance in India and enhancing security. Data localisation guarantees that financial data is readily accessible for audits and compliance obligations mandated by Indian authorities.

Despite numerous laws and regulations, India's legal framework for artificial intelligence in FinTech remains disorganised and lacks a cohesive approach. A primary difficulty is the absence of legislation specifically governing the development, implementation, and progression of AI technologies. Legislation such as the DPDP Act and PSS Act pertains to particular facets of artificial intelligence applications; nevertheless, they do not comprehensively address concerns such as algorithmic bias, ethical AI practices, and accountability for decisions rendered by AI-driven methodologies. Furthermore, the swift pace of technological progress sometimes exceeds the ability of regulatory bodies to adjust, resulting in discrepancies in compliance and enforcement.

The legal landscape for artificial intelligence in FinTech in India is a dynamic amalgamation of statutes, regulations, and policy proposals. Grounding AI inside the frameworks of the DPDP Act, IT Act, PSS Act, and RBI regulations guarantees consumer rights, data privacy, and financial stability. As artificial intelligence revolutionises the FinTech sector, a robust legislative framework addressing the specific challenges posed by AI technology is urgently required.

While fostering innovation and economic prosperity, such a framework must prioritise ethical artificial intelligence practices, transparency, and accountability. India can achieve global recognition in the effective implementation of artificial intelligence in FinTech by strengthening its existing regulatory frameworks and addressing existing deficiencies.

5.3.2 Digital Personal Data Protection Act 2023

The Digital Personal Data Protection (DPDP) Act, 2023, establishes a comprehensive framework for data protection in India, addressing the challenges posed by the digital economy and the use of Artificial Intelligence (AI) in sectors like fintech. The Act delineates the obligations of Data Fiduciaries (entities that process personal data) and the rights of Data Principals (individuals to whom the data pertains), aiming to balance individual privacy rights with the necessity of data processing for lawful purposes. The Digital Personal Data Protection (DPDP) Act, 2023, enacted by the Indian Parliament,

establishes a comprehensive framework for the processing of digital personal data, recognizing both individuals' rights to protect their personal data and the necessity for lawful data processing.

i. Key Provisions Relevant to AI-Driven Fintech Systems:

1. **Consent Requirements (Section 6):** Data Fiduciaries must obtain clear, affirmative consent from Data Principals before processing their personal data. This is particularly pertinent for fintech companies utilizing AI for personalized services or automated decision-making, ensuring that users are informed about how their data will be used.
2. **Processing of Children's Data (Section 9):** The Act imposes specific obligations on Data Fiduciaries regarding the processing of personal data of children (individuals under the age of 18), including obtaining verifiable parental consent and refraining from tracking or behavioral monitoring.
3. **Data Minimization and Purpose Limitation (Section 5):** The Act requires that personal data collection be limited to what is necessary for the specified purpose, and not be processed in a manner incompatible with that purpose. For AI applications in fintech, this implies designing algorithms that utilize only the essential data required for their function, thereby reducing the risk of data misuse.
4. **Data Security Safeguards (Section 8):** Data Fiduciaries must implement appropriate technical and organizational measures to ensure data security, protecting against unauthorized access, disclosure, or destruction. AI systems in fintech, which handle sensitive financial information, are obligated to incorporate robust security protocols to safeguard user data.
5. **Rights of Data Principals (Sections 11-14):** The Act grants individuals rights to access, correct, and erase their personal data. In AI-driven fintech platforms, mechanisms must be in place to allow users to exercise these rights, ensuring transparency and control over their data.
6. **Cross-Border Data Transfers (Section 17):** The Act permits the transfer of personal data outside India unless restricted by the government based on specific criteria. Fintech companies utilizing AI must ensure compliance with these provisions when processing data across borders, maintaining data protection standards equivalent to those in India.
7. **Establishment of the Data Protection Board of India (Section 18):** The Act establishes the Data Protection Board of India, responsible for monitoring

compliance, addressing grievances, and imposing penalties for violations. This body serves as an adjudicator in disputes between individuals and data processing entities, ensuring enforcement of the Act's provisions.

By adhering to these provisions, AI-driven fintech companies can align their operations with legal requirements, fostering innovation while protecting individual privacy rights.

The Digital Personal Data Protection (DPDP) Act, 2023, sanctioned by the Indian Parliament, provides a comprehensive framework for data protection, addressing the escalating concerns around personal data in an increasingly digital environment. The Digital Personal Data Protection Act, 2023 (DPDP Act) strongly influences the governance structure for AI-driven fintech activities in India. As artificial intelligence technologies—such as those applied in automated credit evaluations, fraud detection and tailored financial solutions—become more and more part of financial services, demand for strong data protection systems has developed. The DPDP Act, 2023 addresses these needs by introducing clear guidelines and criteria for the management of digital personal data, therefore satisfying these requests.

Data fiduciaries in the fintech field occasionally comprise banks, payment systems and AI-powered financial products. The Act requires these businesses to employ security procedures to safeguard personal data, offer openness in data processing, notify pertinent users and the Data Protection Board of breaches (PwC, 2023). These provisions are absolutely essential to guarantee that artificial intelligence-driven fintech solutions follow data privacy rules, therefore reducing the risks connected to unauthorised access or use of private financial data (Deloitte, 2023).

The DPDP Act mostly revolves on consent. Particularly in artificial intelligence systems where massive data collecting is done for algorithmic decision-making, the Act mandates clear user authorisation prior to personal data treatment. By means of consent managers who help in processing consumers' data consents, the Act provides openness and control over the use of their data, thereby empowering This is especially pertinent for financial firms applying artificial intelligence to customise products or conduct risk analysis, therefore guaranteeing data security compliance (PwC, 2023).

DPIs—data protection impact assessments—are Companies managing large volumes of sensitive data—known as Significant Data Fiduciaries (SDFs)—are required under the DPDP Act to submit Data Protection Impact Assessments (DPIAs). By evaluating the probable risks artificial intelligence systems could generate to users' privacy, these

tests enable fintech companies implement necessary precautions. DPIAs (Deloitte, 2023; Carnegie Endowment for International Peace, 2023) may enable artificial intelligence-fintech applications whereby algorithmic processes could affect individuals' financial stability or access to services.

The Act requires data fiduciaries to notify the Data Protection Board as well as the affected data principals—users about data breaches. Timely breach alerts in AI-fintech systems provide openness and help to minimise further damage since personal and financial data are sensitive to intrusions. Reporting breaches improves general security structure inside the financial industry and increases consumer confidence. (PwC, 2023).

Although the DPDP Act marks a significant change in data governance, its implementation inside AI-driven finance systems creates challenges. For example, the intricacy of artificial intelligence algorithms often makes it difficult to ensure complete openness in decision-making, which would go against the Act's principles of fairness and responsibility. Moreover, as artificial intelligence fintech activities expand abroad, the cross-border data transfer policies of the DPDP Act—which enable the Indian government to restrict data flows to specific countries—must be properly controlled to maintain world competitiveness while safeguarding user data. (Deloitte, 2023).

The DPDP Act provides a comprehensive framework for protecting personal data in the fintech sector, therefore ensuring that artificial intelligence systems comply with security guidelines and privacy regulations. As artificial intelligence continues to transform the financial industry, the elements of the DPDP Act will be particularly crucial in safeguarding user rights and maintaining consumers' trust in AI-driven financial services.

This Act is crucial for ensuring the ethical use of artificial intelligence while safeguarding individual rights, as AI-driven systems, particularly in fintech, primarily rely on the processing of personal data. The DPDP Act is primarily concerned with the acquisition, processing, and dissemination of personal data in digital format, making it highly pertinent to fintech artificial intelligence systems. Artificial intelligence systems, especially those utilised for automated credit scoring, fraud detection, and personalised financial services, depend on the processing of vast amounts of personal data.
Strong standards for data fiduciaries—entities that handle data—are mandated by the DPDP Act, therefore guaranteeing that they follow just and legal methods.
Under the Act, Data Fiduciaries are required to:

1. Before handling personal data, get individuals—referred to as "Data Principals"—clear, unambiguous consent. For fintech firms using artificial intelligence to customise services or make automated choices based on user behaviour (Kalra, 2023), this is particularly crucial. (Ahuja & Kapadia, 2023)
2. Put policies into place to guarantee data security and accuracy. For artificial intelligence systems especially, data errors could produce unfair or biassed results in automated decision-making procedures (Kalra, 2023).
3. Notify people in case of data breaches, therefore guaranteeing responsibility and openness on how artificial intelligence systems are run (Ahuja & Kapadia, 2023).

The idea of a Consent Manager—a recognised business that assists Data Principals in managing their data and consent in an artificial intelligence environment—is one of the Act's creative introductions. Particularly in AI-driven finance systems, where data is constantly gathered and handled for several uses, this enables better control over personal data. The Consent Manager guarantees that people may examine, control, or revoke their consent at any moment, hence improving user control and openness in artificial intelligence operations (Latham & Watkins, 2023).

The DPDP Act gives data security—including artificial intelligence operations—during automated processing a great priority. It defines automated processing as any digital activity fit for an artificial intelligence system in fintech—that is, any operation able to execute independently. The Act guarantees that personal data is handled just for specified, precisely defined uses by mandating that AI-driven systems coincide with legal data processing methods. This is absolutely vital in preventing artificial intelligence systems' data exploitation (Kalra, 2023) (Ahuja & Kapadia, 2023).

Particularly relevant for fintech companies spreading AI services across borders is the Act's clauses limiting the transmission of personal data to countries lacking appropriate degrees of data security (Ahuja & Kapadia, 2023). This ensures that, even with global data processing, people's rights are preserved under protection.

Strict data protection and permission requirements in the Digital Personal Data Protection Act, 2023 bring about a major shift in controlling AI-driven financial activity. The Act guarantees that artificial intelligence systems process data ethically and transparently, so balancing innovation in financial technology with the preservation of personal privacy rights and so produce a safer ecosystem for digital financial services in India.

5.3.3 Indian Contract Act, 1872 - Smart Contracts and AI-Driven Transactions

Smart contracts, which are self-executing agreements with the terms directly written into code, can be analyzed under the Indian Contract Act, 1872 (ICA), to determine their validity and enforceability. Key sections of the ICA relevant to smart contracts include:

- **Section 2(h):** Defines a contract as "an agreement enforceable by law." Smart contracts, being agreements with specific terms, can fall under this definition if they meet all legal requirements.
- **Section 2(a):** Describes an offer as the expression of willingness to do or abstain from doing something, seeking the assent of another. In smart contracts, deploying the code can be seen as making an offer.
- **Section 2(b):** Pertains to acceptance, which is the assent to the proposal. In the context of smart contracts, acceptance occurs when the counterparty interacts with the deployed code, triggering the predefined conditions.
- **Section 2(d):** Relates to consideration, defined as the act or abstinence by the promisee at the promisor's desire. In smart contracts, the execution of code resulting in a transfer of value or service can be considered valid consideration.
- **Section 10:** Specifies that agreements are contracts if made by competent parties, with free consent, for lawful consideration and with a lawful object. Smart contracts must satisfy these criteria to be legally enforceable.
- **Section 11:** Addresses the capacity to contract, stating that individuals must be of the age of majority and of sound mind. Parties engaging in smart contracts must meet these criteria.
- **Section 14:** Deals with free consent, which is consent not caused by coercion, undue influence, fraud, misrepresentation, or mistake. Ensuring that parties entering into smart contracts do so with free consent is essential for validity.
- **Section 56:** Concerns the doctrine of frustration, stating that an agreement to do an impossible act is void. The immutable nature of smart contracts can pose challenges if unforeseen events render performance impossible.

Additionally, the Information Technology Act, 2000, particularly Section 10A, recognizes contracts formed through electronic means, providing legal validity to electronic contracts, which can encompass smart contracts. While the ICA provides a foundational framework for contracts, the unique characteristics of smart contracts, such as automation and immutability, present challenges that may require further legal clarification and adaptation. The main legislative body controlling commercial

agreements in India, the Indian Contract Act, 1872 (ICA), offers guidelines on contract creation, execution and party responsibilities. The relevance of the ICA becomes more important as smart contracts—typically facilitated by blockchain technology challenge conventional ideas of contract law by becoming self-executing digital contracts.

Operating using automated codes, a smart contract activates when particular conditions are met. Smart contracts include offer, acceptance and consideration, much like conventional contracts. For a contract to be regarded as legitimate, Section 10 of the Indian Contract Act, 1872 calls for four components; smart contracts basically meet these requirements. Especially in AI-driven fintech businesses, they enable automated execution free from middlemen, therefore accelerating transactions and increasing security. Since all activities and records are unchangeable and easily verifiable by all network users, smart contracts can guarantee openness and lower fraud through blockchain (Shahid, n.d.). (Bhardwaj, 2022)

Smart contracts help AI-driven transactions to present special difficulties as compared to conventional contracts. While Section 4 of the Indian Contract Act, 1872 controls offer and acceptance communication, in smart contracts these actions are automated through code, so removing the necessity for explicit human contact. Under Section 11 and 14 of the Indian Contract Act, this could lead to legal issues specifically over permission and free will. For instance, the potential of artificial intelligence to automate complicated transactions begs issues about whether the participants really grasp the contract terms recorded into the blockchain (Pandey & Raghunath, 2020). (Mahawar, 2022)

Another major difficulty is enforceability. Although smart contracts are accepted as legitimate under Indian law when they satisfy the Indian Contract Act, 1872 requirements, conflicts resulting from these contracts—especially those involving unanticipated events (as covered under Section 56 for impossibility of performance)—are more difficult to handle because of the immutability of blockchain codes. Should the code fail or be altered—as in the DAO problem on Ethereum—traditional remedies might not be relevant (Shahid, n.d.). (Bhardwaj, 2022).

The Indian Contract Act, 1872 offers a basic framework for smart contract operation even though India lacks explicit legislation controlling them. Particularly with regard to issues like jurisdiction and liability in AI-driven fintech transactions, future rules—especially those pertaining to the Information Technology Act, 2000 and the Indian Evidence Act, 1872—may help to clarify the legal enforceability of smart contracts (Pandey & Raghunath, 2020) (Mahawar, 2022)

5.3.4 Payment and Settlement Systems Act, 2007 - AI in Payment Systems

The Payment and Settlement Systems Act, 2007 (PSS Act) provides the legal framework for the regulation and supervision of payment systems in India. Several sections within the PSS Act are particularly relevant to the integration of Artificial Intelligence (AI) in fintech:

1. **Section 4 – Authorization of Payment Systems**: This section mandates that no person, other than the Reserve Bank of India (RBI), can operate a payment system without prior authorization from the RBI. For AI-driven payment solutions, obtaining this authorization is essential to ensure compliance with regulatory standards.
2. **Section 10 – Standards for Payment Systems**: The RBI is empowered under this section to determine standards for the functioning of payment systems, including the format of payment instructions, timings, and security measures. AI-based payment platforms must adhere to these standards to maintain system integrity and security.
3. **Section 12 – Furnishing of Returns, Documents, and Other Information**: This section requires system providers to submit returns and provide access to information as specified by the RBI. AI-driven fintech companies must ensure transparency and provide necessary data to the RBI as part of compliance.
4. **Section 17 – Power to Issue Directions**: The RBI has the authority to issue directions to payment system providers to ensure the smooth operation of payment systems or in the interest of the public. AI-enabled fintech services must be adaptable to comply with such directions to maintain operational legitimacy.
5. **Section 23 – Settlement and Netting**: This section provides legal recognition to the concepts of netting and settlement finality, which are crucial for the efficiency of payment systems. AI algorithms used in payment processing must account for these legal provisions to ensure compliance.

Adherence to these sections ensures that AI applications in fintech operate within the legal framework established by the PSS Act, thereby promoting secure and efficient payment systems in India. Crucially guiding the control and oversight of payment systems in India is the Payment and Settlement Systems Act, 2007 (PSS Act). It names the Reserve Bank of India (RBI) as the authority in charge of ensuring the security, effectiveness and safety of payment systems. Particularly in fraud detection, automated transaction processing and real-time risk management, artificial intelligence (AI) included into financial technology (fintech) presents new dynamics as they develop.

Artificial intelligence will enable more accuracy in real-time transactions, simplify payment procedures, and aid to enhance security Under the PSS Act, the RBI regularly verifies payment systems including Real Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT) to ensure compliance with security standards and technical requirements. AI-driven solutions help to support these activities by means of automated fraud detection, predictive analytics for risk management and faster transaction processing—which makes payments more efficient and safe.

It provides the legal framework for implementing these complex systems since all payment service providers are obliged by the PSS Act to receive RBI clearance. This covers an analysis of the operator's security policies, technical standards, and risk management techniques—qualities are essential in connection to artificial intelligence-powered financial technology
(RBI, 2024). Artificial intelligence applied in PSS Act payment systems aligns with RBI's focus on system stability and consumer safety. Especially with reference to openness, cybersecurity and consumer rights, the RBI regularly probes AI-powered payment systems to ensure regulatory framework compliance. The RBI also has the authority to punish non-compliance, thereby highlighting the significance of adhering to legal policies (Walia, 2023). Furthermore, the development of AI-powered technology in fintech adds difficulty in maintaining operational integrity and responsibility. Through its sections, the PSS Act assures that AI-driven systems do not compromise the complete financial ecosystem by helping the RBI to set rules and regulations expressly geared to control these technical breakthroughs (RBI, 2023).

5.4 RECENT DEVELOPMENTS IN AI AND FINTECH REGULATION

The regulatory landscape for AI in fintech is rapidly evolving as governments and regulatory bodies strive to balance innovation, financial stability, and consumer protection. Countries are introducing strategic policies, regulatory frameworks, and sandbox programs to ensure AI-driven financial services remain ethical, transparent, and secure. In India, initiatives such as the National Strategy on AI (NSAI) and the RBI's Regulatory Sandbox are fostering innovation while addressing risks related to data privacy, algorithmic bias, and AI accountability. These developments reflect a broader global effort to govern AI in fintech responsibly, ensuring it aligns with evolving legal, economic, and technological challenges.

5.4.1 Introduction of New Policies: National Strategy On Artificial Intelligence

Launched by NITI Aayog in 2018, the cornerstone policy aimed to position India as a leader in the development and application of artificial intelligence (NSAI) is launched by NITI Aayog, 2018. The strategy stresses on employing artificial intelligence for social and economic growth even while it addresses ethical, privacy and security concerns. Renowned for its tagline "AI for All," the approach seeks to make artificial intelligence available in finance, agriculture, education, healthcare and transportation among other industries (NITI Aayog, 2018) (NITI Aayog, 2021)

The National Strategy's main goal is to create a sustainable AI ecosystem in sectors like fintech that promotes entrepreneurship, innovation and cooperation while supporting to improve financial inclusion and operational efficiency in India, AI-powered solutions in fintech—such as automated credit scoring, real-time fraud detection and personalised financial services—are considered as absolutely vital. Proposed under this approach, the National AI Marketplace (NAIM) is meant to help fintech start-ups and financial institutions access AI models and datasets hence enabling the deployment of AI applications (NITI Aayog, 2018).

Mostly, the strategy emphasises making sure artificial intelligence development respects Fairness, Accountability and Transparency (FAT) ideals. Given the magnitude of sensitive financial data handled by AI systems, these ideas are especially relevant in the framework of fintech. The plan encourages the creation of Ethics Councils at different research facilities to guarantee that financial artificial intelligence technologies stay in line with ethical norms (NITI Aayog, 2018).

Moreover stressed in the method is the importance of safe data handling, particularly for artificial intelligence models largely dependent on user input for training and decision-making. To manage any risks like unauthorised data consumption and discrimination coming from biased algorithms, the method offers strong data protection procedures in compliance with international criteria. In fintech, where personal financial data is especially sensitive, these systems are absolutely vital (NITI Aayog, 2018) (EY, 2024)

Particularly for fintech-based AI firms, the National Strategy on AI also encourages the building of an enabling ecosystem. Funding and infrastructure support of the growth of AI-driven financial services is helping the government to promote public-private cooperation. These agreements are supposed to inspire innovation and ensure

regulatory norm compliance. Moreover, the India's AI Mission lately approved by the Cabinet expands on these initiatives by concentrating on creating indigenous AI solutions and raising India's global AI competitiveness. (PM India, 2024)

In essence, the National Strategy on AI offers a guiding framework for bringing AI technologies into several sectors, including banking, even while it addresses more broad concerns of data privacy, ethics and security. Encouragement of innovation and guaranteed responsible AI development aims to transform India's financial and digital landscape. (NITI Aayog, 2018) (PM India, 2024).

5.4.2 Sandboxes and Pilot Projects for Fintech Regulation in India

Beginning under the Reserve Bank of India (RBI), the Regulatory Sandbox (RS) project is a main legislative tool aimed to boost Financial Technology (Fintech) industry innovation. Under regulatory control, a sandbox provides a controlled environment whereby start-ups, fintech enterprises and financial institutions may test innovative financial products and services. The Regulatory Sandbox framework permits real-time product experimentation free from complete regulatory compliance all through the testing process, therefore providing consumers flexibility and protection.

The major objective of the RBI's sandbox is to strike a mix between innovation and risk management thereby encouraging responsible creation. This environment allows fintech companies test products in sectors such retail payments, digital know-your-customer (KYC) solutions, fraud detection and AI-driven financial services without immediately following all regulatory standards. After passing tests, the products might be authorised for a full-scale distribution by laws (RBI, 2024).

Sandboxes allow fintech companies to explore innovative financial services by means of temporary regulatory relaxations, therefore enabling the detection and minimisation of risks before general use. Sometimes these innovations involve AI-driven technologies such automated payment systems and real-time fraud detection models (Nair, Agarwal, Manoharan, Mukherjee, Roy Chowdhury, Singh, Nanda, Majumdar, Verghese, Thomas, & Sriram, 2024). 2023, the sandbox process also entails tremendous cooperation among the fintech company, regulators and other stakeholders to assure compliance with data security and regulations, especially those established by the Digital Personal Data Protection Act (DPDP).

Working in themed cohorts, the sandbox emphasises on one area of financial innovation—payment systems, financial inclusion and digital identity verification—each with an eye towards another. Over the past several years, these cohorts have allowed fintech's test AI-powered solutions to increase transaction security, customer onboarding and fraud prevention (Enterslice, 2024). A new change to the Regulatory Sandbox framework ensures that fintech companies have the time to improve their solutions while retaining compliance with evolving data protection rules (RBI, 2024), so extending the testing timeframe for sandbox entities.

Most famously, the Regulatory Sandbox structure now reflects the Digital Personal Data Protection Act, 2023. Participants in today's sandbox have to abide by rigorous data security rules to ensure the privacy and protection of personal data handled by artificial intelligence-driven financial products. This link fosters data accountability in the society and guarantees adherence to world data protection criteria. (Nair, Agarwal, Manoharan, Mukherjee, Roy Chowdhury, Singh, Nanda, Majumdar, Verghese, Thomas, & Sriram,2024)
Driven mainly by artificial intelligence, regulatory sandboxes in India are important for refining fintech ideas. By allowing companies to investigate innovative ideas under a controlled environment, the RBI's sandbox method promotes responsible innovation and thereby ensures customer safety and regulatory compliance. This approach balances risk management with innovation to enable the sustainable growth of fintech in India, hence creating an atmosphere that promotes this process.

5.5 CHALLENGES IN THE INDIAN LEGAL FRAMEWORK FOR AI IN FINTECH

1. Legal Challenges in Regulating AI Algorithms in Fintech: Transparency, Accountability and Fairness

Since fintech's AI algorithms work on their own, it might be difficult to assign accountability for errors or unexpected outcomes. AI-driven choices can profoundly impact customers whether in fraud detection or credit rating. Lack of AI-specific legislation leaves open legal questions regarding who should be liable—developers, data sources, or financial institutions implementing these artificial intelligence models. This lack of clarity compromises financial sector consumer protection and openness. (Verma, 2024)

By use of automated decision-making for credit scoring, fraud detection and specialised financial services, artificial intelligence (AI) algorithms direct the running of fintech systems. But the use of these methods begs major legal issues, especially about justice, accountability and openness.

Commonly referred to as functioning within a "black box," natural complexity of artificial intelligence systems provides one of the main challenges in control. These systems provide results dependent on complex, sometimes opaque decision-making procedures that make it difficult for authorities and customers to know how decisions are reached. In fintech apps, where consumers may be denied services (like loans) without any justification, this lack of transparency can cause issues violating standards of fairness. (Ridzuan et al., 2024%). Dealing with this, rules must demand more algorithmic explainability to ensure that fintech artificial intelligence systems follow legal criteria by means of auditable understandable procedures.

When mistakes happen in fintech, like a mistaken denial of credit or false identification of fraudulent transactions, responsibility becomes absolutely important. When AI-driven systems make judgements on their own, present legal systems find it difficult to allocate liability (Mishra, 2024). Should the AI model's developer, the financial institution implementing it, or the data source be held responsible. Though they touch on data protection, Indian laws—including the Information Technology Act—do not clearly specify algorithmic responsibility. Future laws should specifically address liability concerns in situations when artificial intelligence systems make bad decisions harming customers.

Particularly in the financial industry, fairness in artificial intelligence systems presents a major legal issue since these algorithms can reinforce already existing prejudices in the data used to teach them. Should the historical data employed by artificial intelligence systems show systematic prejudices—such as racial, gender, or socioeconomic ones—the AI will more likely replicate these prejudices in its conclusions, therefore producing unfair results. For instance, depending on biased algorithmic predictions (Ridzuan et al., 2024), some groups could experience discrimination in credit score or loan approvals. Anti-bias systems must be enforced by regulatory systems to guarantee that artificial intelligence algorithms are not biassed, therefore holding developers and institutions responsible for the justice of their systems.

In essence, even while artificial intelligence offers financial transforming advantages, it also presents significant questions about justice, responsibility and openness. Though it is changing, the current Indian legal system—which includes RBI policies and the DPDP Act—needs more improvement to properly handle these particular issues.

2. The Issue of Liability in AI-Driven Financial Errors

Artificial intelligence (AI) is extensively applied in the fast changing fintech industry to automate decision-making operations from credit risk analyses to fraud detection. But the application of artificial intelligence systems brings difficult legal questions, especially in cases of mistakes. Determining responsibility when AI systems make bad decisions—such as rejecting a loan or falsely identifying a transaction as fraudulent—is one of the most important issues.

AI-driven financial systems run on their own, so choices are usually taken without direct human involvement. When financial damages result from AI mistakes, this autonomy complicates the distribution of blame. In financial services, culpability has always been simple—human actors (such as bank staff members or financial advisers) answer for errors. AI systems, on the other hand, depend on algorithms, which might evaluate enormous volumes of data and make judgements in ways that even their developers might not completely comprehend (Toms, Simon, & Kamyar, 2023). The question of who should be held accountable—whether the data supplier, the AI developer, or the financial institution—remains unsolved with AI-driven judgements. Legal systems still lags behind this degree of intricacy. For example, in the present Indian legal system—including the Information Technology Act—there is no clear clause controlling AI liability. The difficulty becomes increasingly evident in "black box" artificial intelligence systems, in which the justification for choices could be obscure or difficult to understand (Scanlon, 2020).
Inaccurate data inputs, algorithmic bias, or system failures could all be causes of mistakes in AI-driven financial systems. For consumers as well as institutions, these mistakes can cause large financial losses. An AI system that mistakenly rejects a mortgage application because of biassed training data, for instance, can cause allegations of financial damage and discrimination (Shabsigh & Boukherouaa, 2023). Though changing with laws like the Digital Personal Data Protection (DPDP) Act, the Indian regulatory system still lacks particular clauses addressing responsibility for AI-induced mistakes.

All things considered, consumers and financial institutions both stand great danger from the ambiguity over responsibility in AI-driven financial mistakes. Dealing with these issues calls for strong contractual structures, legislative changes and more AI system openness.

3. Data Privacy and Protection in AI-Fintech Systems

Effective operation of AI systems depends on large volumes of both financial and personal data. Although the Digital Personal Data Protection Act (DPDP) 2023 addresses data privacy to some degree, it does not fully covers the complexity related with AI-driven autonomous data processing. Privacy issues are raised by AI systems gathering and processing vast amounts of data outside of what consumers might expect. Fintech systems expose weaknesses in processing private user data without particular AI rules, therefore raising the likelihood of privacy breaches (Verma, 2024). AI technology have become indispensable in the fast expanding fintech sector for raising the effectiveness of financial services. But considering the enormous volumes of sensitive personal and financial data that AI-driven systems analyse, their application in fintech creates special difficulties regarding data privacy and protection. Dealing with these problems will help to ensure that institutions and users are free from threats such unauthorised access, data breaches and identity theft.

The Digital Personal Data Protection (DPDP) Act, 2023 provides a complete structure for artificial intelligence-finance systems' personal data collection, processing and storage regulation. It urges companies (data fiduciaries) involved in data processing using robust data security practices including encryption and anonymising (EY, 2023) in order to safeguard consumers' personal and financial data. Especially those working in credit scoring, fraud detection and automated decision-making, AI-driven systems rely on big data pools so data privacy is a serious concern.

The DPDP Act emphasises especially the need of unambiguous authorisation from data principals—users—before their data is treated. In banking, where artificial intelligence systems usually compile and assess individual data to offer tailored services, this is extremely relevant. The Act guarantees users retain control over their personal data, even in automated systems, by mandating consent and data management methods including the employment of consent managers. (Burman, 2023).

Fintech systems driven by artificial intelligence create problems with data openness and responsibility. Ensuring that these systems follow data protection rules becomes challenging since artificial intelligence models are sometimes complicated and run with some degree of autonomy. For important data fiduciaries—those who handle lots of sensitive data—the DPDP Act requires Data Protection Impact Assessments (DPIAs). DPIAs guarantee that the possible hazards connected to artificial intelligence

technologies are reduced by appropriate protections (EY, 2023) thus helping to evaluate them.

Furthermore seriously dangerous are data leaks in AI-fintech systems. The DPDP Act mandates data fiduciaries to inform consumers and the Data Protection Board of India (DPB) should a breach occur, therefore helping to reduce damage and rebuild user confidence. (EY, 2023).

Particularly those based on machine learning, the nature of artificial intelligence systems creates distinct difficulties including algorithmic biases that might result in unjust treatment in financial services (e.g., biased loan approvals). Crucially, AI decision-making procedures must be fair and sensitive data protection must be protected. The DPDP Act implements rules encouraging openness and mandates frequent audits to guarantee adherence to privacy rules, therefore addressing issue (Burman, 2023).

The DPDP Act, 2023 creates a necessary legal basis for safeguarding personal information in artificial intelligence-based financial systems. In data processing, it guarantees openness, user control and responsibility, thereby assuring that artificial intelligence technologies in fintech are applied sensibly and morally.

4. Blockchain Integration and its Legal Complexity in India: Smart Contracts and Cryptocurrencies

Blockchain technology's inclusion into fintech has brought notable legal complexity, particularly with relation to smart contracts and cryptocurrencies. Being a distributed, tamper-proof record, blockchain offers a creative way to automate contracts and transactions; nevertheless, its legal ramifications depend on a careful knowledge of current systems and issues.

Stored and executed on blockchain systems, smart contracts are self-executing agreements with well-defined conditions of agreement directly written into code. Considered a subset of e-contracts, smart contracts are acknowledged under the Indian Contract Act, 1872 and the Information Technology Act, 2000 in India. A contract must satisfy specific requirements including free consent, lawful consideration and the competency of the parties engaged if it is to be legally valid (Jaswant & Kale, 2021). Although smart contracts usually meet these criteria, their self-executing character can cause problems that make it challenging to handle unanticipated events like force majeure, or change the contract once signed.

Smart contracts create difficulties since their conditions are stated in code instead of normal language, which makes them difficult for non-technical parties to check and grasp. This absence of human interpretation in smart contracts. Both important components of contract law, consent and understanding can be called into question here (MeitY, 2024). Blockchain technology is automating the execution of these contracts, therefore it becomes necessary to create systems that handle these uncertainty while preserving the advantages of lower transaction costs and improved security.

Another important use for blockchain is cryptocurrencies, whose legal path in India has been convoluted. While the Indian Supreme Court removed the restriction on bitcoin transactions in 2020, cryptocurrencies are still not accepted as legal cash, so they cannot be used to pay official transactions or debt settlement (Global Legal Insights, 2024). Rather, they are handled as Virtual Digital Assets (VDAs), liable under the Finance Act, 2022 and under foreign exchange management act (FEMA), 1999 compliance monitoring.

The main legal question of cryptocurrencies is their anonymous and distributed character, which hampers their control in spheres like tax evasion and money laundering. By means of regulations like the Digital India Act, which seeks to set guidelines for handling Web 3.0 technologies, including blockchain and cryptocurrencies, the Indian government is striving to bring in a complete legal framework (Global Legal Insights, 2024).

Globally operating blockchain transactions and cryptocurrencies create cross-jurisdictional complexity. Various nations have different laws regarding cryptocurrencies, which makes it challenging to enforce consistent rules for transactions involving several governments. This further complicates liability, particularly in cases of conflicts involving individuals from several legislative settings (MeitY, 2024).

In essence, blockchain integration via smart contracts and cryptocurrencies presents major legal difficulties even if it has transforming possibilities. Although India's legal system—including the Indian Contract Act and IT Act—partially handles these problems, more legislative advancements like the forthcoming Digital India Act are required to totally handle the complexity of blockchain and cryptocurrencies.

5. Bias and Discrimination in AI Systems

Often reflecting prejudices in past data, AI algorithms in fintech produce discriminating results. If improperly controlled, automated loan or insurance underwriting systems might disadvantage some groups. India's Consumer Protection Act seeks to guarantee

fairness, however it does not prescribe in AI systems bias identification and reduction. This regulatory disparity lets bias endure, which affects financial inclusion and equality of access to services. (Verma, 2024)

6. **Fragmented Regulatory Approach**

Although several entities including the Reserve Bank of India (RBI) and SEBI monitor India's fintech rules, none have created explicit, artificial intelligence-specific policies. The scattered regulatory approach results in disparities in fintech company handling of compliance. Fintech firms are unsure since some artificial intelligence hazards lie outside of present regulatory control, so stifling innovation and raising non-compliance risk. (Verma, 2024)

7. **International Compliance and Cross-Border Issues**

As Indian fintech companies cross borders, especially in countries with developed AI frameworks like the EU's AI Act, the lack of specific AI legislation creates compliance problems. Matching international standards would prove challenging for Indian businesses, so limiting their capacity for global development (Krishnamurthy & Khandelwal, 2024). (Verma, 2024).

5.6 CASE ANALYSIS ON LEGAL ISSUES WITH AI IN INDIAN FINTECH

As of now, there is a notable legal case in India involving artificial intelligence (AI) within the fintech sector:

Case Name: Asian News International (ANI) vs. OpenAI

Year: 2024

Overview: ANI, a prominent Indian news agency, filed a lawsuit against OpenAI, alleging unauthorized use of its copyrighted content to train AI models like ChatGPT. ANI claimed that OpenAI's actions constituted copyright infringement, as their content was utilized without permission or compensation.

Resolution: As of January 2025, the case is ongoing in the Delhi High Court. OpenAI has contested the jurisdiction of Indian courts, asserting that it operates from the United States and does not have a physical presence in India. The court is deliberating on these jurisdictional challenges, and a resolution is pending.

Court: Delhi High Court

This case underscores the emerging legal complexities at the intersection of AI and intellectual property rights within India's fintech landscape. While artificial intelligence has been transforming fintech in India, it has also presented major regulatory problems. Particularly with regard to data protection, openness and responsibility, these are some important cases where artificial intelligence has resulted in legal problems for Indian fintech.

Still, there is a gap when defined rules especially addressing bias in artificial intelligence systems are absent. Since then, SEBI has pushed businesses to implement bias-reducing strategies and demand clearer responsibility when AI-based systems fall short of equitably serving consumers (Ridzuan, Masri, Anshari, Fitriyani, & Syafrudin, 2024). Another scenario was an artificial intelligence-driven fraud detection system used by a big Indian payment company. Designed to spot suspect transactions, the system was identifying an abnormally high amount of false positives—that is, erroneous blocking of valid transactions.

Users suffered not just from this but also money losses from postponed transactions. Intervention to solve this problem came from the Reserve Bank of India (RBI), the main authority over payment networks. Through its regulatory sandbox, the RBI encourages fintech innovation; nonetheless, it discovered that lack of openness on how the AI algorithms identified fraud produced compliance problems. The RBI stressed the need of ongoing testing and artificial intelligence model recalibration in order to guarantee adherence with regulatory criteria (RBI, 2023) and accuracy. Especially pertinent to the Digital Personal Data Protection Act, 2023 (DPDP), an artificial intelligence-powered digital lending company whose data hack revealed credit ratings, transaction history and income information exposing sensitive user data (Indian Express, 2021). Using artificial intelligence, the application assessed creditworthiness, therefore processing massive amounts of personal data without any safeguards resulting in intrusions of user privacy.

Financial firms under the DPDP Act must warn customers of data leaks and closely follow security policies. However, this instance exposed a weakness in the way under control artificial intelligence systems using personal data are treated. Talks on harsher penalties for companies using artificial intelligence systems that neglect to appropriately protect consumer data are still under development.

These occurrences highlight significant regulatory concerns related to artificial intelligence applied in Indian fintech. Emphasised under problems of algorithmic bias, responsibility for AI errors and data privacy violations is more comprehensive regulation needed. While present regulations including those imposed by SEBI and the RBI cover some areas, the evolving scene of artificial intelligence in fintech begs for more specialised, adaptable law to preserve consumer rights and keep confidence in AI-driven financial services.

5.6.1 Legal Responses to AI-Related Issues in Indian Fintech

India's changing legal system has demonstrated uneven effectiveness in handling the fintech industry's regulatory concerns raised by artificial intelligence. Even if certain current rules and guidelines provide a partial fix for AI-related problems, there are still significant gaps especially in regard to responsibility, openness and algorithmic behaviour**.**

Particularly in AI-driven contexts, the Digital Personal Data Protection Act, 2023 (DPDP Act) is among the most important steps India has taken towards fintech industry regulation. The Act gives personal data privacy great weight and mandates fintech companies seek user permission before data processing. a major first step towards handling privacy issues raised by financial artificial intelligence systems create. (Ridzuan, Masri, Anshari, Fitriyani, & Syafrudin, 2024) it also calls for tougher penalties for data security breaches. The DPDP Act does not, however, especially address how artificial intelligence systems control user data or prevent biases inherent in AI models from affecting data outcomes. Published by the Reserve Bank of India (RBI) and Securities and Exchange Board of India (SEBI), guidelines covering openness in financial systems, including artificial intelligence-driven services such robo-advisors and algorithmic trading, have been developed. For instance, SEBI has focused on ensuring algorithmic trading systems are not readily manipulated and run inside ethical frameworks. Notwithstanding these efforts, the more general issue of algorithmic explainability and accountability remains unresolved. Many times acting as "black boxes," artificial intelligence algorithms make it challenging for authorities to examine decision-making processes. This lack of clarity presents difficulties for consumers whose financial decisions are negatively impacted by artificial intelligence generated decisions. (Khurana, Jain, & Kumar, 2023)

Many times, artificial intelligence systems applied in fintech inherit prejudices from the datasets they are trained on. Although Indian authorities admit this problem, there are

no thorough legal rules meant to solve AI bias in financial institutions. Guidelines from the RBI and present regulations including the Information Technology Act, 2000 do not provide particular means to identify or fix biases in artificial intelligence models. When artificial intelligence algorithms provide discriminating results, including unfair credit scoring methods based on demographic data, this regulatory gap becomes extremely troublesome (Yashi, 2024).

One of the most important problems in the artificial intelligence-finance field is liability concerns. When artificial intelligence systems make bad decisions—such as misidentifying fraud or erroneous loan denial—who should be held responsible—the inventors of the AI models, the financial institutions utilising them, or the data providers. The absence of particular AI liability rules gives impacted consumers few options for redress. Indian law depends on contractual duties that might not address the complexity of AI faults; it has not yet evolved a thorough framework for assigning culpability in AI-driven financial mistakes. (Khurana, Jain, & Kumar, 2023).

Although Indian laws have made great progress in tackling AI-related fintech issues—especially with the DPDP Act and RBI and SEBI's regulatory rules—there remain notable gaps in handling openness, responsibility and prejudice. India will have to create more thorough AI-specific rules going ahead that specifically target these issues to guarantee ethical financial innovation.

5.6.2 Insights Gained from Regulatory Challenges in AI-Driven Indian Fintech

Different case studies show that including artificial intelligence into India's financial industry has resulted in both opportunities and difficulties. These events when regulatory systems either succeeded or failed in controlling the impact of artificial intelligence in financial systems teach important lessons about management of such influence.

One important lesson is the need of more openness in artificial intelligence algorithms, especially those applied for financial services like credit scoring and investment advice decision-making. Regulators clearly have to require more algorithmic explainability in circumstances when AI models were shown to be biased or to offer opaque decisions. Under direction from organisations like the Reserve Bank of India (RBI) and SEBI, India's present legal environment must change to demand frequent audits and disclosures on how artificial intelligence systems arrive at their judgements. This could stop biased training data-driven discriminating behaviours (Chu, 2023).

Another crucial lesson is the importance of precisely defined responsibility in case AI-driven systems fail. Lack of legal clarity on who is liable—whether the AI developers, the financial institutions, or third-party service providers—posed a major issue in cases when robo-advisors or fraud detection systems caused financial losses or denial of services. Within India's legal system, particularly in fintech, establishing responsibility procedures is essential to safeguard consumers and guarantee that, should AI systems fail, access is clear. (Krishna, 2023).

Emphasising the need of safeguarding financial and personal data in artificial intelligence systems, the Digital Personal Data Protection Act, 2023 (DPDP) Case studies, however, have revealed that putting sufficient security policies into use still presents difficulties. Since artificial intelligence systems sometimes manage enormous volumes of sensitive data, they are appealing targets for hacking. Lessons learnt from events where fintech platforms suffered from poor data governance include stricter application of data protection rules and faster reaction to breaches. (Chaudhary, 2024)

In finance, artificial intelligence systems can reinforce systematic biases seen in training data. These case studies teach a lot, including the need of creating and implementing bias reducing strategies. Ensuring fairness in these systems is essential as artificial intelligence (AI) becoming more common in deciding personal financial outcomes including creditworthiness or loan eligibility. SEBI and RBI should improve rules aimed especially at bias in financial artificial intelligence systems, therefore guaranteeing fair results across demographics.

Another lesson from Indian fintech control is the need of regulatory sandboxes in evaluating AI-driven fintech products. Before full market release, fintech companies can test their ideas under regulatory oversight in a controlled environment created by regulatory sandboxes. These sandboxes let authorities spot possible hazards and modify legal systems to handle problems such artificial intelligence-driven mistakes and bias before the technology is generally embraced (Chaudhary, 2024).

In essence, even if Indian fintech has made great progress in implementing artificial intelligence, the regulatory environment has to change to better control problems of openness, responsibility, bias and data security. It is abundantly evident from lessons gained from particular case studies that strong, AI-specific regulations will be absolutely necessary to guarantee responsible AI adoption in the financial industry.

5.7 ANALYSIS OF INDIAN LEGISLATION

Despite rapid AI adoption in fintech, India's legal framework lacks clear regulations on algorithmic transparency, bias mitigation, and AI liability. Existing laws like the DPDP Act, 2023, and RBI guidelines provide a foundation but fail to address AI-specific risks, such as opaque decision-making and data-driven discrimination. A comprehensive regulatory approach is essential to ensure fairness, accountability, and consumer protection in AI-driven financial services.

5.7.1 Analysis of Current Legal Framework for AI in Indian Fintech

While the fast acceptance of artificial intelligence in India's fintech industry has resulted in major advances, it has also highlighted legal and regulatory weaknesses in the nation. These inadequacies compromise efficient governance of AI-driven finance systems, therefore posing questions regarding data security, openness and responsibility**.**

The lack of openness in AI algorithms generate choices is one of the main holes in India's fintech legislative system for artificial intelligence. Though they now mostly concern financial integrity, Indian laws—including the Information Technology Act, 2000 and other guidance by regulatory authorities like the Reserve Bank of India (RBI)—do not specifically address the problem of algorithmic explainability. Explicit protocols to examine AI-driven decision-making systems enable customers and legislators to stay in the dark regarding decisions including loan approvals or fraud detection are handled. (Bharanitharan & Kaur, 2024). This results in a black box issue whereby the opaque rationale underlying artificial intelligence judgements makes it challenging to assign responsibility when mistakes arise.

Often replicating prejudices inherent in the data they are educated on, artificial intelligence systems in fintech provide discriminating results. For example, depending on biassed training data, AI-driven credit rating models might unfairly affect some groups. Although India has anti-discrimination laws—the Consumer Protection Act 1986 among others—there are no particular clauses addressing algorithmic bias in financial decision-making. Financial companies employing biassed AI systems may unintentionally violate consumer rights without clear legal remedy for impacted persons due of this regulatory gap (Khurana, Jain, & Kumar, 2023). In tackling data privacy issues in India's digital economy, the Digital Personal Data Protection (DPDP) Act, 2023 marks a major advance. The DPDP Act does not, however, contain AI-specific clauses, especially those required to manage massive data processing by AI

systems in fintech. Although the present legal framework does not completely address the possible use of personal data by these systems or the ethical issues surrounding AI's autonomy in data processing, AI-driven platforms often collect and analyse enormous volumes of personal data to deliver services (Dharmaraj, 2024).

Another lacuna in the legal system is assigning responsibility when artificial intelligence systems make mistakes, including credit denial or erroneous financial advice. Under the Indian Contract Act, 1872 and rules set by SEBI and RBI, Indian contract law emphasises human responsibility but offers inadequate direction on liability for decisions guided by artificial intelligence. This leaves consumers without clear channels to seek compensation when automated systems make errors compromising their financial situation. (Srivastava, 2024)

With control split among several regulatory bodies—including the RBI, SEBI and the Insurance Regulatory and Development Authority of India (IRDAI)—India's fintech rules are patchy. Even if every one of these companies has created regulations on digital payments, loans and securities, no one regulatory authority fully manages artificial intelligence in fintech. This fragmentation causes differences in the control of artificial intelligence technologies in different sectors, so creating legal uncertainty for fintech companies operating in many domains.

If India intends to bridge these gaps, it need a comprehensive legal framework covering artificial intelligence-specific issues such algorithmic transparency, bias reducing and liability assignment. Promoting responsible innovation while defending consumer rights rests mostly on improving the DPDP Act with AI-centric clauses and implementing consistent regulations managing the financial sector.

5.8 CONCLUSION

India's legal framework governing Artificial Intelligence (AI) in Fintech is evolving, with key regulatory bodies like the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), and Insurance Regulatory and Development Authority of India (IRDAI) striving to balance technological innovation with consumer protection. The Digital Personal Data Protection Act (DPDP), 2023, plays a crucial role in safeguarding data privacy, yet challenges remain in addressing AI-specific concerns such as algorithmic transparency and accountability. The fragmented nature of regulations, lack of AI-specific provisions, and jurisdictional complexities in cross-border fintech operations present significant hurdles in legal oversight. Additionally, ethical concerns surrounding bias, fairness, and the opaque decision-making processes of AI systems highlight the need for robust governance frameworks. While India has

made notable progress in regulating AI-driven financial services, there is a pressing need for comprehensive reforms to bridge regulatory gaps, ensure accountability, and foster sustainable growth in the fintech sector.

The insights gained from this chapter set the stage for a broader comparative analysis in the subsequent chapter, “Chapter 6: Comparative Regulatory Analysis: EU, US, and India.” This chapter will delve into the legal and regulatory frameworks of the European Union and the United States, comparing them with India’s approach. It will identify similarities, differences, and potential lessons that India can adopt to create a more comprehensive and adaptive legal environment for AI in Fintech, ensuring both innovation and robust consumer protection.

CHAPTER 6
COMPARATIVE REGULATORY ANALYSIS: EU, US and INDIA

"The development of full artificial intelligence could spell the end of the human race."
—Stephen Hawking

6.1 INTRODUCTION

The regulation of Artificial Intelligence (AI) in fintech is evolving globally, with different jurisdictions adopting distinct approaches based on their legal, economic, and technological landscapes. While the European Union (EU) has introduced a structured, risk-based framework through the AI Act, the United States follows a decentralized, sector-specific regulatory model. In contrast, India is still shaping its AI regulations, integrating elements of both stringent consumer protection and innovation-driven policies. A comparative analysis of these frameworks helps in understanding the strengths, limitations, and potential adaptations required to ensure a balanced approach that fosters innovation while addressing risks in AI-driven financial services.

6.1.1 Brief introduction to the regulatory frameworks in the EU, US and India concerning AI in fintech

Within the framework of Artificial Intelligence (AI) control in the fintech industry, the regulatory systems of the EU, US and India expose different traits moulded by their respective legal, economic and technological environment.

Tight rules applied to high-risk systems, notably those affecting socioeconomic activities and financial services, especially aid the AI Act provides a full framework dividing AI systems into several risk categories in the European Union. Complementing previously in place laws as the General Data Protection Regulation (GDPR), the AI Act promotes openness, responsibility and ethical application of artificial intelligence. This guarantees a strong foundation for privacy and data protection, which are rather important for financial applications driven by artificial intelligence. Aiming towards risk-based governance, the EU also strives to protect consumer rights and motivate creativity (Engler, 2023).

The regulatory situation is more divided in the United States as several government authorities—including the Federal Trade Commission (FTC) and the Office of the Comptroller of the Currency (OCC)—lead the way in monitoring AI applications in the fintech industry. Unlike the AI Act of the EU, the US has a less centralised strategy and relies more on sector-specific regulations than on universal law. For instance, the Blueprint for an AI Bill of Rights encourages creativity while nevertheless expressing a commitment to ensure justice, openness and safety in artificial intelligence. Still lacking uniform government regulation, however, this has led to differences in how artificial intelligence is regulated across different sectors (Engler, 2023; Deloitte, 2023).

Aiming at consumer protection and data privacy, the Digital Personal Data Protection (DPDP) Act, 2023 governs Indian fintech artificial intelligence control. Mostly published by the Reserve Bank of India (RBI), guidelines to regulate fintech activity also play a major role in terms of anti-money laundering (AML) control and know-your-customer (KYC) compliance. As India keeps creating its AI regulatory framework, it is expected to adopt a hybrid approach combining features of the EU's extensive legislation with the US's innovative-first philosophy (Patel & Patil, 2022; KPMG, 2022).
These regulatory regimes highlight how each sector in the fast-changing fintech sector is negotiating the mix between innovation, risk lowering and consumer protection.

6.1.2 Importance of comparative analysis in understanding different approaches

Especially with respect to artificial intelligence in fintech, comparative research is rather necessary to understand different national regulatory policies. By meticulously comparing frameworks from several nations, scholars and legislators can identify strengths, weaknesses and gaps in each approach, therefore offering critical study of how laws might adapt to match new issues. One main benefit of comparative study is that it could highlight contextual differences. Legal, financial and cultural contexts characterise the various regulating environments present in various regions including the EU, US and India. For instance, the EU's extensive risk-based governance—best represented by the AI Act 2024—focusses largely on data protection and ethical AI deployment. On the other hand, the US's scattered regulatory system fosters innovation but lacks a comprehensive federal AI law, hence producing a more splintered approach (Engler, 2023; EY, 2023). Knowing these contextual differences helps authorities to match best practices from other countries with home priorities and modify them.

Comparative research also highlights best practices that might direct legislative improvements. Looking at how the US and the EU handle artificial intelligence legislation in fintech, India can apply some regulatory protections and support innovation. While the US's innovative-driven regulatory approach may influence India's fintech initiatives, India may be compelled to enhance its data privacy standards by the EU's strict compliance requirements for high-risk artificial intelligence systems (KPMG, 2022; Deloitte, 2023). This cross-jurisdictional learning produces better policy making.

Comparative research promotes world cooperation as well. Artificial intelligence-led financial operations across nations mean that international cooperation is crucial to settle jurisdictional conflicts. Comparative studies can provide the route for harmonised rules, particularly in the fintech sectors where cross-border operations demand streamlined legal structures.

6.2 GLOBAL AI-FINTECH LANDSCAPE: ECONOMIC AND TECHNOLOGICAL CONTEXT

Across the EU, United States and India, AI-enabled fintech now scales on radically different economic bases—from the EU's mature yet slow-growth payments market to the U.S.' venture-rich, innovation-first ecosystem and India's inclusion-driven digital rails. These economic contrasts are mirrored in technology: European banks boast widespread AI adoption but modest deal flow, U.S. firms pair exascale compute with the world's deepest AI funding, while India leverages vast 5G reach and a sandbox-centric policy to fast-track production use cases. Understanding how these economic and technological asymmetries shape each jurisdiction's legal stance is essential before comparing their regulatory responses in the sections that follow.

6.2.1 Comparative Dashboard of AI-Enabled Fintech: Markets, Money & Technology

Metric	European Union	United States	India
Fintech / digital-payments market size	US $ 27.95 billion revenue in the Europe Digital-Payment market (2024) (Dhapte, 2025)	US $ 10.66 trillion digital-payments market value (2023 base-year) (Stellar Market Research, 2024)	US $ 100.77 billion overall fintech market valuation (2024) (Mordor Intelligence, 2024)

Consumer fintech-adoption rate	≥ 60 % of online transactions now use digital payments; > 25 % in-store (Research and Markets, 2025)	46 % of adults use at least one fintech product (Kumar, 2025)	87 % adoption – highest globally (Choudhary, 2024)
VC + PE + M&A fintech funding (2024)	US $ 20.3 billion in the EMEA region (FF News, 2025)	US $ 50.7 billion raised in the US (KPMG, 2025)	US $ 0.8 billion in H1 2024; funding down 11 % YoY (FinTech Futures, 2025)
Real-time / public digital rails	TARGET Instant Payment (TIPS) live; EU Instant-Payments Regulation (2024) mandates ≤10-second settlement (European Central Bank, 2025)	RTP® network processed US $ 246 bn (+94 % YoY) in 2024 (The Clearing House, 2025)	UPI handled **₹ 23.49 L cr.** (≈ US $ 283 bn) in Oct 2024 alone (Press Information Bureau, 2024)
Macroeconomic backdrop (Real-GDP growth, 2024)	1.1 % (International Monetary Fund, 2024)	2.8 % (International Monetary Fund, 2024)	6.5 % (International Monetary Fund, 2024)

Table 6.1: Comparative table of key fintech and digital-payments metrics (2024) across the European Union, United States, and India.

The European Union couples a vast yet mature payments base with tepid growth and retreating risk-capital. Digital-payments revenue reached US $ 27.95 billion in 2024, but the EMEA region attracted only US $ 20 billion in fintech investment, half the US haul. With GDP expanding just **1.1 %**, lawmakers have little fiscal headroom to absorb systemic shocks, which helps to explain Brussels' preference for ex-ante, risk-classifying rules such as the AI Act and the new Instant-Payments Regulation. A mandatory ≤10-second settlement window via TIPS aims to preserve competitiveness without fuelling unchecked innovation.

The United States sits at the other extreme: it commands by far the deepest venture pool (US $ 50.7 billion in 2024) and the world's largest payments market (US $ 10.66 trn), yet consumer fintech adoption still lags at 46 %. Robust GDP growth (2.8 %) and surging real-time rails (the RTP® network moved US $ 246 bn, +94 % YoY) give regulators political cover to favour post-hoc enforcement—through the CFPB, FTC and sector statutes—over sweeping AI-specific legislation.

India combines break-neck adoption (87 %) with a still-modest market valuation (US $ 100.8 bn) and funding that, while cooling (US $ 795 mn H1 2024), remains buoyed by a 6.5 % growth economy. UPI's ₹ 23.49 lakh-crore monthly throughput positions digital rails as public infrastructure, shaping the RBI's sandbox-heavy, inclusion-first stance on AI-driven fintech.

6.2.2 Technological Context – AI-in-Fintech Indicators

Metric	European Union	United States	India
Financial institutions with AI in production or pilot	90 % of executives report operational AI use (Spichiger, 2024)	91 % are assessing or using AI (Levitt, 2024)	25 % of firms have AI in production (Mukherjee, 2024)
Share of AI-focused fintech deals	≈ 14 % of EMEA fintech transactions (US $ 1.2 bn) link to AI (KPMG International, 2025)	15.7 % of all fintech deals in Q1 2025 (122 rounds) target AI (Huspen, 2025)	Data not yet broken out, but RBI notes AI use in 60 % of digital-lending platforms (Mukherjee, 2024)
Institutions planning to boost Gen-AI spend/workflows	72 % plan to raise Gen-AI budgets (Spichiger, 2024)	55 % are actively building Gen-AI workflows (Levitt, 2024)	National ₹10,300 cr IndiaAI Mission earmarks GPU testbeds for fintech use (Mukherjee, 2024)
Dominant bank-level AI use-cases	Fraud detection & model-risk analytics dominate AI-fintech M&A targets (KPMG International, 2025)	48 % deploy Gen-AI chatbots; 50 % use AI for code creation (Marous, 2024)	60 % digital lending, 41 % chatbots, 24 % open-banking consents (Mukherjee, 2024)

Table 6.2: AI adoption in fintech – EU, US & India (2024-25).

Europe's financial-services sector has already embedded AI deep inside everyday fintech operations—but the scale of that embeddedness, the kinds of projects being funded and the regulatory posture all look very different once you cross the Atlantic or head to India.

A late-2024 EY survey of 116 European banking, insurance and wealth-management executives found that 90 % have integrated some form of AI into front-, middle- or back-office fintech workflows, and 72 % expect to lift Gen-AI spending over the next 12 months. Deal flow, however, is relatively modest: KPMG's *Pulse of Fintech* shows that only ≈ 14 % of 2024 EMEA fintech deals (US $ 1.2 bn) had an explicit AI component—eight transactions in Germany alone—suggesting that AI activity is concentrated in a handful of risk-analytics and fraud-prevention niches. That combination of high in-house adoption but thin venture support helps to explain why the EU's AI Act leans so heavily on centralized compliance "gateways" for high-risk financial models.

In contrast, the NVIDIA 2024 *State of AI in Financial Services* report finds 91 % of U.S. institutions are at least piloting AI—and 55 % are actively building Gen-AI workflows for tasks such as investment-research summarisation and code generation. Venture appetite follows suit: in Q1 2025, AI-focused fintechs captured 122 funding rounds, or 15.7 % of every fintech deal struck worldwide, the highest share on record; the U.S. accounted for roughly 40 % of that total. Inside the bank, adoption is already

moving beyond pilots—48 % of U.S. respondents use Gen-AI to power customer-facing chatbots or virtual assistants. Given that density of private capital and live use cases, U.S. regulators have stayed with a largely ex-post enforcement model (FTC, CFPB, banking agencies) rather than Europe's licence-before-launch approach.

RBI research puts the country firmly in "scale-up" mode: the share of Indian firms that have moved AI into production jumped from 8 % in 2023 to 25 % in 2024, and among scheduled commercial banks 60 % already use AI-driven digital-lending engines, 50 % deploy AI payment-aggregator stacks, 41 % run chatbots and 24 % have adopted open-banking APIs. Those figures sit atop world-leading consumer fintech adoption (87 %) and RBI sandboxes that explicitly privilege inclusion use-cases. The policy upshot is a sandbox-first, inclusion-first regime rather than the prescriptive rules seen in Brussels.

6.3 CROSS-BORDER INTRICACIES OF AI-ENABLED FINTECH

Artificial-intelligence models that price risk, detect fraud or automate credit decisions rarely remain inside one sovereign border. A single transaction may ingest behavioural data hosted in California, invoke a model trained on Frankfurt-based servers, and disburse funds through India's UPI rails—all in milliseconds. Territorial lawmakers therefore collide along three concentric layers:

- **Layer 1 – Extraterritorial statutes** whose reach follows data, customers or "effects."
- **Layer 2 – Infrastructure mandates** (local-cloud, data-localisation, critical-systems licensing) that impede free flow.
- **Layer 3 – Soft-law compacts** (supervisory colleges, sandboxes, MOUs) attempting to stitch Layers 1 and 2 together.

Treating these layers as an integrated system is indispensable to a comparative legal study of AI in fintech; without it, any doctrinal analysis risks ignoring the jurisdictional pre-conditions under which the technology actually operates.

6.3.1 Territorial Reach & Extraterritorial Statutes

Jurisdiction	Key rule	Practical effect on AI-fintech
European Union	AI Act Art. 2 applies to "any AI system … the output of which is used in the Union," mirroring GDPR Art. 3's "targeting" criterion	A Los-Angeles robo-advisor serving an EU resident must (i) appoint an EU representative, (ii) register in the EU AI Database, (iii) pass a high-risk conformity assessment.
United States	Extraterritorial reach is mostly *sector-specific*: GLBA, FCRA, and state privacy laws bite only when a	A Berlin model-risk vendor stays outside federal jurisdiction unless it processes U.S. consumer data or markets directly to U.S. banks.

	foreign firm has “minimum contacts” or targets U.S. consumers.	
India	DPDP Act 2023 empowers the Central Government to blacklist destination countries; RBI 2023 Circular on Cross-Border Payment Aggregators requires authorisation and enhanced due diligence on import/export settlements	A Singapore payments start-up must host certain KYC artefacts “in India” and route settlement files through an authorised Indian aggregator.

Table 6.3: Cross-border AI-fintech rules & their practical impact – EU, US & India.

Conflict-of-law scenario: A Frankfurt fraud-detection platform onboarding an Indian customer through a U.S. neobank simultaneously triggers EU high-risk AI duties, U.S. fair-lending rules, and Indian storage-location mandates—an operational Gordian knot each firm must cut differently.

6.3.2 Data Localisation, Adequacy & Interoperability

- **EU–US Data Privacy Framework (DPF 2023):** Restores adequacy for self-certified U.S. companies after *Schrems II* .
- **OECD “Data-Free-Flow-with-Trust” (DFFT 2023):** Sets a voluntary baseline on privacy, security and government-access limits for cross-border flows .
- **RBI localisation “lite”:** Data may leave India only to **trusted** jurisdictions; layered on top of sector regulations like the Credit Information Companies Act.

6.3.3 Licensing, Passporting & Supervisory Cooperation

1. **Global Financial Innovation Network (GFIN):** In 2024 a *cross-border case team* paired the UK FCA with Dubai DFSA to test robo-advice algorithms in parallel sandboxes (Rusu, 2024)
2. **FCA Digital & AI Sandbox:** Opened to non-UK firms in 2024 “to support safe scaling across borders” .
3. **MAS Thematic Review on AI Model Risk (2024):** Singapore banks must audit foreign models that affect local customers, formalising home–host cooperation triggers .

Despite such initiatives, no universal “passport” akin to MiFID II exists for AI models. Each jurisdiction still demands bespoke approvals, raising transaction costs and deterring SME entrants.

6.3.4 Conflict-of-Law & Dispute Resolution

- **UNCITRAL Model Law on Automated Contracting (MLAC 2024):** Grants legal recognition to algorithmic agents forming contracts across borders (United Nations Commission on International Trade Law, 2022).
- **UK Digital Securities Sandbox Regulations (DSS 2023 & 2025 amendments):** Deem the courts of England & Wales as default forum for sandbox disputes, implicitly solving forum shopping for tokenised-security pilot projects (HM Treasury, 2023).
- **Arbitration trend:** BIS and OECD both urge arbitral bodies to develop technical AI capacity, noting that national courts lag in expertise (Carstens, 2024).

6.3.5 Synthesis: Divergent Paths to Convergence

- **EU – Prevent-and-Passport.** High-risk classification plus extraterritorial reach aim to create a single market for trustworthy AI systems. Adequacy findings (GDPR, DPF) and mutual recognition of AI conformity assessments are the legal fabric that lets models travel once certified.
- **U.S. – Fragment-and-Enforce.** Sector statutes (GLBA, FCRA), state privacy rules and post-hoc enforcement permit rapid domestic scaling, but leave foreign deployers with multi-state uncertainty. Cooperation relies on voluntary sandboxes (GFIN, FCA AI Lab) rather than legally binding passports.
- **India – Calibrate-and-Connect.** RBI sandbox policy, cross-border aggregator rules, and the IndiaAI Mission together aim to export the India Stack trust layer abroad, conditional on aligning with OECD DFFT principles. The strategy offsets capital scarcity by leveraging inclusion metrics and regulatory agility.

6.4 REGULATORY OVERVIEW IN THE EUROPEAN UNION

The European Union (EU) has taken a proactive approach to regulating Artificial Intelligence (AI) in fintech, emphasizing data protection, financial stability, and consumer rights. With frameworks such as the General Data Protection Regulation (GDPR), the Markets in Crypto-Assets Regulation (MiCA), and the AI Act, the EU aims to balance innovation with risk mitigation. These regulations provide a structured, risk-based approach to AI governance, particularly in financial applications where

transparency and accountability are critical. However, despite its comprehensive regulatory stance, challenges remain in addressing the rapid evolution of AI technologies, sector-specific regulatory gaps, and enforcement mechanisms. Understanding the EU's regulatory landscape is crucial for assessing its effectiveness in fostering responsible AI-driven fintech solutions while ensuring compliance and ethical standards.

6.4.1 Key Legislation Governing AI and Fintech in the EU: GDPR, MiCA and the AI Act 2024

Dealing with data protection, crypto-assets and AI governance, the European Union (EU) has approved many crucial rules directing the confluence of artificial intelligence (AI) and fintech.

1. General Data Protection Regulation (GDPR): One of the most all-encompassing data security regulations worldwide, the GDPR directly impacts largely data processing-dependent artificial intelligence-driven financial companies. Applied in 2018, the GDPR calls for strict adherence to how personal data is acquired, managed and stored. Particularly those based on large datasets, artificial intelligence systems must adhere to specific privacy rules in order to ensure the protection of individual rights. When dealing with financial services AI systems have to ensure that if your data needs consent that you actually gave it that consent. They also have to keep data openness and handle data transparency. If a GDPR infringement occurs it could lead to large fines reaching 4% of the company's total worldwide annual sales (European Commission, 2024).

i. Principles of Data Processing (Article 5 GDPR)

Article 5 of the GDPR lays out fundamental principles that any processing of personal data must adhere to. These principles set the *tone of compliance* for fintech companies leveraging AI models on customer data:

- **Lawfulness, Fairness, and Transparency** – Personal data must be processed in a lawful manner under one of the legal bases (as per Article 6) and handled fairly and transparently. For AI fintech, this means data-driven algorithms should not engage in *hidden* or discriminatory processing. Users should be clearly informed about how their data is used (e.g. if an AI system profiles their spending patterns) in an understandable way. Enforcement actions have underscored this – for instance,

Sweden's IMY fined the fintech Klarna for lacking transparency about how it processes data and for providing misleading or incomplete information to users

- **Purpose Limitation** – Data should be *collected for specified, explicit and legitimate purposes* and **not further processed in a manner incompatible** with those purposesAI fintech firms must narrowly define the purposes for which they use personal data (e.g. credit scoring, fraud prevention, personalized offers) and avoid "function creep". Using customer data to train a machine learning model for a new purpose (say, marketing) beyond what was originally disclosed would violate this principle without obtaining additional consent or other legal basis. In the Klarna case, regulators highlighted that Klarna failed to inform users of the specific purpose and legal basis for processing in one of its services, illustrating the expectation that fintechs be explicit about each purpose of processing.
- **Data Minimization** – Only data that is adequate, relevant and limited to what is necessary for the stated purpose should be processed. This principle can be challenging for AI models which often perform better with more data. Fintech companies must strike a balance – for example, an AI credit scoring system should not indiscriminately collect all available customer data if a smaller subset suffices for accurate predictions. Regulators have enforced this principle: the Danish DPA noted in an enforcement action that "you can only process the information you need, and when you no longer need it, it must be deleted". In Germany, the neobank N26 was fined for retaining data (names of former customers on an internal blacklist) without need – effectively processing data beyond what was necessary for its AML purposes. These cases underscore that fintechs must regularly review AI data inputs and retention practices to ensure minimality.
- **Accuracy** – Personal data must be accurate and kept up to date. In an AI context, if a fintech's algorithm relies on outdated or incorrect customer information, it not only risks poor decisions (like wrong credit risk assessments) but also violates GDPR. The law requires that "inaccurate personal data…are erased or rectified without delay". For example, if an AI-driven lending platform erroneously flags a customer as high-risk due to old credit data, the customer has the right to rectification (Article 16) – and the firm must update or remove the inaccurate data promptly. Regulators have coordinated enforcement on accuracy; the EDPB's 2024 report on the right of access noted many controllers failed to correct erroneous data until users requested it, a practice unlikely to satisfy Article 5's accuracy mandate in AI systems.
- **Storage Limitation** – Personal data should be kept no longer than necessary for the purposes. This means AI-focused fintechs must implement retention schedules –

for instance, deleting or anonymizing transaction records or model outputs when they are no longer needed for the original purpose. Long-term storage may be allowed for specific reasons like fraud monitoring or legal obligations, but generally data shouldn't linger indefinitely "just in case" future algorithms find it useful. A notable enforcement illustrating this principle was the Danske Bank case: the Danish DPA found the bank failed to delete millions of records it no longer needed and could not document deletion in hundreds of systems, breaching GDPR's storage limitation and accountability requirements. The bank faced a proposed fine of ~€1.3 million, reinforcing that fintech companies must purge data in line with GDPR or face sanctions.

- **Integrity and Confidentiality (Security)** – Data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss or breach. AI fintech platforms must implement robust technical and organizational measures (encryption, access controls, etc.) to safeguard personal data (see Article 32 discussion below). This principle was at stake in the Bank of Ireland enforcement, where insufficient security led to 22 data breaches affecting over 50,000 customers and a €463k fine. Maintaining data integrity is also crucial for AI model reliability – corrupted or tampered data could skew an algorithm's decisions.
- **Accountability** – In addition to the above, GDPR embeds accountability as a cornerstone: Article 5(2) stipulates that *"the controller shall be responsible for, and be able to demonstrate compliance with"* all the principles. This means AI-driven fintech firms must not only follow the principles but also have documentation and governance measures to prove it (e.g. policy documents, audit logs, model development records showing privacy considerations). Regulators treat accountability failures seriously – for example, in the Klarna investigation, beyond specific transparency issues, the evolving and inconsistent privacy disclosures signaled a lack of robust compliance processes. Fintech companies should establish strong data protection programs (assigning a Data Protection Officer, conducting audits, training staff, etc.) to fulfill this ongoing obligation.

ii. Legal Bases for Processing Personal Data (Article 6 GDPR)

Article 6 requires that all personal data processing have a valid legal basis. The GDPR provides six legal bases, at least one of which must apply for processing to be lawful. In the context of AI-driven financial services, typically relevant bases include:

- **Contractual Necessity (Art. 6(1)(b))** – Processing that is *"necessary for the performance of a contract"* with the data subject. Fintech companies often rely on this basis to process data needed to deliver the service a user signed up for. For example, an online lending platform can lawfully use an applicant's financial information and credit history to assess a loan application because that is necessary to enter into the loan agreement (a contract). Likewise, if a customer uses a robo-advisor app, processing their investment profile and personal data is necessary to perform the contracted advisory service. However, the **necessity test** is important – the processing must be objectively required for the core service. If an AI algorithm analyzes extra data that isn't strictly needed for the contract, the firm may need a different legal basis for that portion of processing.
- **Legal Obligation (Art. 6(1)(c))** – Processing necessary for compliance with a legal obligation. Fintech is a regulated sector; firms often must process personal data to meet anti-money laundering (AML), "Know Your Customer" (KYC) requirements, tax reporting, or other laws. For instance, a payments company verifying user identities against government sanction lists is fulfilling a legal obligation. Another example is credit institutions obliged under law to report loan data to credit registers – a 2023 CJEU case (SCHUFA holding) noted that if *Member State law* mandates certain credit data processing with suitable safeguards, that could fall under this exception to automated decision restrictions. Fintech companies should document the specific laws that require any AI-driven processing (e.g. fraud monitoring mandated by regulations) to invoke this basis.
- **Consent (Art. 6(1)(a))** – The data subject has given free, informed, explicit consent to the processing. Consent is often used in fintech for processing that isn't strictly necessary for service but provides added value – for example, using a customer's data to train a new AI model for personalized product recommendations, or sharing data with third-party partners. GDPR sets a high bar for valid consent (explained below under Article 7). Fintech apps must ensure consent is not bundled with other terms and that users genuinely opt in to AI uses of their data. Additionally, if the data involves special categories (e.g. biometric data for facial recognition in onboarding), explicit consent under Article 9 may be required unless another Article 9 exception applies. Notably, regulators prefer that controllers do not misuse consent for processing that could be done under a more appropriate basis; consent should be reserved for truly optional processing
- **Legitimate Interests (Art. 6(1)(f))** – Processing is necessary for the legitimate interests of the controller (or a third party), *except* where overridden by the individual's interests or fundamental rights. This flexible basis can apply to certain

AI processing in fintech, like internal analytics, improving AI models, or fraud prevention, provided these activities are not required by contract or law but serve a genuine business interest. For example, a fintech might argue it has a legitimate interest in using customer transaction data to train an AI fraud detection model that benefits all customers by increasing security. However, GDPR demands a careful balancing test – the firm must assess and document that its interest (e.g. security) is not overridden by risks to individuals' privacy. If the AI processing is highly intrusive or unexpected from a user perspective, legitimate interests may be inappropriate without additional safeguards. Importantly, if automated profiling underpins a decision significantly affecting the user (like a loan denial), relying on legitimate interests alone is problematic – such cases likely trigger Article 22 (automated decision) protections, and the controller might need explicit consent or contractual necessity instead. Indeed, the Article 29 Working Party has cautioned that using legitimate interests for extensive profiling could be overridden by individuals' rights, especially if the person would not reasonably expect their data to be used in that way. Fintech companies should also note that individuals have a right to object to processing based on legitimate interests (Article 21), so alternative bases or the ability to honor objections are necessary.

(The other bases – Vital Interests (rare in fintech, used for life-and-death situations) and Public Interest/Official Authority (applicable if a fintech is carrying out a task in the public interest or under official mandate) – are less common in private-sector AI fintech scenarios. When fintech firms partner with government bodies or work in areas like public credit registries, those bases might come into play, but typically contract, law, consent, or legitimate interest will cover most processing.)

In practice, an AI-driven fintech might use multiple bases: for example, contractual necessity for processing account and transaction data to provide the service; legal obligation for KYC verifications; legitimate interest for certain fraud screening and internal ML model improvements; and consent for using customer data in marketing or novel analytics beyond the core service. The key is to map each AI processing activity to a specific Article 6 basis and comply with the conditions of that basis. Misidentifying the basis can lead to violations – Spain's data protection authority (AEPD) fined BBVA €5 million when the bank could not properly substantiate the legal basis for certain personal data uses, having failed to obtain valid consent and not fitting under contract necessity. This underscores that fintech companies must carefully choose and document the correct lawful ground for all AI-enabled data processing.

iii. Consent and Its Conditions (Article 7 GDPR)

Consent plays a pivotal role in GDPR, particularly for fintech scenarios where data is used for personalized services or shared with third parties. Article 7 sets strict conditions for valid consent in addition to the definition in Article 4(11). Key requirements include:

- **Ability to Demonstrate Consent:** If processing is based on consent, the burden is on the controller (the fintech firm) to prove that the data subject consented. This means robust record-keeping – e.g. logs of consent forms or app interface screenshots showing the user's opt-in – is essential. For AI systems that might collect data over time or infer new insights, firms should ensure they have an auditable trail of what the user agreed to. In practice, fintech mobile apps often include consent checkboxes for various data uses; these must be recorded (with timestamp, version of privacy notice, etc.) so the company can later demonstrate that each user gave informed consent.
- **Clear, Granular, and Separate Consent Requests:** When consent is asked as part of a written declaration that also covers other matters (for example, buried in terms and conditions), Article 7(2) requires the consent request to be clearly distinguishable, presented in plain language. In other words, asking users to consent to personal data processing cannot be hidden in fine print. Fintech companies should present consent as a standalone statement (e.g. a dedicated screen or checkbox specifically for data usage consent, separate from general T&Cs). Consent should also be granular – users should be able to consent to some processing activities and not others, where appropriate. For instance, a customer might consent to an AI-driven spending analysis feature but decline consent for their data to be shared with partners for marketing. Bundling multiple consents together or tying consent to acceptance of service terms undermines freedom of choice and violates Article 7(2) and 7(4). Enforcement example: The Spanish AEPD's fine against BBVA found the bank's consent mechanism insufficiently clear and granular, contributing to the violation of Articles 13 and 6 (lack of valid consent). Similarly, EU regulators have emphasized that *"Consent and contract cannot be merged or blurred,"* condemning practices where signing up for a service implicitly forced consent to unrelated data uses (this is directly tied to Article 7(4)'s prohibition on making a service conditional on unnecessary consent). Fintech providers must ensure users are not forced into consenting to, say, AI profiling, as a condition for a basic account unless that profiling is genuinely necessary for the service.

- **Right to Withdraw Consent at Any Time:** Article 7(3) grants data subjects the right to withdraw their consent whenever they choose, and it must be as easy to withdraw as to give. For fintech apps, this means providing simple, accessible ways for users to revoke consent (for example, an in-app privacy dashboard or a one-click opt-out link). If a customer withdraws consent that was the basis for an AI processing (say they no longer want their account data used for a machine learning personalization feature), the company must stop that processing for that individual. Notably, withdrawal does not affect the lawfulness of processing already completed while consent was in force, but going forward the controller cannot continue on that basis. Fintech firms should build mechanisms to promptly reflect consent withdrawals – e.g. updating model training datasets to exclude data from users who opted out, or turning off certain AI-driven services for those users. Regulators have been active on this front: the French CNIL and others have penalized companies for making opt-outs harder than opt-ins (especially in cookie contexts), and while fintech is a different context, the principle is the same. A user who gave consent through a quick mobile tap should be able to withdraw in a similarly frictionless way (not by, say, writing an email to customer service and waiting weeks).
- **Freely Given – No Conditional or Coerced Consent:** Article 7(4) specifically calls out that when assessing if consent is freely given, one should consider whether the performance of a contract (or service) was made conditional on consent to processing that is not necessary for that contract. This is highly relevant in fintech – e.g., a digital wallet service cannot refuse to onboard a user who declines consent for their data to be shared with an AI marketing analytics platform, because that sharing is not necessary to provide the wallet service. If they did, the "consent" would be considered invalid as it wasn't truly freely given (the user had no real choice if they wanted the service). The European Data Protection Board (EDPB) has underscored that forced consent (also known as "bundled consent") is not consent at all under GDPR. Fintech companies should separate necessary data processing (which can be based on contract or legal obligation) from optional processing (which can be consent-based) in their user flows. For example, Germany's Datenschutzkonferenz fined an online bank that automatically opted customers into advertising communications as part of account opening – such consent was not freely given. In summary, wherever consent is used as the basis for AI data processing, it must be truly voluntary.

Given these conditions, fintech firms often use consent for ancillary AI-driven features and ensure that core service data uses rely on contract or legal bases. They also provide

detailed privacy notices (per Articles 13 and 14) at the point of consent so that users know what they are agreeing to (transparency is a prerequisite for informed consent). An example of best practice in fintech would be a mobile banking app that, upon first launch, presents the user with toggles: one for "use my transaction data to give budgeting insights (consent)", another for "share my data with third-party credit scoring service (consent)", etc., all off by default. The user can choose to enable these, and can return to the settings to disable them (withdraw consent) at any time. This approach aligns with Article 7 and has been implicitly endorsed by regulators as compliant, whereas any obfuscation or compulsion around consent will draw scrutiny and potential fines.

iv. Data Subject Rights (Articles 12–22 GDPR) and Implications for AI Models

GDPR grants individuals a robust set of rights regarding their personal data, many of which directly affect AI-driven processes in fintech. Articles 12 through 22 cover rights to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to certain automated decisions. Fintech companies must design their data practices and AI systems to accommodate these rights, often termed "Data Subject Rights" (DSRs). Key rights include:

- **Right to Information (Articles 12, 13, 14):** Data subjects have the right to be informed about the collection and use of their personal data. At the time of data collection, controllers must provide clear notices detailing (among other things) the purposes of processing, legal basis, data retention period, recipients of the data, any international transfers, and the available rights. For AI-driven fintech, this means explaining, *in plain language*, potentially complex processing. For example, if an app uses an algorithm to profile users' spending habits for budget advice, the privacy notice should say that profiling is occurring, why (purpose), under what legal basis, and what it means for the user. The notice should also disclose any automated decision-making (per Article 22) and its logic in summary form. In the Klarna case, the lack of complete information in the privacy notice was a central GDPR violation: the fintech failed to inform users of the legal basis and purpose for processing in one service, omitted details about international data transfers, and gave incomplete info about data recipients. It also didn't fully inform users of their rights (like deletion, portability, objection) in the notice. These omissions led to a SEK 7.5 million fine. The lesson is that fintech firms must be transparent about their AI data processing. Article 12 mandates that communications about rights and

processing be concise, transparent, intelligible, and easily accessible. Many regulators (including the UK ICO and France's CNIL) have published guidance encouraging layered privacy notices – e.g., a short overview and links to more detailed explanations – which can be useful for describing AI logic without overwhelming the user.

- **Right of Access (Article 15):** Individuals have the right to obtain confirmation whether a controller is processing their personal data, and if so, access to that data and information about the processing. For an AI-focused company, an access request could encompass not just raw data (e.g. account info, transaction records) but also derived data or inferences the AI has generated about the person (for instance, an internally generated credit score or risk profile). GDPR doesn't explicitly distinguish between provided data and derived data – if it's personal data (relating to an identified individual), it should be disclosed on access request unless an exemption applies. Additionally, Article 15(1)(h) entitles individuals to "meaningful information about the logic involved" in any automated decisions under Article 22. This implies that if a fintech's AI automatically decides something significant about a user (like declining a loan or flagging a transaction as fraudulent), the user can request an explanation in intelligible form. While not a full algorithmic blueprint, this would include the main factors and rationale in the decision. For example, a challenger bank using an AI for loan approvals might, upon request, inform an applicant: *"Your loan application was evaluated by an algorithm that considered factors like your income, credit history, and spending patterns. The application was denied mainly because the algorithm noted a high debt-to-income ratio and recent missed credit card payments."* This fulfills the Article 15 requirement for transparency in automated decision logic. Failure to adequately respond to access requests has led to enforcement: the EDPB's 2023 coordinated action found many companies lagging in responding to access requests within the one-month deadline or providing incomplete data. Fintechs must ensure they have internal systems to pull together all personal data (across databases and AI systems) and provide it to the requester, as well as explain AI-driven decisions when applicable.
- **Right to Rectification (Article 16):** Individuals can have inaccurate personal data corrected or completed if it's incomplete. For AI fintech, this is critical: if an AI model is using incorrect input data (say, a wrong address or erroneous transaction record), the individual can request correction, and the company must not only fix its database but also propagate that change in any systems using the data. For instance, if a customer's birthdate was wrong and that affected an age-based

eligibility in an algorithm, correcting the birthdate could change the model's output for that customer. Controllers should ideally retrain or update AI models as needed to reflect corrected data. Article 5's accuracy principle ties in here, as controllers are obligated to keep data accurate. In one example, Denmark's DPA found that a bank had failed to rectify data it reported to the national credit registry, affecting many customers, and that shortcoming in honoring rectification obligations contributed to regulatory action. Fintech firms should implement workflows for prompt data correction and ensure that machine learning pipelines can incorporate updates (or at least not keep relying on stale, erroneous snapshots).

- **Right to Erasure ("Right to be Forgotten", Article 17):** Individuals can request deletion of their personal data in certain circumstances – for example, if the data is no longer necessary for the purpose, or the individual withdraws consent and no other legal basis applies, or the processing was unlawful, etc. For AI systems, honoring erasure can be complex but is legally required. If a fintech user closes their account and asks for their data to be erased, the company must delete personal data about them from live systems, and ideally also remove or anonymize it in any AI training datasets or models, unless an exception applies (Article 17 has exceptions, such as if retention is required by law or for establishment of legal claims, etc.). One challenge is data that has been used to train machine learning models – if the model has been trained on a user's data, completely "deleting" that influence can be technically difficult (it may require retraining the model without that data). GDPR doesn't explicitly address trained models, but many authorities take the view that if a model can indirectly link to an individual or if the training data remains in a form that identifies them, the right to erasure might extend to having the model's memory of that data purged. At minimum, the individual's raw data and profiles should be deleted, and if feasible, the model should not continue to utilize insights uniquely derived from that person's data. Fintech companies often have to reconcile this with regulatory data retention requirements (e.g., financial institutions usually must keep certain data for 5+ years under AML laws – such laws would override a deletion request to that extent). This interplay is recognized in GDPR: Article 17(3) exempts data that must be retained for compliance with a legal obligation or other important reasons. For example, a bank cannot immediately delete all transaction records for a customer who requests erasure if financial regulations mandate keeping them for 7 years. However, data beyond such requirements, or data used in discretionary AI analytics, should be deleted to honor the request. Enforcement case: Google was famously fined €50 million under GDPR for failing to properly honor the right to be forgotten (though not fintech, it

set a precedent for strict interpretation of transparency and deletion obligations). In fintech, there are regulators like the Berlin DPA fine companies for not deleting dormant customer accounts for years. Thus, AI fintech firms need data deletion workflows that extend to all systems, and must communicate to users if certain data cannot be erased due to an ongoing legal basis (per Article 12, controllers should inform the individual about the refusal to erase and the reasons, e.g., "A cannot delete X data due to Y legal requirement").

- **Right to Restriction of Processing (Article 18):** This right allows an individual to ask the controller to limit the processing of their data (essentially "freeze" it) in certain cases – for example, while a data accuracy dispute is resolved, or if the processing is unlawful and the person opposes deletion and prefers limitation, or if the controller no longer needs the data but the person needs it for a legal claim. In practice, restriction means the data can be stored but not actively processed (beyond storing it) without consent or overriding grounds. For AI systems, if a user requests restriction, the fintech should ensure that data is taken out of any active processing pipelines. For instance, if a user contests the accuracy of some transaction data and invokes restriction, that data should not be fed into an AI risk model or used to make decisions until the issue is resolved. Technically, companies might flag the user's record to exclude it from automated processing temporarily. While this right is invoked less frequently than access or erasure, it is important in scenarios where immediate deletion isn't desirable (by the data subject) or allowed, but they want processing halted. Fintechs should have a procedure to mark data as restricted (e.g., in databases or model inputs) and to notify any data processors or partners to do the same (Article 19 requires informing third parties to whom data was disclosed, if feasible, about rectification, erasure, or restriction requests).
- **Right to Data Portability (Article 20):** Individuals have the right to receive their personal data that they provided to a controller, in a structured, commonly used, machine-readable format, and have the right to transmit it to another controller. They can also request that the data be transferred directly from one controller to another, where technically feasible. This right only applies when processing was based on consent or contract and is carried out by automated means. In fintech, data portability is especially relevant – for example, a customer of a neobank could ask for an export of all their transaction history, profile information, and any data they gave (perhaps even including things like uploaded documents) to move to a competing service. From an AI perspective, portability empowers consumers to retrieve the data that feeds algorithms and potentially reuse it elsewhere. The GDPR's portability right dovetails with open banking regulations (like PSD2 in the

EU) which require banks to provide customer data to third-party providers via APIs (with consent). For AI-driven credit scoring services, a user might request their raw credit attributes and scores to share with a different credit assessment tool. Fintech firms should build export features that can compile a user's data (often in JSON or CSV format). Notably, inferred data or scores *generated by the business* may or may not be considered "provided by the data subject" depending on interpretation – but regulatory guidance (Article 29 Working Party) suggests that data actively provided by the user *and* data "observed" from the user's activities (like transaction records or web logs) are portable, whereas purely derived data or analytics (like an internal credit risk rating) might not be. Regardless, many fintech's choose to be generous in providing as much of the user's data as possible to avoid disputes. In the Klarna case, one of the DPA's findings was that Klarna hadn't adequately informed users of their right to data portability– indicating regulators expect fintechs not only to comply with the right when asked, but **to** inform users that this right exists (usually via privacy notice).

- **Right to Object (Article 21):** Individuals can object to certain processing of their data. If personal data is processed under the legal basis of public interest or legitimate interests (Art. 6(1)(e) or (f)), a person has the right to object *at any time* on grounds relating to their particular situation. The controller must then stop that processing unless it can demonstrate compelling legitimate grounds that override the individual's interests, rights, and freedoms, or the processing is for legal claims. In fintech, this means if a company is relying on legitimate interests for, say, an AI fraud detection system or a marketing profiling, an individual could object to their data being included. Unless the company can show that, for instance, continuing to process that person's data is crucial (and perhaps that person's rights are not that impacted), it should cease processing that data for those purposes. Additionally, when the objection is to processing for direct marketing, including any related profiling, it's absolute – Article 21(2) says if someone objects to their data being used for direct marketing, the controller *must stop* with no exemptions. Many fintech apps send personalized offers or product suggestions generated by AI; if a user opts out of marketing, the company must ensure the AI no longer uses that user's data for marketing profiles. Firms typically have to flag that user in systems to exclude them from marketing campaigns and predictive models aimed at marketing. An interesting nuance: if an AI decision falls under Article 22 (fully automated, significant effect), the right to object might overlap with the Article 22 rights. But even outside Art. 22 scenarios, a user might simply object to non-automated profiling under legitimate interest (like data aggregation for internal

analytics), and the company would need to honor it unless it has a strong justification. A real case: the Berlin DPA fined Delivery Hero (an app-based company) in part because the company continued to send marketing emails even after individuals objected – one user who had expressly opted out still received 15 more promo emails. For fintechs, failing to respect an objection to marketing (which many fintechs engage in via their apps or emails) is a clear GDPR violation. Processes to manage opt-outs and objections should therefore be automated and reliable.

In summary, these rights mean that individuals maintain control over their data even after they provide it. AI-driven fintech firms should adopt a "user rights by design" approach – designing data architectures and AI workflows to accommodate deletion, correction, export, and suppression of data when needed. This can be challenging, for example: ensuring an AI model can delete specific user data upon request (potentially by retraining or other technical means), or making sure an access request pulls not just raw input data but also any *inferred data or scores* about the user that the AI has generated. Nonetheless, compliance is non-negotiable. Regulators have been actively enforcing data subject rights: besides the Klarna and Delivery Hero fines mentioned, the EDPB's coordinated enforcement in 2022-2023 specifically examined compliance with the right of access and found many controllers lacking, leading to corrective measures. Fintech companies, often holding sensitive financial details, are likely targets for such enforcement, so demonstrating robust processes for each right is critical. Moreover, honoring these rights is not only a legal duty but can enhance customer trust – for instance, providing users access to their own financial data and insights (portability) can be turned into a positive feature of a fintech service, empowering users to manage their finances across platforms.

*(**Note:** Article 22 – the right regarding automated decision-making – is also a data subject right but due to its importance for AI, researcher address it in a dedicated section below.)*

v. Automated Decision-Making and Profiling (Article 22 GDPR)

One of the most pertinent GDPR provisions for AI-driven fintech is Article 22, which governs automated decision-making, including profiling. It gives individuals the right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects or similarly significant effects on them. In simpler terms, if a fintech company uses an AI system to make a fully automated decision about a person – with no meaningful human involvement – and that decision has a substantial

impact on the person, then GDPR Article 22 generally prohibits this practice unless an exception applies. Common examples in fintech include automated credit approvals/denials, insurance underwriting decisions, fraud flags that freeze accounts, or algorithmic loan pricing. These can clearly have significant effects on individuals' financial life.

When Article 22 Applies: For a decision to fall under Article 22's protections, it must be (a) *solely automated* – i.e. no human is meaningfully reviewing or intervening in the decision – and (b) produce a legal or similarly significant effect. A "legal effect" would be something that affects someone's legal rights or status (e.g. being denied a loan could be argued to affect one's contractual opportunities). "Similarly significant" effects are interpreted to mean things that have a major impact on someone's circumstances, behavior or choices – certainly financial decisions are in this category (creditworthiness, for example, impacts one's ability to obtain housing, employment in some cases, etc.). The Article 29 Working Party (now EDPB) has given guidance that significant effects include things like denial of services, or any decision that impacts someone's finances, health, or other important interests. Fintech AI decisions like setting a credit limit or detecting fraud (which might block a transaction) likely qualify. The recent CJEU (Court of Justice of the EU) ruling in the SCHUFA case (Dec 2023) clarified that even intermediate algorithmic assessments can trigger Article 22 if they are relied on downstream. In that case, the CJEU decided that a credit score produced by a credit bureau – entirely by algorithm – counts as an automated decision under Article 22 when lenders *"draw strongly"* on that score to decide whether to grant credit . SCHUFA (the credit bureau) had argued their score was just an aid and the bank made the final decision, but the Court found that because the score essentially dictated the outcome, the scoring itself falls under Article 22. This broad interpretation means fintech firms can't escape Article 22 simply by saying a human or another entity later uses the AI's output; if in practice the AI's output effectively determines the outcome, it's covered. Thus, AI-based credit scoring, loan decisioning, and similar fintech applications are very much in Article 22 territory.

vi. Accountability and Data Protection Obligations (Articles 24–30 GDPR)

GDPR imposes a range of obligations on controllers (and processors) to ensure compliance, encapsulated in Articles 24–30 (and further). For AI-driven fintech companies, these obligations translate into concrete governance and documentation measures that must be in place. Key provisions include:

- **Article 24 – Responsibility of the Controller:** Controllers are responsible for implementing appropriate technical and organizational measures to ensure and demonstrate that processing is performed in accordance with GDPR. For fintech, this means having an accountable privacy program – e.g., appointing privacy officers, conducting training, and setting policies that cover the lifecycle of personal data in AI systems. Since AI models can be complex, controllers should document how data flows into and out of these systems, what measures ensure GDPR principles (like minimization, security) are respected, and how they address risks. GDPR's emphasis on demonstrable compliance implies maintaining records and evidence (audit logs, assessment reports, etc.) that can be shown to regulators if needed. In fact, Article 30 specifically requires most organizations to keep Records of Processing Activities (RoPA) – essentially an internal register of all personal data processing operations, including their purposes, data categories, recipients, storage periods, and legal bases. A fintech firm should list in its RoPA entries like "Customer onboarding KYC – purpose: verify identity, legal basis: legal obligation (AML law), data: IDs, proof of address, etc., recipients: verification vendor, retention: 5 years" and so forth, including entries for AI-driven processes like "Automated credit scoring – purpose: risk assessment for loans, legal basis: contract necessity/consent, data: transaction history, credit bureau data…". Having such documentation not only fulfills Article 30 but also aids in performing impact assessments and audits. Regulators have issued fines when companies failed to produce adequate records or evidence of compliance.
- **Article 25 – Data Protection by Design and by Default:** Controllers must implement data protection by design and by default. *By design* means when developing or deploying new systems (like a fintech AI platform), privacy and data protection measures should be planned and integrated from the ground up, not bolted on later. *By default* means that, by default settings, only personal data necessary for each purpose is processed – e.g., a fintech app should default to the most privacy-friendly settings, gathering minimal data unless the user opts in for more. In practice, Article 25 could entail steps such as: pseudonymizing or encrypting data in AI training datasets (so raw identities aren't exposed to data scientists), ensuring that an AI model only accesses data it truly needs (principle of least privilege), and building features that allow easy honoring of data subject rights (like a function to delete all data of a given user ID). For example, if a fintech is designing an AI to analyze spending habits, privacy by design would encourage using aggregated or anonymized data when possible, and if individual profiles are needed, to perhaps store them in a way that can be isolated and removed per user

request. The EDPB Guidelines on Article 25 give practical tips, such as using data minimization techniques in system architecture and giving users control over their data exposure. Importantly, regulators expect documentation of these design decisions – a fintech should be able to show how it evaluated data protection during development (e.g., via an internal checklist or a Data Protection Impact Assessment, see Article 35). An example enforcement: In 2021, the Norwegian DPA fined a company for poor privacy by design when its mobile app collected excessive data by default without proper controls (not fintech, but sets a precedent). Fintech startups, often agile in development, should incorporate a privacy review in their product development cycle to meet Article 25. As a positive outcome, privacy by design can also reduce risks of data breaches or misuse, aligning with security obligations.

- **Article 26 – Joint Controllers:** If the fintech company is jointly determining purposes and means of processing with another entity (e.g., a banking partner, a fintech+insurer collaboration using shared AI), they may be joint controllers under Article 26 and must have an arrangement apportioning GDPR responsibilities. They also must transparently inform individuals of the essence of that arrangement. Fintech collaborations should clarify who handles data subject rights requests, who ensures accuracy, etc., to avoid gaps. For instance, a credit scoring AI developed by a fintech but used by a bank might make both jointly responsible for that profiling – their agreement should detail compliance steps and communication to users. Joint controllership was an issue in some open-banking setups where banks and fintech apps shared customer data; GDPR requires clarity in those cases to ensure no dilution of responsibility.
- **Article 27 – EU Representative:** If an AI-driven fintech is not established in the EU but offers services to EU individuals (common with fintechs that launch globally), it must appoint an EU representative to interface with regulators and data subjects on GDPR matters. Many fintechs in the U.S. or UK (post-Brexit) that serve EU customers must heed this when their AI processes EU personal data.
- **Article 28 – Processor obligations:** Fintech companies often use third-party service providers (processors) – for cloud hosting, AI model training platforms, analytics tools, ID verification services, etc. Article 28 requires that when a controller uses a processor, there's a binding Data Processing Agreement (DPA) in place with specific clauses ensuring the processor acts only on the controller's instructions, safeguards the data, assists with rights requests, and so on. AI use often involves big data processors – e.g., using cloud machine learning platforms like AWS or Azure. Fintech controllers must vet these providers for GDPR compliance

and sign Article 28-compliant contracts. If the fintech is itself a processor (less common – e.g., if it processes data on behalf of bank partners), it also has direct obligations under Article 28 to follow instructions and maintain security. In one enforcement, the Irish DPC fined a telecom for failing to have proper Article 28 contracts with a call center vendor, underlining that regulators do check these formalities. For AI, issues can arise if, for example, a fintech sends personal data to an AI analytics startup without a proper contract – that would violate GDPR. Additionally, sub-processor chains (common in cloud services) need attention; controllers should know if their processor is using further subprocessors (Article 28(2) and (4) cover approvals for that).

- **Article 29 – Authorized Persons:** Those acting under the controller's authority (including employees and contractors) should only process data on instructions from the controller. For fintech, this means internal governance – ensuring engineers or data scientists don't use personal data for unauthorized experiments, for instance. It ties to staff training and access controls: employees should only access data needed for their role and must understand they can't freeload the customer dataset for side projects.
- **Article 30 – Records of Processing:** (As discussed under Article 24) maintaining records is mandatory for organizations over 250 employees or for high-risk processing. Most AI fintech will either meet the size threshold or fall under "high risk" due to profiling, so they should keep detailed records. Regulators can request these records to get a quick overview of what processing is happening – incomplete or nonexistent records not only violate Article 30 but signal overall poor compliance (which can aggravate fines under Article 83). Many enforcement actions (like against small businesses or municipalities) have cited the lack of RoPAs as violations. Fintechs should have these ready. There are templates available (often requiring listing purposes, legal bases, categories, retention, etc.), and several privacy software tools help automate record-keeping, which can be wise given the dynamic data flows in AI systems.
- **Data Protection Officer (Articles 37–39):** Although not in 24–30, it's worth noting: if a fintech's processing activities *require regular and systematic monitoring of data subjects on a large scale* or involve large-scale processing of special categories, GDPR mandates a Data Protection Officer (DPO) be appointed. Many large fintechs or those engaged in extensive profiling will fit this criteria. The DPO is an independent advisor/monitor of GDPR compliance within the org. While not asked in the question, this is part of accountability. For example, an AI-driven

credit bureau or payment platform in the EU would almost certainly need a DPO, who would, inter alia, oversee DPIAs and training.

- **Data Breach Response (Articles 33–34):** Again slightly beyond 24–30, but integral to accountability: controllers must notify the supervisory authority of personal data breaches within 72 hours (unless unlikely to result in risk) and notify data subjects if there's high risk. Fintechs being frequent cyber-attack targets must have incident response plans. A breach in an AI database (e.g., exposure of a trove of customer financial data used for model training) would trigger these duties. Enforcement for breach handling has been heavy (e.g., the UK ICO's proposed fines against British Airways and Marriott for breaches under GDPR). A fintech's accountability framework should integrate breach response drills and clarity on when/how to notify customers and authorities.

In essence, Articles 24–30 require that fintech companies *own* the responsibility for data protection. This goes beyond paper compliance – they should integrate GDPR requirements into corporate governance. A concept introduced by GDPR is demonstrable accountability – being able to show your work. Fintech regulators (and investors, and partners) increasingly expect to see evidence of things like privacy risk assessments, training logs, policy documents, and technical measures (encryption, access control lists, etc.). One case that illustrates the cost of poor internal compliance is the German real estate firm Deutsche Wohnen's fine (~€14.5 million) for not having a proper data deletion schedule or lawful archiving – basically an accountability lapse where data was kept unnecessarily in an archive system. That fine was one of Germany's first big GDPR fines and it was under Article 5 and 25 principles, not a breach. A fintech that similarly stockpiles data "just because our AI might need it in the future" can face similar trouble. Conversely, those that build compliance in (privacy by design, minimal retention, etc.) are less likely to err.

Finally, a crucial obligation deserving its own focus is the **Data Protection Impact Assessment (DPIA)** under Article 35 – especially relevant for high-risk AI systems.

vii. Data Protection Impact Assessments for High-Risk AI (Article 35 GDPR)

Article 35 GDPR requires controllers to perform a **Data Protection Impact Assessment (DPIA)** for any processing that is likely to result in a *high risk* to individuals' rights and freedoms, particularly when using new technologies. Given that AI in fintech often involves extensive profiling or sensitive decisions, DPIAs are a critical compliance step. They are essentially risk assessment reports that must be done

before launching the processing and should evaluate the necessity and proportionality of the processing, the risks to individuals, and measures to address those risks.

When is a DPIA mandatory? Article 35(3) provides examples of processing that always require a DPIA, which map closely to common AI-fintech activities:

- **Systematic and extensive evaluation of personal aspects via automated processing, including profiling, with decisions producing legal or similarly significant effects**

This directly covers things like automated credit scoring or eligibility assessments – essentially the Article 22 scenario. A bank or fintech that uses algorithms to evaluate customers (creditworthiness, insurance risk, etc.) triggers this criterion. The European Commission explicitly lists *"A bank screening its customers against a credit reference database"* as an example where a DPIA is required. That description fits automated credit checks or fraud scoring. So any fintech engaging in such profiling should conduct a DPIA.

- **Large-scale processing of special category data** (sensitive data like health, biometrics, etc.).

While most financial data isn't "special category" under GDPR, some fintech use cases might be: e.g., processing biometric IDs for onboarding (face scans, fingerprints) is processing of sensitive biometric data, or processing data about criminal convictions (Article 10 data) for compliance checks. If done at scale, a DPIA is needed. For instance, a payment app that uses facial recognition for payments would require a DPIA for that feature due to biometrics.

- **Systematic monitoring of a publicly accessible area on a large scale**

This is more about CCTV and similar, but in fintech context not typical – unless a fintech uses video analytics of people in branches or ATMs, etc. (Likely not applicable to most). Beyond these explicit cases, the GDPR and regulators have issued lists and criteria. The Article 29 Working Party (WP248) set out nine criteria (such as evaluation/scoring, automated decision-making, systematic monitoring, sensitive data, data processed on a large scale, matching datasets, vulnerable data subjects, innovative tech, and when processing prevents rights or service) – if a processing meets several of those, a DPIA is recommended. AI-driven fintech operations often hit multiple: they use innovative tech, do profiling, maybe involve vulnerable individuals (financially

vulnerable or those with low credit). Therefore, in practice, many AI fintech projects will require DPIAs. Data Protection Authorities in the EU also have published blacklists and whitelists for DPIA. For example, France's CNIL mandates DPIAs for processing credit scores or payment defaults; the UK ICO requires DPIAs for profiling that affects people's access to services, etc. Fintech use cases commonly appear in these lists (credit scoring, fraud monitoring, wealth profiling have been cited). So the safest course is whenever a new AI system is being introduced in a fintech context, perform a DPIA.

viii. Security of Personal Data (Article 32 GDPR)

With great troves of financial data comes great responsibility to protect it. Article 32 GDPR mandates that controllers and processors implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. For AI-driven fintech firms, strong security safeguards are crucial not just to comply with GDPR, but to maintain customer trust in digital financial services. It's risk-based: Companies must consider "the state of the art, the cost of implementation, the nature, scope, context and purposes of processing, and the risk to individuals' rights" when deciding on security measures. A high-volume fintech handling sensitive personal and financial information must implement industry-leading security, whereas a small low-risk processing might get by with less. Given fintech data often includes bank account details, transaction histories, national IDs, and sometimes passwords or biometric identifiers, the risk is typically high – warranting robust measures. AI systems can introduce additional risks (e.g. big aggregated datasets become honeypots for attackers; API endpoints serving AI models could be abused if not secured).

- **Pseudonymization and encryption of personal data**– FinTech's should encrypt personal data both at rest (databases, data lakes) and in transit (HTTPS, secure APIs). Strong encryption thwarts data breaches (GDPR considers encrypted data unreadable to attackers, so if encrypted properly, a breach may not even trigger notification under Art. 34). Pseudonymization (replacing identifying information with codes) is especially relevant in AI: companies often pseudonymize datasets used for model training so that analysts work with user IDs rather than real names or SSNs. This way, if the AI environment is compromised, the data isn't directly identifying without the key. Many payment processors also tokenize card numbers (a form of pseudonymization). These techniques align with both security and data minimization principles
- **Ability to ensure ongoing confidentiality, integrity, availability and resilience of systems**– This encompasses a broad range of IT security practices: access controls (ensuring only authorized staff or processes can access data –

confidentiality), data integrity checks and permissions (prevent unauthorized alteration of data, and logging changes), availability and resilience (uptime plans, redundancy, protection against data loss or attacks like DDoS). Fintech services must have strong uptime and disaster recovery because outages or data losses can directly impact customers' finances. From GDPR's perspective, losing personal data due to poor backups is a security failure. Resilience includes having fail-safes for AI systems – e.g., if an automated fraud detection system crashes, the system should default to secure behavior rather than let all transactions through unchecked.

- **Ability to restore availability and access in a timely manner if an incident occurs**– Regular backups, disaster recovery plans, and business continuity plans are implied. A fintech must be able to recover customer data and resume services after, say, a server crash or ransomware attack. Many financial regulators (outside GDPR) also require this, but GDPR reinforces it. For AI, if critical decision-making systems fail, there should be backups or manual fallback to avoid outright denial of service to customers.
- **Regular testing and evaluation of security measures**– This means penetration testing, vulnerability scanning, security audits, etc., should be periodically done to ensure safeguards remain effective as systems evolve. Fintechs, especially startups, frequently update their apps and algorithms; each change can introduce new vulnerabilities. GDPR expects a cadence of testing. Also, if using third-party AI services, one should assess their security. For example, if a fintech sends data to an AI credit scoring API, it should vet that API's security (is the connection encrypted? is the provider certified or audited?). Adhering to security certifications or frameworks (ISO 27001, PCI DSS for payments, etc.) can demonstrate compliance with Article 32 – indeed, Article 32(3) notes that approved codes of conduct or certifications can be used to prove security compliance
- **Ensure processing under authority**: Article 32(4) adds that anyone acting under the controller/processor's authority must only process data on instructions. This reiterates internal access control and employee training – staff should know they can't snoop or take data out of company systems. Fintechs should enforce this with technical controls (individual accounts, role-based access, no shared credentials, etc.) and legal measures (NDAs, employment contracts). Given many fintech breaches result from internal mistakes or rogue insiders, this is salient.

When fintech companies fail to protect data, GDPR enforcement follows. There have been numerous fines for poor security (often under Article 32) – e.g., a telecom in Greece fined because an unprotected server led to a breach of customer data; or the UK

ICO's heavy fines (under pre-GDPR law but illustrating the point) for failure to prevent known web vulns. Under GDPR, fines for security lapses fall under the *lower tier* (up to €10M or 2% of turnover) if it's categorized as violation of Article 32 obligations. But breaches can also lead to higher fines if the breach also violates principles (e.g., confidentiality is one of the Article 5 principles).

One fintech-specific enforcement: The Bank of Ireland case (2021) where the DPC fined the bank €463k resulted from a series of data breaches – the bank had inadvertently exposed personal info of over 50k customers via letters to wrong addresses and other errors. While some issues were human/process error, it signaled inadequate technical measures to prevent or quickly correct such mistakes (like address validation failures). The GDPR fine indicated that even partial security/control failings in financial institutions are taken seriously. Another case: Klarna (again) was not about an external breach, but the Swedish DPA noted Klarna's privacy notice failed to mention countries to which data was transferred and safeguards– that touches on Article 32(1)(d) in a way (safeguards for transfers also relate to security).

AI systems introduce security considerations such as adversarial machine learning (attackers trying to manipulate models by injecting malicious data) and model inversion (extracting personal data from trained models). While GDPR doesn't explicitly mention these, the principle of integrity and confidentiality means fintechs should guard against such AI-specific threats too. For instance, if offering a public credit scoring API, one must ensure an attacker can't query it in such a way to deduce someone else's data from the model. Pseudonymization and limiting model outputs can mitigate that.

Importantly, encryption is stressed in Article 32 and many DPA guidance documents, because it's a measure that can prevent harm even if data is accessed. For fintechs, full-stack encryption (client-side or end-to-end where feasible) might be a selling point. GDPR recitals (Recital 83) also mention encryption as an example of appropriate security. Finally, GDPR's security requirement is continuous: threats evolve, so fintechs should actively monitor and upgrade their security. Many use bug bounty programs, third-party audits, and automated monitoring of systems for intrusions – all recommended practices aligning with Article 32's mandate to *regularly assess* security.

In essence, Article 32 compels fintech companies to treat cybersecurity as a foundational aspect of their AI and data infrastructure. By doing so, they not only comply with law but protect their customers and their own business from potentially devastating breaches.

ix. Enforcement: GDPR Fines and Penalties (Articles 83–84)

GDPR has gained a reputation for its teeth – namely, the significant fines that regulators can impose for non-compliance. Article 83 lays out the general conditions for administrative fines, including the two-tier fine structure, and Article 84 allows member states to enact other penalties (like criminal sanctions) for infringements not already covered by fines. Understanding the enforcement mechanism is crucial for fintech firms, as many have already faced penalties for GDPR violations.

Two-Tier Fine Structure: Article 83 differentiates infringements by severity:

- **Lower tier (Art. 83(4))** – up to **€10 million** or 2% of the worldwide annual turnover (whichever is higher). This tier applies to violations of more *procedural or internal* obligations. For instance, infringements of obligations of controllers and processors under Articles 8 (child consent), 11, 25–39, 42, 43 fall here. For a fintech, this means if you fail in areas like privacy by design (Art. 25), security (Art. 32), breach notification (Art. 33–34), DPIA (Art. 35–36), DPO provisions (Art. 37–39), or processor contract requirements (Art. 28), you're in the 2%/€10M range. These are serious, but considered less directly impactful on individual rights than the core principles and rights. Many early GDPR fines to companies (especially SMEs) were in this category, like fines for not having a DPA with a processor or not doing a DPIA.
- **Higher tier (Art. 83(5))** – up to **€20 million** or 4% of worldwide turnover (whichever higher). This covers violations of the fundamental parts of GDPR: the basic principles of processing (Articles 5, 6, 7, 9), data subjects' rights (Articles 12–22), cross-border data transfer rules (Articles 44–49), and non-compliance with orders from a DPA. For AI fintech, this means if you breach principles like lawfulness, transparency or violate Article 5 (e.g., processing data you have no legal basis for, or retaining data excessively), or if you trample data subject rights (ignore access requests, refuse deletion without basis, etc.), you face the higher fines. Notably, issues around consent (Art. 7) and automated decision rights (Art. 22) fall in this tier, as they tie to fundamental rights. This is why cases like BBVA's failure to obtain valid consent or Google's lack of transparency/consent in ad personalization (fined €50M by CNIL in 2019) drew multi-million fines – they were categorized under violation of core principles and rights (transparency and consent are Art. 5 and Art. 6/7 issues).

Additionally, Article 83(2) outlines factors that authorities must consider when deciding fine amounts: the nature, gravity and duration of the infringement, number of

affected data subjects and harm suffered, intentional or negligent character, actions taken to mitigate damage, previous infringements, degree of cooperation with the DPA, categories of data involved, how the DPA learned of it (did the company self-report?), adherence to codes of conduct, and any other aggravating/mitigating factors (like financial gain from the infringement). For example, if a fintech's AI practice caused denial of service to thousands of customers and the company didn't act even after warnings, that's aggravated. If it quickly cooperated and fixed issues, that's mitigating. In the Danske Bank case about retention, the long duration of non-deletion (going back years) and large number of data subjects (millions) aggravated the situation, though the proposed fine was moderate perhaps due to cooperation. Regulators also consider if an infringement was deliberate or just sloppy. Repeated offenders get higher fines – say a fintech was warned or lightly fined once and then commits a similar breach, the next fine will escalate (GDPR allows considering past infractions across the EU, not just the same country).

Article 83(3) prevents stacking fines beyond the maximum for linked violations – if one action violates multiple provisions, they generally issue one fine (whichever highest cap applies). But they can cite multiple articles in the decision. For example, an AI misuse could be cited as violating Article 5 (principle), Article 6 (lawfulness), and Article 22 (automated decision rules) simultaneously, but the fine would be up to 4% not triple that.

Article 84 leaves room for member states to impose other penalties (like administrative sanctions not covered by Article 83, or even criminal penalties for certain GDPR breaches). Many countries have, for instance, made it a criminal offense to obstruct a DPA or to unlawfully re-identify pseudonymized data. But for companies, the administrative fines are the primary concern. One quirk: some countries (e.g., Denmark) require the DPA to route fines through police/prosecutors because their legal system treats them differently, but the end result is similar fines. In the Danske Bank case, the DPA had to *recommend* a fine and send it to police for formal action

Thus, GDPR remains highly relevant and in force for AI-driven fintech, and navigating its requirements is now part of the cost (and responsibility) of doing business in this data-rich, algorithm-driven sector. The debates and challenges continue to be worked out in courtrooms, regulatory guidelines, and boardrooms, but the direction is clear: AI in fintech must respect individuals' data rights and be auditable and accountable. Companies that embrace this will be better prepared as laws tighten around AI; those that ignore it face both legal penalties and loss of user trust.

2. Markets in Crypto-Assets Regulation (MiCA):

In 2023 the MiCA regulatory framework was adopted. The MiCA regulatory framework makes new rules for the field of crypto-assets and prevents complexities of current regulation causing fragmentation across the member states. The MiCA rules primarily focus of fintech's that are the main users of artificial intelligence to provide the likes of a crypto-asset wallet, exchange or an initial coin offering (ico) falling into the field of crypto-assets. The MiCA rules are set for consumer protection, market integrity and financial stability for the area of finance. The MiCA rules has placed upon AI driven fintech's that they will need to gain regulatory approval and comply with the MiCA rules when offering their services in the EU (European Commission, 2024) (EIOPA, 2024).

3. EU AI Act 2024:

As the proliferation of AI tools advanced across Europe, authorities realized the acute need for an appropriate legal framework that would guarantee sound AI introduction. The EU thus took the lead by adopting the AI Act in 2023, which aims to establish a risk-based approach to regulation, ensuring the protection of fundamental rights while promoting innovation. The AI Act, the first ever legislation to meaningfully and purposefully regulate AI systems in the world encompasses the creation, deployment and use of AI applications, including its use in the European Union (EU). The AI Act (which is yet to be implemented but was adopted in 2023) takes a risk-based regulatory approach to the uses of Artificial Intelligence, and is to be implemented fully by 2025. AI systems are arranged according to their possible threat to basic rights, health and safety. AI systems used for credit scoring, financial assessments and insurance pricing, for instance, are categorised as "high-risk," and must be closely examined prior to deployment including third-party conformity assessments and adherence to openness and human oversight requirements (Henderson, Scott, Moille, Dixon-Ward, & Popescu, 2024; EIOPA, 2024). Furthermore, forbidden under the AI Act are "unacceptable risks," such those allowing governments or businesses to create social scores (European Commission, 2024).

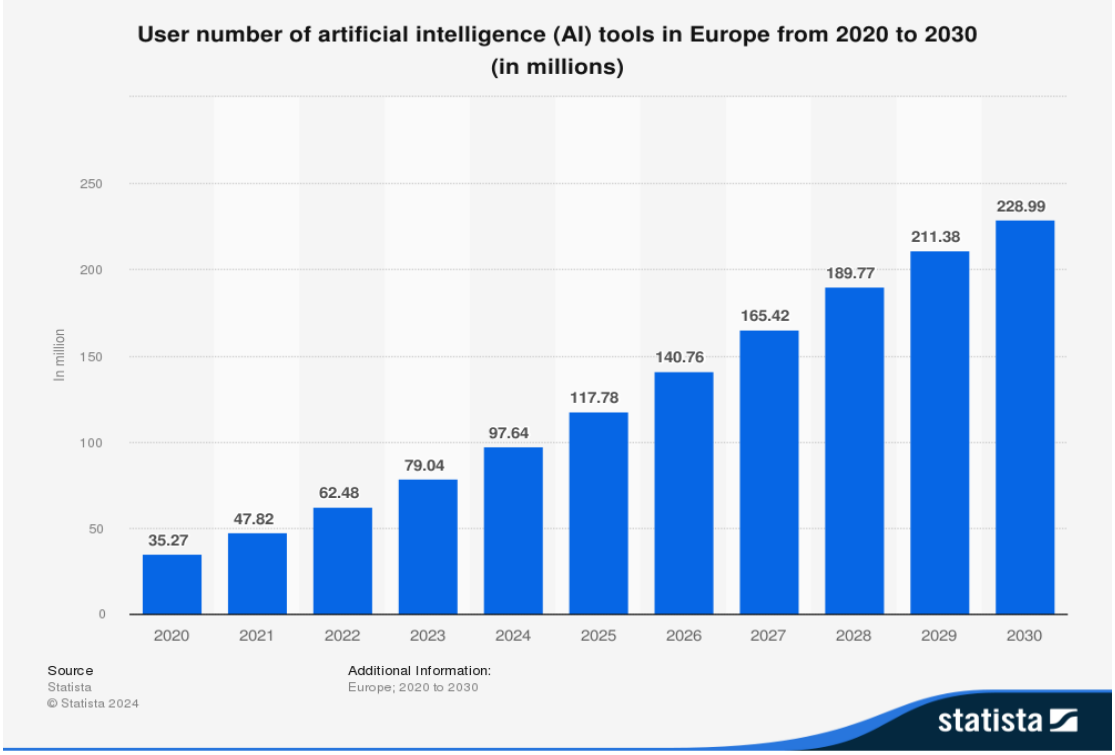

Figure 6.1: Usage of AI Tools in Europe

Source: Statista

The above figure explains the usage of AI Tools in Europe. Since the users are increasing, it also brings the potential cause of enacting AI Act. EU AI Act 2024 classifies AI systems by risk (unacceptable, high, limited, minimal) and imposes corresponding compliance obligations. In the financial domain, AI systems for creditworthiness assessment and insurance risk pricing are designated "high-risk" (Annex III), triggering strict requirements. Below is a detailed breakdown of key provisions and articles relevant to fintech, covering risk classification, transparency/explainability, human oversight, bias mitigation, and enforcement. It is also noted how these rules align with broader EU regulations like GDPR (data protection) and MiCA (crypto-assets regulation).

i. Risk Classification and Compliance Requirements for AI in Fintech

High-Risk Classification: The AI Act deems certain financial AI uses as *"high-risk"* due to their impact on individuals' rights and financial stability. Notably, AI systems used to evaluate consumer creditworthiness or to establish credit scores are classified as high-risk (Annex III, point 5(b)). Similarly, AI for life and health insurance risk assessment or pricing is high-risk (Annex III, point 5(c)). *Recital 37* explains that credit scoring AI "should be classified as high-risk" because such systems determine people's access to financial resources or essential services and may lead to discriminatory

outcomes if unchecked. By contrast, the Act explicitly carves out AI used solely for fraud detection from this high-risk category. In other words, an AI system assessing transactions for fraud *is not automatically treated as high-risk* under Annex III. (This carve-out was welcomed by financial institutions, though it's still expected that fraud detection AI comply with general requirements and sectoral law.)

Compliance Requirements: Providers and deployers of high-risk AI in fintech must meet a comprehensive set of trustworthiness requirements before and during deployment. Article 9–15 outline these obligations, which include:

- **Risk Management (Article 9):** Implement a continuous risk management process to identify, assess, and mitigate risks (financial, operational, ethical) posed by the AI system. For example, a bank deploying an AI credit scoring tool must evaluate risks to consumers (e.g. error rates, bias) and document mitigations.
- **Data Governance (Article 10):** Ensure high-quality datasets – training and test data should be relevant, representative, and free of errors or bias to minimize discriminatory outcomes. This means fintech AI models should be trained on accurate, unbiased data (avoiding historical prejudices) and comply with data minimization principles (using only data relevant to the decision), in line with GDPR's requirements.
- **Technical Documentation (Article 11) & Record-Keeping (Article 12):** Maintain detailed documentation about the AI system's design, logic, and performance, and log its operation for traceability. This documentation must enable regulators or auditors to **understand how the model works and verify compliance**, which is crucial in fintech where model transparency can be challenging (e.g. in complex credit scoring algorithms).
- **Transparency to Users (Article 13):** Provide clear information and instructions to the AI system's users (the deploying entity) about the system's capabilities, limitations, and intended use. For instance, a fintech provider must supply a bank with info on an AI loan approval model's expected accuracy, risk of errors, and guidelines for proper use, so the bank can use it appropriately and inform customers as needed.
- **Human Oversight (Article 14):** Design the AI system to allow effective human oversight and intervention. High-risk fintech AI cannot operate as a black box beyond human control – there should be mechanisms (or policies) enabling human controllers to monitor the AI's decisions and override or stop the system

if it behaves erratically or harmfully. (Details on oversight are expanded in section 3 below.)

- **Accuracy, Robustness, and Cybersecurity (Article 15):** Ensure the AI's performance is reliable. Fintech AI must meet appropriate accuracy standards, be robust against errors or adversarial manipulation, and include safeguards against cybersecurity threats. For example, an AI fraud detection tool should have protections against attackers manipulating its inputs, and an AI trading algorithm should be tested to avoid extreme erratic behavior that could threaten financial stability.

In practice, these requirements mean financial institutions or fintech firms using high-risk AI must implement rigorous controls and quality checks at each stage of the AI system's lifecycle. Before such an AI system can be put into use, an ex-ante conformity assessment is mandatory. This assessment (akin to a certification) verifies that the AI system complies with all the above requirements. Once compliance is confirmed, the provider affixes a CE marking to the AI system, signifying it meets EU standards. High-risk AI systems must also be registered in an EU database before deployment, increasing regulatory visibility and transparency. Importantly, the AI Act's risk-based compliance model aligns with existing financial regulations to avoid duplication. It leverages sectoral rules already applicable to banks and insurers. For example, EU banking law (CRD IV, Directive 2013/36/EU) requires banks to have robust governance and risk controls; the AI Act acknowledges that if a regulated credit institution complies with those existing rules, certain AI Act obligations are considered fulfilled or can be met through the same processes. Specifically, when a bank is a provider or user of a high-risk AI system, its established internal risk management and oversight frameworks can satisfy analogous AI Act duties. The Act explicitly allows that a bank's compliance with its prudential obligations can count for requirements like having a Quality Management System (Article 17) and ongoing monitoring of the AI system's performance. Likewise, obligations on record-keeping and logging (Articles 18, 20) and even the *post-market monitoring* and incident reporting duties (Articles 61–62) may be fulfilled via the bank's existing compliance and audit routines. This coordination ensures consistency with EU financial law and prevents double-regulation. It also designates financial supervisory authorities as key enforcers: Article 63(4) provides that the authorities overseeing EU financial services (e.g. banking and insurance regulators) shall also act as AI market surveillance authorities for high-risk AI in their sector. In summary, fintech AI systems that are high-risk must navigate both

the AI Act and relevant financial regulations, but the frameworks are designed to align and reinforce one another.

ii. **Transparency and Explainability in AI-Driven Financial Decision-Making**

Transparency Obligations: The AI Act mandates transparency at multiple levels to ensure AI-driven financial decisions are not made in secrecy. For high-risk systems, Article 13 requires that providers supply deployers (e.g. a fintech company or bank using the AI) with essential information about the system's operation. This includes clear instructions for use, the AI's intended purpose, its performance characteristics, and any known limitations or risks. In a credit scoring context, for instance, the AI system's developer must give the lender documentation describing how the model arrives at a score, what data it uses, how accurate it is, and under what conditions its output may be unreliable. Such transparency helps the deploying financial firm understand and responsibly integrate the AI into their decision-making processes.

Beyond technical docs, the Act also imposes public-facing transparency in certain cases. While much of fintech AI will fall under high-risk obligations (with internal transparency requirements), the Act additionally contains transparency rules for AI systems that interact directly with people (even if not high-risk). For example, an AI chatbot or virtual assistant used by a bank for customer service must disclose to users that they are interacting with an AI (a principle from Article 52 of the original proposal). Likewise, if an AI system generates content that could be mistaken for human-made (say, an automated advisory report or a synthetic voice call), it requires a disclosure so customers know it's machine-produced. These provisions ensure no "hidden AI" in consumer interactions, reinforcing trust. In summary, fintech firms deploying AI must be upfront about AI involvement in services – both to regulators (via documentation) and to users (via notices when appropriate)

Explainability and Consumer Rights: Transparency in the AI Act goes hand-in-hand with the goal of explainability – the ability to interpret and understand AI decisions. High-risk AI systems should be designed and deployed in a manner that allows humans to interpret the rationale behind outputs. This is crucial in finance: if an AI model denies a loan or flags a transaction as fraudulent, both the institution and the affected customer will seek an explanation. The AI Act's requirements (data transparency, documentation, human oversight) collectively push providers toward Explainable AI (XAI) techniques, so that meaningful justifications can be given for automated decisions. For instance, a bank using an AI credit scoring tool should be able to break down the main factors that led to a low score – rather than simply saying "the computer

says no." Researchers and regulators have emphasized developing interpretable models or post-hoc explanation methods to meet this need. The Act stops short of mandating a specific explainability technique, but by requiring provable risk mitigation and human review, it indirectly ensures that "black-box" models without any interpretability are discouraged in high-stakes uses. Crucially, the AI Act complements existing rights under the GDPR (General Data Protection Regulation) that give individuals a say in automated decisions. GDPR Article 22 already grants EU citizens the right not to be subject to solely automated decisions with significant effects (like credit denials) without certain safeguards, and it entitles them to request human intervention and an explanation of the decision. The AI Act reinforces this by making sure the technical ability to deliver such explanations exists. In practice, EU consumers will be informed when AI is used in credit or insurance decisions and can request explanation or human review. Recital 37 of the AI Act and related provisions underscore that when a bank assesses creditworthiness using AI, it must account for the impact on the person's fundamental rights and be prepared to explain the outcomes. Indeed, under the AI Act, individuals affected by a high-risk AI decision "must be able to receive an explanation of the decision and have the right to lodge complaints" with supervisory authorities. For example, if a borrower is rejected by an AI-driven process, they should be told that AI was used and be given an avenue to ask for clarification on what factors led to the negative outcome. Financial firms will thus need to implement processes to provide meaningful explanations to customers about AI-driven decisions, bridging the gap between complex algorithms and consumer understanding. This transparency and explainability focus aligns the AI Act with broader EU principles of fairness and accountability in automated processing, as seen in the GDPR and consumer protection laws.

iii. **Human Oversight and Accountability Measures in Fintech AI Applications**

Human-in-the-Loop Oversight: The AI Act places heavy emphasis on keeping human oversight at the core of high-risk AI systems (Article 14). Providers must design systems so they can be effectively overseen by people, and deployers must use them in a manner that humans remain in control of critical decisions. In fintech use-cases like loan approvals or fraud detection, this means AI does not get the final say without the possibility of human review. Article 14 specifies that appropriate measures (automated alerts, manual override options, etc.) should enable human controllers to monitor AI outputs and intervene if necessary to prevent harm or errors. For instance, if an automated insurance underwriting AI starts denying an unusually large number of claims or flagging an atypical number of legitimate transactions as fraud, human

supervisors should be able to notice this and step in to adjust or suspend the AI's operation. The goal is to avoid unchecked "black box" decisions – a human should *ultimately* be accountable for decisions affecting customers.

Organizational Accountability: The Act also spells out concrete obligations for deployers (users) of high-risk AI to ensure oversight. Financial institutions using such AI must assign human personnel with appropriate training and authority to supervise the system's functioning. These humans in charge should understand the AI's output well enough to challenge or override it in questionable cases. According to the Act, deployers are required to: use the AI system in accordance with the provided instructions*,* continually monitor its performance*, and* keep logs of the AI's activity for auditability. They must also inform the AI's provider or regulators of any significant incidents or risks identified during operation. In practice, a fintech firm might establish an internal AI oversight committee or assign responsible AI officers who review the outcomes of algorithms (say, reviewing a sample of credit decisions regularly to catch biases or errors). The Act insists that those overseeing the AI are not just figureheads – they must have the "necessary competence, training and authority" to properly supervise the system. This may involve upskilling staff (AI literacy training) and ensuring that management empowers them to pause or modify AI processes when warranted.

Accountability for Outcomes: The presence of human oversight ties into legal accountability. Under the AI Act, responsibility for AI outcomes squarely rests on the provider and the user of the system, not on the technology itself. Financial firms cannot deflect blame by saying "the AI made a mistake" – they are expected to prevent and correct AI errors as part of their oversight duties. To reinforce this, the Act introduces a requirement for a Fundamental Rights Impact Assessment (FRIA) for high-risk AI (Article 27). Fintech companies must assess how using the AI could affect individuals' rights (privacy, non-discrimination, etc.) *before* deployment and take steps to mitigate any adverse impacts. This proactive assessment increases management accountability, ensuring that issues like bias or unjust outcomes are considered at the design stage. Furthermore, the Act's enforcement scheme holds both providers and users liable for non-compliance. If a bank or fintech deploys an AI system without proper oversight or in violation of the rules, they can face regulatory sanctions (including fines) just as AI providers can. In other words, the duty of care extends through the entire AI value chain – developers must build compliant, controllable AI, and financial institutions must use it responsibly under human supervision. This dual accountability echoes the GDPR's approach of joint controller/processor responsibility and ensures there is always a

human answerable for how an AI in finance operates. The outcome is a higher level of trust: regulators and customers can be confident that *"humans remain ultimately accountable"* for AI-driven financial decisions, satisfying ethical requirements and legal standards for due diligence.

iv. Bias Mitigation and Fairness Provisions (Credit Scoring & Fraud Detection)

Data Quality to Prevent Bias (Article 10): The AI Act directly addresses the risk of biased AI outcomes, which is a paramount concern in credit scoring and fraud detection. Article 10 on data governance requires that training data sets for high-risk AI are sufficiently representative and inclusive to avoid discrimination against protected groups. This means a fintech AI model should not be trained on skewed data that, for example, over-represents one gender or excludes certain ethnic minorities, as that could lead to systematically biased decisions (e.g. higher loan rejection rates for certain demographics). Providers must analyze their data for imbalances or errors and correct them before deployment. They also need to ensure any personal attributes used are relevant and justified for the decision – reflecting GDPR's principle that you should only process data necessary for the purpose. Using sensitive attributes (race, religion, health, etc.) in AI decisions is heavily restricted by GDPR and typically would violate non-discrimination laws, so AI Act compliance goes hand-in-hand with those rules. In short, the Act demands a "bias check" at the dataset level, forcing firms to think critically about how their AI might replicate or amplify historical prejudices and to document measures taken to counteract that.

Fairness in Outcomes: The classification of creditworthiness AI as high-risk was largely due to fairness concerns. *Recital 37* explicitly notes that such AI systems can "lead to discrimination of persons" if not properly controlled. Thus, the Act embeds fairness as a key performance criterion: high-risk AI must be designed and tested to ensure equal performance across demographic groups and avoid unjust bias. For credit scoring, this could involve testing the model's error rates or approval rates for different groups (e.g. comparing outcomes for different ages, genders, or regions) and demonstrating no unfair disparity. If biases are found, the provider should tune the model or use techniques like algorithmic debiasing to mitigate them. Article 15 (on accuracy and robustness) implicitly covers fairness too – a system that is consistently less accurate for a minority group would not meet the robustness and accuracy requirements. In fraud detection, while these AI systems aren't classified as high-risk by default, the expectation of fairness still applies under general principles (and any

extreme biases could trigger regulatory scrutiny under consumer protection or anti-discrimination laws). For instance, an AI anti-fraud system used in payments should not unfairly flag transactions just because the customer's name or origin is from a high-fraud region, without a legitimate basis. Financial firms are encouraged to apply bias mitigation tools and rigorous testing for fairness in these AI models. Indeed, the Act prohibits "discriminatory outcomes" in a broad sense – it would violate fundamental rights requirements if an AI system's output constituted unequal treatment of individuals based on protected characteristics.

Ban on Social Scoring and Unfair Profiling: The AI Act outright bans certain AI practices (Article 5) deemed unacceptable, one of which is social scoring. "Social scoring" systems – AI that evaluates or ranks people's trustworthiness based on their behavior or personality traits in a broad context – are prohibited. This ban is highly relevant to fintech fairness: it prevents financial service providers (or public authorities) from using composite indicators of "social" behavior to make decisions like lending or insurance pricing. For example, an AI that scrapes a person's social media or purchasing history to produce a generalized "social credit score" that could deny them financial services would be illegal in the EU. The rationale is to avoid digital profiling that punishes or rewards individuals in ways that undermine human dignity or equal treatment. Financial institutions must therefore stick to relevant financial data and risk factors in their AI models – any attempt to incorporate extraneous personal behavior metrics could be seen as a form of social scoring or unjustified profiling. Additionally, the Act's provisions were influenced by concerns of algorithmic discrimination. The legislative debate saw regulators like the European Banking Authority (EBA) and European Insurance and Occupational Pensions Authority (EIOPA) stress that AI in credit or insurance should not replicate unlawful bias and that existing fairness and consumer protection rules (like the Equal Treatment Directives or credit anti-discrimination laws) remain fully applicable. In response, the final text includes cross-references to fundamental rights and sectoral laws, making clear that compliance with the AI Act includes ensuring alignment with EU non-discrimination standards.

In summary, the AI Act pushes fintech AI developers to prioritize **fairness at every stage: from input data curation to model training and deployment monitoring**. Credit scoring algorithms must be transparent and justifiable, treating applicants fairly and providing explanations that are free from biased reasoning. Fraud detection tools, while exempt from high-risk classification, should still follow industry best practices for fairness and **avoid disproportionate impacts on any one group**. These measures are reinforced by GDPR (which mandates fairness in processing and can penalize

processing that leads to discriminatory effects) and by financial regulations that require credit decisions to be based on creditworthiness, not irrelevant factors. The AI Act essentially operationalizes these principles into technical requirements, making **bias mitigation a legal compliance item** for AI systems – a significant step toward **"algorithmic fairness"** in financial services.

v. Regulatory Reporting and Enforcement Mechanisms for AI in Financial Services

Incident Reporting and Monitoring: The AI Act establishes ongoing oversight through reporting obligations. Providers of high-risk AI systems must perform post-market monitoring (Article 61) – essentially a continuous evaluation of the AI once it's deployed, to see if it behaves as expected or if new risks emerge. If a serious incident or malfunction occurs (for example, an AI trading system that causes a major loss due to a glitch, or an AI credit system that erroneously rejects a large number of eligible applicants due to a hidden bug), the provider is required to notify authorities within strict timelines**.** Article 73 specifies that any serious incident linked to a high-risk AI must be reported to national market surveillance authorities "immediately, and no later than 15 days" after the provider or user becomes aware of it. In especially critical cases (e.g. widespread issues or incidents causing death or serious harm), the Act shortens this to as little as 2 days for reporting. For a fintech example, if an AI-powered fraud detection system in a bank falsely labels a large volume of legitimate transactions as fraud (potentially disrupting many customers), the bank (as deployer) and the AI provider should escalate this to regulators quickly and investigate the root cause. They must also share findings and cooperate with authorities during any investigation. These reporting duties parallel those in other financial regulations (for instance, under the Digital Operational Resilience Act, significant ICT incidents must be reported). By capturing AI incidents, regulators can analyze trends, issue guidance, or require fixes to prevent systemic issues – a proactive enforcement approach.

Supervision and Authorities: Enforcement of the AI Act in financial services will largely be carried out by the same bodies that oversee financial markets, ensuring integrated supervision. As noted, Article 63(4) directs that sectoral regulators (like central banks, financial supervisory agencies) be appointed as the AI market surveillance authorities for their domain. This means, for example, that a national banking supervisor or the European Central Bank (for significant banks) will monitor compliance of AI systems used by banks, alongside their regular prudential supervision . These authorities can conduct inspections, request documentation (which firms are

obliged to provide per Article 21), and test AI systems for compliance. If non-compliance is found, they have powers to order corrective actions or even prohibit the use of the AI system until issues are fixed (similar to how unsafe products can be pulled from the market). The Act is enforced in a "product safety" style manner (under the framework of the EU Market Surveillance Regulation 2019/1020), meaning regulators can impose measures like fines and require recalls or updates to non-compliant AI. Additionally, individuals who feel harmed by an AI decision have the right to lodge complaints with these authorities, much as they can file complaints with data protection authorities under GDPR. For example, a consumer who suspects a lending AI discriminated against them can complain to the national AI regulator or financial ombudsman, prompting an inquiry into that AI system's compliance.

Penalties: The AI Act introduces a tiered penalty regime that mirrors the GDPR's heavy fines, underscoring how seriously the EU takes AI compliance. For the most egregious violations – using AI for prohibited practices (e.g. social scoring or illicit manipulation) – fines can reach €35 million or up to 7% of the company's global annual turnover (whichever is higher). This is even higher than GDPR's maximum (4%/€20M), reflecting the high stakes of AI misuse. For non-compliance with high-risk AI obligations (e.g. failing to implement the required risk controls, data governance, transparency, etc.), the Act provides for fines up to €15 million or 3% of global turnover . This would apply if, say, a fintech company deployed an AI credit scoring system without undergoing a conformity assessment or without ensuring data quality and human oversight – both the provider and the user of the system could face these penalties for negligence. Lesser offenses, such as supplying incorrect information to regulators or failing to cooperate, can incur fines up to €7.5 million (or 1% of turnover) . Importantly, users (deployers) of AI are also directly liable under the Act, not just AI vendors. A bank that uses a high-risk AI in violation of the rules (for instance, ignoring the provider's usage instructions or not monitoring outcomes) can be fined for that misuse. This shared liability model ensures everyone in the AI supply chain is incentivized to uphold the standards. The Act also contemplates adjustments for SMEs – fines for smaller enterprises may consider the lower of the percentage vs. absolute cap, to avoid disproportionate punishment.

The GDPR, MiCA and AI Act together provide a multifarious regulatory environment that guarantees the ethical, transparent and safe use of artificial intelligence in the fintech sector while so encouraging innovation and safeguarding of consumer rights.

6.4.2 Focus Areas of EU Regulation: Data Protection, Consumer Protection and Financial Stability

Three main elements define the regulatory approach of the European Union regulating artificial intelligence and fintech: data security, consumer protection and financial stability. By focusing on these areas of attention, it will guarantee a safe and open, in line with EU value and EU citizens rights' AI application in the financial services.

1. Data Protection

Of special interest to the EU focussed monitoring is industry compliance with the EU's General Data Protection Regulation (GDPR), legislated in 2018 to put strict measures in place to deal with the collection, manipulation and storage of personal data, an area of over-riding concern for AI led fintech's. Artificial intelligence algorithms used in credit scoring or consumer profiling, also in financial services working with private data, would have to comply to the GDPR's that address privacy. In order to assist users in maintaining control of their information, this law necessitates a degree of openness, which demands developers to ensure transparency of access and utilization of data, clear consent for data collection and storage along with the option for withdrawal of this consent. As it applies to financial firms which utilize artificial intelligence to handle massive amounts of data, it is of the utmost importance that data privacy isn't violated in any circumstances, as within recent years, the ramifications of such actions have translated to significant fines (European Commission, 2024).

2. Consumer Protection

With recognition of the increasing use of artificial intelligence in financial sectors, the EU has also made great progress in consumer protection. While MiCA (Markets in Crypto-Assests Regulation) to assure the customers safety in the crypto-assets market, which usually are driven by AI algorithms, DSA (Digital Services Act) demands more transparency on online platforms and AI-based services to black list the behaviours, which put customers in danger, and to have more transparency in terms of financial products, which usually are driven by AI. Financial decision-making artificial intelligence systems should not exploit consumer vulnerabilities; any decisions influencing consumers' financial situation—such as computerised credit scoring or loan approvals—must be just and logical.

3. Financial Stability

Financial stability is another crucial objective of EU control, especially in view of the development of fintech solutions driven by artificial intelligence that disclose new

hazards to financial markets. Here, the AI Act is rather significant since it distinguishes some AI applications as "high risk," particularly those used in insurance pricing, credit scoring and financial risk analysis. These high-risk artificial intelligence systems have to be completely conformable to ensure they do not jeopardise the stability of the financial system. Laws such as the Digital Operational Resilience Act (DORA) also ensure that banking sector artificial intelligence systems remain robust to resist disruptions, therefore lowering systematic risks (European Commission, 2024).

The EU's emphasis on data protection, consumer protection and financial stability guarantees that artificial intelligence in fintech runs inside a well-regulated environment, therefore combining innovation with safety and ethical issues.

6.4.3 AI in Fintech: Regulatory Gaps and Challenges in the EU

Although the EU has moved significantly towards controlling artificial intelligence in fintech using important frameworks like the AI Act and GDPR, some legal loopholes create difficulties especially considering the explosive speed of AI-driven developments.

1. Speed of Innovation versus Legislative Response

One of the main difficulties is that the fast-developing AI technologies in fintech outpace the legislative framework. Although the AI Act offers a risk-based regulatory framework and is expected to be fully adopted by 2025, fintech innovations as distributed finance and algorithmic trading keep developing faster than laws can change. This delay underregulates some artificial intelligence applications, especially those using machine learning algorithms for financial trading, therefore posing possible hazards for market integrity and financial stability (European Business Organisation Law Review, 2024). One such issue that is insufficiently addressed by present rules is the procyclical behaviour of algorithmic trading systems, whereby identical AI-driven trading tactics increase financial risks (Lee, 2020).

2. Sector-Specific Regulatory Guidelines

Although the AI Act offers overall control, the financial industry lacks particular rules for AI uses. AI systems applied in credit scoring, fraud detection, or investment advice, for instance, can bring algorithmic bias or discriminatory outcomes—which are not sufficiently controlled by present systems—for which there is need for regulation (Goodwin Law, 2024). Without sector-specific rules in fintech, some high-risk areas—

including peer-to-peer lending platforms and robo-advisory systems—are left open to possible legal uncertainty and under-regulation (Yordanova & Bertels, 2024) (Omarova, 2020)

3. Cross-Border Regulation and Fragmentation

The scattered rules across various EU members present still another major obstacle. Notwithstanding efforts at regulatory harmonisation by the EU, member states may see and apply artificial intelligence-related rules differently. For fintech businesses functioning internationally, particularly in areas like distributed finance and cross-border payments, this generates regulatory friction. Regulatory fragmentation can make fintech technologies less scalable inside the EU and raise compliance costs for businesses (Yordanova & Bertels, 2024) (Lee, 2020).

4. Challenges in Monitoring and Enforcement

Implementing AI rules still presents a difficult task. The AI Act labels some artificial intelligence systems—such as those used for credit scoring and risk assessments—as "high-risk" and imposes strict compliance rules upon them. But notably for smaller fintech companies who might lack the means to fulfil these legal requirements, enforcement systems are sometimes lacking. Furthermore, authorities could find it difficult to properly oversee AI systems technologically (Henderson, Scott, Moille, Dixon-Ward, & Popescu, 2024) given their technological complexity. Stronger enforcement of these high-risk systems' compliance with transparency, fairness and data protection requirements can help to ensure these things (EIOPA, 2024) (Yordanova & Bertels, 2024)

5. Ethical Considerations and AI Transparency

Furthermore lacking in attention is the ethical connotations of artificial intelligence in fintech. While the GDPR addresses data protection, AI system transparency still presents a problem. Financial decision-making artificial intelligence models—such as loan approvals or fraud detection—often function as "black boxes," where it is challenging for both consumers and authorities to grasp how judgements are taken. Maintaining customer confidence and avoiding unfair or biased results depend on these artificial intelligence systems being transparent and accountable (European Commission, 2024) (Omarova, 2020).

6.5 REGULATORY OVERVIEW IN THE US

The regulatory landscape for AI in fintech in the US is a complex mix of federal and state-level regulations, balancing innovation, consumer protection, and financial stability. Key federal laws, such as the Bank Secrecy Act (BSA) and regulations enforced by the Federal Trade Commission (FTC), focus on financial integrity, fraud prevention, and data security. However, the fragmented state-level regulations, including the California Consumer Privacy Act (CCPA) and New York's BitLicense, create compliance challenges for fintech firms operating across multiple jurisdictions. While the US prioritizes innovation-friendly policies, gaps remain in AI explainability, algorithmic bias mitigation, and unified oversight, necessitating a more coordinated federal approach to AI regulation in financial services.

6.5.1 Key Legislation Governing AI and Fintech in the US

Federal and state rules, each striving to balance innovation, consumer protection and financial stability, control the regulatory environment for artificial intelligence and fintech in the United States. Among the important federal rules and authorities engaged in this field are the Bank Secrecy Act (BSA), Federal Trade Commission (FTC) and several state-level laws.

1. Bank Secrecy Act 1970 (BSA) and Anti-Money Laundering (AML) Regulations

Approved in 1970, the Bank Secrecy Act (BSA) is among the main federal statutes used to fight financial crimes and money laundering. It calls on financial institutions—including technology startups managing payments and cryptocurrencies—to help government agencies spot and stop money laundering. In fintech, where artificial intelligence is applied in digital wallets, payments processing and bitcoin transactions, this is very crucial. Fintech businesses under the BSA have to create rigorous compliance processes to track dubious behaviour and notify the Financial Crimes Enforcement Network (FinCEN). Ensuring that artificial intelligence-driven financial systems do not support illicit activities like fraud or money laundering depends critically on the BSA (Song, 2021)

2. Federal Trade Commission 1914 (FTC) Involvement

Focussing mostly on consumer protection and fair competition, the FTC is essential in the control of artificial intelligence and fintech. Relevant to fintech businesses, the FTC enforces many consumer protection regulations like the Gramm-Leach-Bliley Act (GLBA) which controls consumer financial information exchange and the Fair Credit

Reporting Act (FCRA). Particularly with regard to data protection and fraud, the FTC also takes enforcement proceedings against fintech companies who break these rules. The FTC has lately increased its efforts to control AI-related misleading behaviour including algorithms that disfavour customers or misleading AI-generated financial advice. The FTC's involvement guarantees that financial technologies driven by artificial intelligence answer for their effect on consumer rights and data protection (Stackhouse, 2019; Scott, 2020).

3. State-Level Regulations

Apart from federal supervision, state-level rules add still another degree of complexity to fintech governance in the US. The New York State Department of Financial Services (NYDFS) and the California Department of Financial Protection and Innovation (DFPI) are two states with agencies that monitor state-chartered banks, non-bank financial institutions and fintech startups. Regarding consumer protection, money transmission and licencing, these state bodies guarantee respect to state-specific legislation. For instance, since New York controls the operations of fintech companies involved in virtual currency exchanges, its BitLicense requires strong anti-money laundering and cybersecurity policies. Many state-level regulatory regimes can result in regulatory fragmentation, which poses difficulties for fintech companies operating in numerous jurisdictions (Pandev, 2024).

Federal and state rules taken together define the US regulatory environment for fintech and artificial intelligence. Although local compliance is guaranteed by state agencies such as NYDFS and DFPI, consumer protection provisions of the Bank Secrecy Act and FTC are vitally essential in lowering financial crimes and protecting consumer rights. Taken collectively, these guidelines aim to strike a balance in the quickly evolving finance environment between ensuring justice and safety and fostering creativity.

6.5.2 State-Level Legal Variations in the USA: Implications for AI in FinTech

Because of the United States having a dual governance structure consisting of federal and state jurisdictions, the regulatory framework for AI in FinTech in the United States is highly complex and fragmented. Though there is not any national federal law regarding the AI for financial technology field, many states have passed some regulations around AI for financial services or have some proposals regarding AI in financial services. Although this landscape is fragmenting, it is essential to understand

that this is of significant advantage and often disadvantage to AI driven Fintech solutions operating across the country.

At the state level, important law includes the California Consumer Privacy Act (CCPA) and the expansion of the legislation via the California Privacy Rights Act (CPRA). This law particularly targets data privacy and transparency and is very strict, even provided for data protection and transparency for automated decision-making systems.

CCPA (2018) Key Provisions:

- **Section 1798.100:** Grants consumers the right to know what personal information businesses collect.
- **Section 1798.105:** Provides the right to request the deletion of personal data.
- **Section 1798.120:** Allows consumers to opt out of the sale of their personal information.
- **Section 1798.150:** Grants consumers a private right of action in case of data breaches.
- **Section 1798.121:** Introduces the right to restrict the use of sensitive personal information.
- **Section 1798.185:** Establishes the California Privacy Protection Agency (CPPA) to enforce data privacy laws.
- **Section 1798.140:** Defines **"automated decision-making technology"**, requiring businesses to disclose its use and allow consumers to opt out of automated profiling.
- **Section 1798.185(a)(16):** Mandates businesses to provide consumers with clear information about **AI-driven automated decision-making systems**, ensuring transparency and accountability.

These provisions significantly enhance consumer control over personal data, extend regulatory oversight, and establish clear obligations for businesses leveraging **automated decision-making systems**. However, Texas, along with Florida, has less strict privacy regulations, which allow more flexibility but create discrepancies for FinTech companies operating on a country wide level.

Innovative regulatory approaches have come to the fore. For example, Arizona has put in place a FinTech Sandbox to foster innovation and whereby allows companies to test AI-driven financial products with some light-touch regulation. For the same reason, the great state of Wyoming has set the bar for blockchain-friendly legislation, recognizing

decentralized autonomous organizations (DAOs) and enabling smart contract applications which often integrate AI. Nevertheless, states like New York, have introduced difficult licensing regimes, such as the BitLicense which influenced AI applications in cryptocurrency and blockchain technologies. As a result of this, staying in accordance with regulations in FinTech becomes increasingly difficult as firms scale from state to state, constituting the need for a specific compliance strategy for each individual state. Although certain states, for example California and New York, foster consumer protection and work hard to have strong oversight, there are others who seem to give more preference to innovation and embracing diverse economic development. This mishmash of rules reflects the broader issue of how to regulate AI and FinTech, globally a subject on whether to seek regulation innovation or regulation itself.

A number of other states have enacted legislation or are promoting initiatives that, while not specifically focused on AI, indirectly impact its application within FinTech. They are:

1. **Massachusetts:** Strong consumer protection laws affect AI-driven lending and credit practices. Proposed initiatives aim to regulate algorithmic bias in financial services.

2. **Connecticut:** The **Connecticut Data Privacy Act (CDPA)** includes provisions for automated decision-making and transparency, aligning with frameworks like the CCPA.

3. **Utah:** The **Utah Consumer Privacy Act (UCPA)** impacts AI applications by regulating data processing and requiring transparency in automated systems.

4. **Washington:** Proposed AI-related bills focus on transparency and accountability in automated decision-making, especially regarding consumer data.

5. **Maryland:** Ethical AI bills target government and consumer-facing technologies, indirectly affecting AI-driven FinTech solutions.

6. **North Carolina:** Regulatory discussions on blockchain and AI integration, driven by Charlotte's FinTech hub, emphasize innovation in decentralized systems.

These developments illustrate the growing momentum toward regulating AI applications, despite the absence of a unified, comprehensive framework.

6.5.3 Focus Areas of US Regulation: Emphasis on Innovation, Consumer Protection and Anti-Money Laundering (AML) Efforts

In the USA task of building a fintech regulatory framework was divided into three components which increase creativity blooming whilst protecting its user, long with the fact that it must eventually comply with the anti-money laundering (AML) legislation. These areas of concentration consist:

1. Innovation

The regulatory landscape in the U.S. is focused on promoting innovation in the fintech industry so that emerging technologies such as artificial intelligence, blockchain, and digital financial services can flourish in a conducive environment. Federal agencies and even the Office of the Comptroller of the Currency (OCC) have established programs. These programs are known as innovation programs, and one popular type of innovation program is a responsible innovations framework. FedNow, which offers actual-time payment systems, is a way the Federal Reserve also lent a lot of support in enabling innovation in fintech. FeedNow allows consumers to be able to receive money immediately, rather than the regular transaction process by conventional banks. Furthermore, numerous U.S. states have created regulatory sandboxes to inspire fintech startups to create and test new technologies under a less strict regulatory environment prior to complete compliance being needed (Pandev, 2024)

2. Consumer Protection

The Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) show how much U.S. fintech rules still centre consumer protection. While addressing concerns about openness and fairness in AI-driven fintech services like lending and credit scoring, the CFPB guarantees that fintech companies follow consumer protection regulations such the Fair Credit Reporting Act (FCRA) and Truth in Lending Act (TILA). Under laws such the Gramm-Leach-Bliley Act (GLBA), the FTC monitors privacy issues and makes sure fintech companies safeguard consumer data. Under the Electronic Fund Transfer Act, Regulation E also guarantees consumer safeguards for electronic transfers and remittances, therefore guaranteeing fintechs follow error-resolution policies and disclose fees (Scott, 2020).

3. Anti-Money Laundering (AML) Efforts

Particularly through AML rules controlled by the Bank Secrecy Act (BSA) and implemented by the Financial Crimes Enforcement Network (FinCEN), the U.S. regulatory framework gives great weight on stopping financial crimes. Particularly

those handling digital payments and cryptocurrencies, fintech organisations must establish strong compliance programs comprising Know Your Customer (KYC) processes, transaction monitoring and reporting of suspicious activity. Under the BSA, the travel rule requires fintechs to provide thorough sender and recipient information during specific financial transactions in order to help identify illegal activity. These rules guarantee that fintech innovation does not help with terrorist funding or money laundering (Pandey, 2024)

Ultimately, U.S. fintech rules strike a compromise between defending consumer rights and ensuring the financial system stays free from illegal activity, so balancing the demand to progress technology with protection of consumer rights. Regulators build a strong but adaptable framework by emphasising innovation, consumer protection and AML initiatives that lets the fintech sector grow while keeping necessary protections.

6.5.4 U.S. AI Bill of Rights (Blueprint for an AI Bill of Rights, 2022)

In October 2022, the White House Office of Science and Technology Policy (OSTP) released a "Blueprint for an AI Bill of Rights" as a framework to guide the design and use of AI systems in a manner that protects civil rights and consumer rights (The White House Office of Science and Technology Policy, 2022). This blueprint was developed in response to growing concerns that automated systems were increasingly used in sensitive areas – from banking and housing to employment and education – without adequate safeguards (The White House Office of Science and Technology Policy, 2022). Algorithms across many sectors had been found to exhibit bias or to operate opaquely, threatening the rights of millions (especially in historically marginalized communities) by surveilling, ranking, or making decisions without regard to their real-world consequences. The U.S. AI Bill of Rights thus sets out a principled vision for protecting the public from harms of AI, articulating five key principles (or "rights") that AI systems **should** respect in order to be trustworthy and fair.

- **Safe and Effective Systems:** Individuals should be protected from unsafe or ineffective automated systems, which must be thoroughly tested and monitored to ensure they are not causing harm. This entails risk assessment and mitigation to guarantee that AI tools (including those used in finance) are valid and reasonably error-free in their intended context.
- **Algorithmic Discrimination Protections:** Citizens should not face unjust discrimination by algorithms; AI should be designed and used in equitable ways that *proactively prevent* biased outcomes. Designers and deployers of AI are

called upon to take "proactive and continuous measures" to protect individuals and communities from algorithmic bias (Cooley LLP, 2023), including steps like ongoing disparity testing and independent evaluation of AI models for fairness (Cooley LLP, 2023).

- **Data Privacy:** People deserve built-in *privacy protections* and agency over how data about them is used. In practice, this means AI systems (including fintech applications) should incorporate data minimization, security safeguards, and user control consistent with modern privacy standards.
- **Notice and Explanation:** People have the right to know when an automated system is being used and to understand how it impacts them. Transparency is key: users should receive clear notice when AI influences significant decisions (such as credit determinations) and an explanation of the logic or factors driving those outcomes.
- **Human Alternatives, Consideration, and Fallback:** Wherever appropriate, individuals should be able to opt out of purely automated decisions, and have access to a human reviewer who can promptly consider and remedy problems. In other words, important decisions shouldn't be left with "black box" algorithms alone – there should be a human fallback to address errors or appeals.

Legal Status and Structure: Importantly, the AI Bill of Rights is a *policy blueprint* and not a binding law or regulation. It was issued as guidance by the Biden Administration and outlines non-enforceable principles rather than imposing new legal obligations. The document's approach is explicitly rights-oriented – focusing on core values of safety, fairness, and accountability – and it includes a technical companion with examples of how these principles can be put into practice across sectors. The Blueprint itself does not create new rights or override existing laws; instead, it is meant to inspire industry best practices and inform future policymaking. OSTP encouraged policymakers to consider codifying these principles or issuing sector-specific guidance based on them. Indeed, the influence of this framework can already be seen in subsequent federal initiatives (for example, a 2023 AI Executive Order builds on these principles) and in agency guidance. However, absent new legislation or regulations, the Blueprint remains advisory – a statement of ideals that lacks direct enforcement power (Turner Lee & Malamud, 2022). Analysts have noted that without congressional action to anchor these principles in statute, there is no "effective, credible enforcement regime" to ensure compliance. In essence, the AI Bill of Rights conveys the administration's expectations and vision for responsible AI, while relying on existing laws and voluntary adoption for effect.

Relationship to Existing Laws: Although nonbinding, the Blueprint aligns with and reinforces many obligations already found in U.S. law, especially in regulated sectors like finance. Federal regulators have made clear that *"advances in technology do not render existing … requirements or expectations inapplicable"* and that existing statutes and regulations generally apply to AI in the same way as to traditional processes. For example, the principles of the AI Bill of Rights closely mirror mandates under consumer protection and anti-discrimination laws in financial services. The call for algorithmic discrimination protections echoes the Equal Credit Opportunity Act (ECOA)'s core ban on lending discrimination. In fact, even before the Blueprint's release, regulators warned that improper use of AI could violate laws like "the Federal Trade Commission Act, the Fair Credit Reporting Act and the ECOA" if it leads to unfair or biased outcomes. Likewise, the Blueprint's emphasis on notice and explanation dovetails with existing requirements under ECOA and the Fair Credit Reporting Act (FCRA) that borrowers receive specific reasons for adverse credit decisions. The Consumer Financial Protection Bureau (CFPB) has affirmed that ECOA's adverse action notice rule "applies equally to all credit decisions, regardless of the technology used", meaning lenders cannot hide behind opaque AI models – they must be able to explain why a credit application was denied. This effectively prohibits the use of "black box" credit underwriting algorithms that cannot generate understandable explanations (Consumer Financial Protection Bureau, 2022), underscoring the Blueprint's point that transparency is a right even in automated decisions.

Implications for AI in Fintech: Although the AI Bill of Rights is broad and cross-sector, it has clear relevance for AI-enabled financial technology (fintech) use cases such as algorithmic lending, credit scoring, fraud detection, and digital banking services. In these domains, the Blueprint's principles provide a normative guide for regulators and firms to evaluate AI tools:

- **Algorithmic Lending & Credit Scoring:** The Blueprint's anti-discrimination principle has particular force in lending. AI-driven underwriting models must be designed to avoid disparate impacts on protected classes, reflecting long-standing fair lending laws. The White House explicitly cautions that designers of AI should "take proactive and continuous measures" to prevent algorithmic bias. This has prompted financial institutions to strengthen fairness testing of credit risk models (e.g. testing for racial bias in loan approvals) and to document measures that ensure credit algorithms are used "in an equitable way". Additionally, the notice/explanation principle means fintech lenders should

provide clear, intelligible reasons for credit decisions made by AI. This aligns with regulatory expectations under ECOA – for instance, if a machine-learning model declines a loan, the consumer is entitled to know the key factors (low income, high debt, etc.) that contributed to that outcome. The CFPB and other agencies have highlighted that the use of complex AI does not excuse lenders from these transparency obligations (Consumer Financial Protection Bureau, 2022). In practice, the AI Bill of Rights bolsters the regulatory stance that automated credit scoring and underwriting systems must be auditible and accountable, effectively shaping industry best practices for algorithmic lending and credit analytics.

- **Fraud Detection and Financial Crime Prevention:** Fintech companies and banks widely use AI for fraud screening, transaction monitoring, and identity verification. The Blueprint's call for "safe and effective systems" is especially pertinent here, as false positives or inaccurate models in fraud detection can unfairly block customers from accessing financial services. Regulators expect firms to rigorously validate AI fraud models to ensure they are accurate and do not disproportionately target or exclude certain groups without justification. The principle of human fallback also plays a role: if an automated fraud system flags a legitimate customer or transaction as suspicious, there should be a mechanism for prompt human review and correction. This is in line with emerging best practices in digital banking, where customers must be given an avenue to challenge automated freezes or denials (for example, speaking to a fraud analyst to resolve an account lockout). Moreover, the data privacy principle reinforces existing financial privacy rules by urging minimization of personal data use in AI-driven fraud tools and ensuring any data sharing (even for fraud prevention) respects consumers' consent and privacy rights. In sum, the AI Bill of Rights framework pushes fraud detection AI toward greater accuracy, fairness, and user accountability, complementing regulatory goals in anti-fraud and anti-money-laundering efforts.
- **Digital Financial Services and Advice:** Beyond credit and fraud, fintech encompasses robo-advisors, algorithmic trading, personal finance management tools, and more. The Blueprint's "safe and effective" standard implies that fintech AI models (for investment advice, insurance underwriting, etc.) should be thoroughly tested to avoid faulty outcomes that could harm consumers financially. Its data privacy tenet resonates with the Gramm-Leach-Bliley Act and other financial privacy laws, meaning fintech firms should build robust privacy safeguards as they deploy AI-driven services (Mallett, 2023). The

notice principle suggests that customers using digital finance apps have a right to know when AI is making decisions on their behalf – for example, a personal finance app should disclose if an "AI advisor" is categorizing transactions or making budget recommendations. And if such algorithmic services err (say, a robo-advisor makes a problematic trade), the human alternative principle would support giving clients recourse to a human customer service agent or the option to override automated decisions. While these practices are not yet uniformly required by law, the AI Bill of Rights provides a blueprint for what responsible AI in fintech should look like. Financial regulators have noted that its best-practice recommendations closely "align with" existing legal principles and consumer protection goals in finance.

The U.S. AI Bill of Rights represents a seminal policy statement on trustworthy AI, and it carries significant weight in shaping the regulatory narrative around AI in fintech. Its five principles – though not legally binding – serve as a benchmark for ethical AI deployment. Regulators at agencies such as the CFPB, FTC, and banking supervisors are using these principles to frame guidance and enforcement, ensuring that AI-driven financial technologies do not run afoul of anti-discrimination rules, consumer privacy rights, or safety standards. The Blueprint's influence is evident in the convergence of policy: existing financial laws are being interpreted in light of its themes, and new initiatives (like sector-specific guidelines or proposals in Congress) are drawing on its vocabulary of rights and protections. For fintech firms, the AI Bill of Rights effectively signals the future of AI governance – a future in which fairness, transparency, and accountability will be expected norms for algorithms that lend money, evaluate credit, detect fraud, or manage our financial lives. By articulating these norms now, the Blueprint is shaping a regulatory environment where innovative AI in finance must also be responsible AI, aligning technological progress with fundamental rights and values.

6.5.5 AI in Fintech: Regulatory Gaps and Challenges in the US

The U.S. regulatory framework for AI in fintech faces several gaps and challenges, largely stemming from inconsistencies between federal and state regulations, the rapid pace of AI innovation and difficulties in balancing innovation with effective oversight.

The U.S. fintech regulatory landscape is fragmented, with different federal and state authorities applying distinct sets of rules. At the federal level, agencies such as the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC) and Federal Reserve have jurisdiction over various aspects of fintech, but their approaches

are not always coordinated. Not only is this inconsistent, but it often results in regulatory uncertainty, especially for fintech firms operating across multiple states. For instance, the New York Department of Financial Services (NYDFS) has introduced its own set of state-level regulations, such as the NYDFS BitLicense for cryptocurrencies, which only adds another layer of complexity to the whole process and means more work and compliance for companies (Scott, 2020; Pandey, 2024).

The rapid pace of AI-powered fintech innovation is challenging for regulators to keep up with. Fast-evolving technologies which are used in fintech, such as algorithmic execution or blockchain, could be re-shaping the financial markets so fast as to make real-time regulation difficult. It is important for law authorities to control all the new technology for several reasons. Models are evolving quickly in areas such as fraud detection, credit scoring, and investment advising using techniques like deep learning and reinforcement learning, and the regulations have not fully addressed the risks that these new model pose. So, for example, there might be algorithmic biases in AI-based credit scoring and there clearly are some that have been pointed and have led to maybe discriminatory outcomes but there is no standard on how to approach that across the regulatory spectrum (Bahoo, Cucculelli, Goga, et al., 2024).

AI systems, above all those which implicate machine learning and neural networks, habitually work as “black boxes,” thereby to say that it’s decisions cannot be expressed in terms of simple if-then or rule-based logic. A lack of explainability is of concern which would make it challenging for regulators to evaluate whether these systems are in compliance with existing laws such as the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA) that are intended to protect consumer rights. Explainable AI (XAI) in finance is not yet fully understood but its importance is growing. There is no traces of regulatory guidance; it is however, a very important subject for all fin-techs as they look to understand how to make those AI models more interpretable.

This is where the United States prevails, their focus on innovation often comes with an expense for the consumer protection. Consumer Financial Protection Bureau (CFPB), a regulatory body, has been trying to ensure that the fintech’s who are using AI, are following the standards such as data privacy, consumer protection etc. Having said that, the contrary being possible, perhaps with fintech industry, they could break more regulatory norms and they could do more of the stuff of that might actually endanger the customers if they were being fintech and being much be in general to that of normal bank actually allowed those type of customers do like crypto currency training, bitcoin

for that matter given recent legislation, peer-to-peer lending and so forth. Additionally to further complicate this issue, there are no consistent and broadly accepted guidelines or oversight procedures with regards to AI and data manipulation or AI targeting vulnerable populations.

To find a solution for this regulatory gap in the fintech landscape in the United States it would need to be solved in a manner that is ordered and balanced in its regulations to allow for innovation. Regulatory approaches are to be synchronized at both the federal and state level, there is a need to raise awareness for the enormous potential of AI-driven fintech applications, and a means must be found to maximize consumer protectionism without nipping technology itself in the bud, or at an early stage of development.

6.6 REGULATORY OVERVIEW IN INDIA

6.6.1 Key Legislation Governing AI and Fintech in India

The DPDP Act, 2023 and the guidelines set out by the Reserve Bank of India (RBI) help facilitate the regulation mechanism in India for AI and the adoption of fintech. The importance of these legal instruments in assuring AI-driven financial innovation are converging with the data protections standards to the stability of the financial system.

1. Digital Personal Data Protection (DPDP) Act, 2023

The first-ever Act in India to provide protection to personal data by defining it within the framework of the digital ecosystem is The DPDP Act, 2023. The Act places extensive obligations on data fiduciaries (entities that collect data) and would likely be most relevant to AI-based fintech firms that deal with a lot of consumer data that is sensitive.

Key Sections Relevant to AI in Fintech

Section 4: Lawful Processing of Personal Data

- Requires fintech companies, including those using AI algorithms for credit scoring, fraud detection, and automated loan approvals, to obtain explicit user consent before processing personal data.
- AI models must adhere to data minimization principles, ensuring only the necessary amount of data is collected and retained.

Section 6: Notice and Consent Framework

- Fintech firms employing AI-driven financial advisory tools must inform users about the data being collected and obtain clear, affirmative consent before processing.
- AI models must be transparent, explaining their decision-making processes in cases like credit scoring and risk assessment.

Section 9: Rights of Data Principals (Users)

- Grants individuals the right to correction, erasure, and access to their personal data, crucial for AI-based fintech models that rely on automated decision-making.
- Users can challenge biased AI outputs if they believe their credit or financial assessment was unfairly determined by AI algorithms.

Section 10: Duties of Data Fiduciaries

- AI-powered fintech firms processing large-scale consumer financial data must implement robust security measures to prevent AI model bias, unauthorized data access, and cyber risks.
- Ensures accountability for automated decision-making that impacts financial transactions, loan disbursements, or investment recommendations.

Section 11: Significant Data Fiduciaries (SDFs)

- Allows the government to designate AI-driven fintech platforms as Significant Data Fiduciaries (SDFs) based on factors such as:
    - Volume and sensitivity of data processed
    - Impact on financial security and user privacy
- SDFs must appoint a Data Protection Officer (DPO) and conduct Data Protection Impact Assessments (DPIA) to ensure AI compliance with privacy laws.

Section 16: Cross-Border Data Transfers

- AI-driven fintech firms leveraging international AI models for financial predictions or fraud detection must comply with India's cross-border data transfer restrictions.

- Limits sending sensitive financial data to AI processing hubs in foreign jurisdictions without regulatory approval.

Section 19: Penalties for Non-Compliance

- AI-powered fintech firms failing to ensure data privacy, consent management, or transparency can face penalties of up to ₹250 crores.
- This applies to AI-driven automated lending platforms that engage in biased decision-making, excessive data collection, or unauthorized profiling.

The DPDP Act emphasizes three criteria such as consent-based processing, purpose limitation, and data minimization. The Fintech companies such as those using Artificial Intelligence in personalized financial services have to take the explicit consent from its customers before processing their data and need to ensure transparency with respect to the handling of data (Burman, 2023). Additionally, there is a provision under the DPDP Act that allows the government to designate certain entities as Significant Data Fiduciaries (SDFs) based on certain factors such as volume and sensitivity of data processed. Moreover, these organisations are additionally required to meet more onerous requirements, such as the appointment of a data protection officer and the necessity to carry out an assessment of the impact of data protection. Given that AI-powered fintech firms that operate at scale typically fall within this category, it is very important that they manage to comply with these obligations to dodge the penalties that are likely to accrue as a result.

3. Payment and Settlement Systems Act, 2007 (PSA)

The PSA, 2007, under the Reserve Bank of India, regulates payment systems, digital transactions, and electronic fund transfers. This is particularly relevant for AI-driven fintech firms involved in payment processing, digital banking, and automated financial transactions.

Section 10(2) – RBI's Data Localization Mandate

- Requires all payment-related data to be stored in India, affecting AI-driven payment processors like Google Pay, Paytm, and PhonePe.
- Ensures AI-powered fraud detection and payment monitoring comply with India's domestic data regulations.
- Aligns with RBI's 2018 circular on Storage of Payment System Data.

Section 18 – Oversight of Payment Systems

- RBI has authority to supervise and regulate fintech companies offering AI-driven payment services.
- AI models used in digital fund transfers, UPI payments, and real-time transaction monitoring must comply with RBI's regulatory framework.

Section 26 – Penalties for Non-Compliance

- AI-based fintech firms failing to comply with payment security standards may face fines up to ₹5 lakh per day for continued violations.
- Ensures AI-powered financial platforms adopt robust cybersecurity and fraud prevention measures.

4. Prevention of Money Laundering Act, 2002 (PMLA)

The PMLA, 2002 imposes anti-money laundering (AML) compliance on fintech firms, particularly those using AI in lending, digital payments, and fraud detection.

Section 3 – Definition of Money Laundering

- AI-powered financial platforms engaged in automated risk assessment and fraud detection must ensure they are not being used for money laundering activities.
- AI models must detect and flag suspicious transactions to prevent financial crimes.

Section 12 – Know Your Customer (KYC) and Reporting Obligations

- Fintech companies using AI-driven KYC verification must follow stringent identity authentication protocols.
- AI-driven fraud detection models must report suspicious transactions to the Financial Intelligence Unit (FIU-IND) under RBI's AML regulations.

Section 17 – Search and Seizure Powers

- AI-driven digital lending and payment platforms must ensure data integrity and transparency, as authorities have the power to investigate fintech platforms suspected of AML violations.

5. Banking Regulation Act, 1949 (BRA)

The Banking Regulation Act (BRA), 1949, governs banking institutions and fintech firms operating under banking partnerships, digital lending, and AI-driven financial services.

Section 21 – RBI's Control over Advances

- Regulates AI-powered credit scoring, automated lending, and loan disbursement models.
- AI models must ensure fair, non-discriminatory, and risk-based lending.

Section 35A – RBI's Power to Issue Directions

- RBI can restrict or modify AI-driven lending models that pose risks to financial stability.
- AI-powered loan underwriting and credit risk assessment must comply with RBI's lending policies.

Section 36 – Penalties for Non-Compliance

- AI-based fintech firms failing to meet RBI's governance, compliance, and fraud detection standards may face penalties.

2. Reserve Bank of India Guidelines

Primarily, the Reserve Bank of India (RBI) is responsible for regulating fintech area in India which includes digital payments, lending, and use of AI in financial services. The RBI has a localization mandate for payments data, this is one of their most important regulatory instruments, which says that all the data related to payment transaction will be stored locally in India. The effect of this regulation is a direct effect on fintech companies in payment processing using artificial intelligence, they must have to make sure, the data for all transactions is within India because of RBI's Data Localization requirement (RBI Bulletin, 2024).

Moreover, the Reserve Bank of India (RBI) has also issued Guidelines on Digital Lending to regulate the operations of AI-driven digital lending platforms. If a fintech decides to use an AI to evaluate credit worthiness, or automatizing loan decisions, the fintech has to make sure that the AI is working in a transparent and fair way, prevent over-indebtedness and protect the consumer rights. To prevent systemic risks, AI's use

is overseen by RBI, especially in areas like risk management and fraud detection (Kalra, 2023).

When it comes to India's regulatory approach to AI in fintech, it all starts with the relatively benign sounding DPDP Act and RBI guidelines. The DPDP Act by and large looks after ensuring data protection, on the other hand RBI's regulations keeps proper watch over the well-being of our financial system and also on risks to financial stability, that could result from AI-driven innovations in the financial sector.

6.6.2 Focus Areas of Indian Regulation: Financial Inclusion, Consumer Protection and Data Privacy

India's regulatory landscape for fintech is built on the principles of financial inclusion, customer protection, and data privacy. The object is to instil an environment of balanced growth - ensuring access to financial services by all, safeguarding the customers' rights/concerns and at the same time, setting out the rules regarding usage/storage of personal data by new age fintech companies.

1. Financial Inclusion

Extending financial services to the unbanked and underbanked, is one of the core objectives in Indian fintech regulation. The Reserve Bank of India has played a major role, especially through its support for Unified Payments Interface (UPI) and the Pradhan Mantri Jan Dhan Yojana, 2014 (PMJDY), which have enabled millions of Indians to join the formal financial system. Utilizing wide-ranging and universal digital financial technology innovations have used mobile banking, digital lending, etc., for addressing, resolving the issue of availability and accessibility of financial services, particularly in certain rural areas where the existing traditional banking infrastructure is at a deficit (PwC, 2024; Jain, 2023). Included in the National Strategy for Financial Inclusion is a detailed plan on how to expand access to banking services and make sure fintech works to produce fair financial growth (PwC, 2024) (Jain, Khurana, & Kumar, 2024).

2. Consumer Protection

India focuses a great deal on consumer protection when it comes to fintech regulations. To ensure that fintech firms maintain a certain level of responsibility, especially in digital lending and payments systems, they have put in place comprehensive guidelines that they have set for the RBI to enforce. The Digital Lending Guidelines are a new set of rules introduced in 2022 and make it necessary for all Fintech companies to provide complete information to customers about their loans, ensure that there's no predatory

lending and that the recovery process is fair and doesn't cause any mental stress to the victims. The framework is intended to safeguard consumers from fraud, excessive debt, and other risks posed by illegal digital lending platforms (Ahluwalia, Malhotra, & Kharmih, 2024) (Jain, 2023).

Another program is the RBI's regulatory sandbox initiative. The initiative allows fintech firms to run prototype financial products in a controlled environment. The objective of the program is to reduce the risk on the consumers and promote innovation. The aforementioned method has proven to be imperative in the reinforcement of consumer confidence whilst simultaneously deterring exploitation in emerging sectors of fintech, such as peer-to-peer lending and microfinance (Ahluwalia, Malhotra, & Kharmih, 2024).

3. Data Privacy

With the significant amount of sensitive data that the fintech companies handles, indeed, data privacy is escalating as a concern in the Indian fintech landscape. To secure personal information there is the recently passed Digital Personal Data Protection, (DPDP) Act of 2023. By implementing the DPDP Act, fintech firms will have to gain users' explicit consent for data collection and processing, ensure that personal data is handled in a transparent and secure way. By implementing these rules, privacy issues will be regulated, particularly since more fintech companies are using artificial intelligence and big data to provide personalized financial services (Ikigai Law, 2023) (Kalra, 2023).

When it comes to regulating fintech, India's focus is on enhancing financial inclusion, ensuring robust consumer protection, and making sure data privacy is not compromised. The regulatory environment seeks to strike a balance between innovation and the need to safeguard vulnerable populations and the financial ecosystem. This is accomplished by these focus areas which forge the foundation of the regulation.

6.6.3 AI in Fintech: Regulatory Gaps and Challenges in India

A number of regulatory gaps and challenges continue to accompany India's growing fintech landscape, particularly in addressing the integration of AI-driven innovations within the sector. The lacunas exist in respect of issues like data privacy, algorithmic transparency, AI governance and cross-jurisdictional regulatory coordination.

India faces several challenges in regulating AI in fintech including data privacy and security. Though the Digital Personal Data Protection (DPDP) Act, 2023 is dedicated

towards protecting personal data yet rapid advancements of AI-driven financial services such as the machine learning algorithms which is primarily used for credit scoring and the risk assessment has not been explicitly addressed and represented under the current regulations. As AI systems are powered by very complex algorithms and vast data sets , they often contain very sensitive and personal information and so it is key they are safeguarded and robust protections have to be in place to protect the data. On the contrary, the privacy laws of today may not be able to handle the specific challenges that AI present in specifically data minimization and purpose limitation due to the fact that AI systems are constantly changing their value using real time data inputs (Burman, 2023).

There is another great gap of regulation from lack of transparency in the AI algorithm that produced the credit scoring in the fintech firm. AI models. Specifically, models based off of machine learning and deep learning are called “black box” models because it is difficult for regulators to understand how these systems come to the decisions that they do. With little transparency there can be a lack of knowlege on the unfair practices, or any inherent algorithmic or unintended biases, which would lead to lending based on discrimination and credit scoring reporting incorrectly (Bharanitharan & Kaur, 2024). As of now, AI-driven fintech services in India do not have regulations specific to making them explainable, which can cause an issue in deploying trustworthy and accountable automated decision-making (Ridzuan, Masri, Anshari, Fitriyani, & Syafrudin, 2024).

The fragmentation of the regulatory framework governing fintech in India is another challenge. There are guidelines issued by various regulators which includes Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI) etc on different aspects of Fintech and sub categories in it such as digital lending, digital payments etc. Nonetheless, there is no comprehensive and widely accepted operational risk management frameworks for these AI/Fintech related areas. The fragmentation can result to a lacking of regulator consistence and potentially provide a barrier for fintech firms to operate in different jurisdictions within India (Jain, Khurana, & Kumar, 2024). When expanding into foreign territory and engaged in cross-jurisdictional fintech activities, the lack of cross-jurisdictional coordination also makes it more difficult to ensure consistent regulatory compliance and for consumers to be equally well protected (World Economic Forum, 2024).

Unfortunately, India’s current fintech regulation still lacks AI-specific guidelines that dive deeper into the various risks associated with AI in finance. While efforts, such as

the RBI's Regulatory Sandbox and the launch of the Make AI in India mission, have been made to spur innovation in the country, the legal framework in India is not fully able to grapple with the nuances AI has introduced. One specific area where government regulation is clearly needed is artificial intelligence in financial services. To date there has been no regulation suggesting what would be the ethical deployment and use of AI and how to ensure transparency and human accountability in cases where machines make decisions. Consequently, fintech firms may exploit these regulatory lacunae, potentially leading to consumer detriment and systemic risk (RBI, 2024).

Though there have been very strong advancement in the regulation of fintech ecosystem in the country of India, there only seem to be some amount of gaps when it comes to management of artificial intelligent driven financial service that is aim at bringing financial in inclusion. Notable among the gaps are inadequate data privacy protections, lack of algorithmic transparency, weak regulatory frameworks, and undeveloped AI-specific regulations. A proactive response to these challenges from regulators will require the development of a harmonized and adaptable legal framework that promotes innovation and ensures both consumer protection and the integrity of the system.

6.7 KEY SIMILARITIES IN REGULATORY APPROACHES: EU, US and INDIA

Aspect	European Union (EU)	United States (US)	India
Primary Data Protection Law	General Data Protection Regulation (GDPR, 2018)	California Consumer Privacy Act (CCPA, 2018) & Proposed ADPPA (2022)	Digital Personal Data Protection (DPDP) Act, 2023
Key Principles	Data minimization, purpose limitation, consent-based processing	Opt-out rights, transparency in data handling, sectoral regulations	Purpose limitation, consent-based processing, deemed consent exceptions
Consumer Rights	Right to access, correct, delete data, right to be forgotten	Right to opt-out, access personal data, limited deletion rights	Right to access, correct, and erase data, but no right to be forgotten
Data Breach Notification	Mandatory reporting within 72 hours	Sector-specific breach notifications, varies by state and law	Mandatory reporting, but cross-border data transfer is eased
AI in Financial Risk Management	AI Act imposes strict governance and transparency for high-risk AI	Federal Reserve emphasizes AI model validation and risk assessment	RBI monitors AI-driven fintech for compliance and risk management
AI Regulations for Financial Stability	AI Act classifies financial AI as high-risk and mandates explainability	Regulatory agencies oversee AI models but lack unified AI law	AI in financial services is regulated through RBI and DPDP guidelines

Key Risks Identified	Model risk, concentration risk, AI bias, systemic vulnerabilities	Fragmentation in AI oversight, over-reliance on automated models	AI bias, financial inclusion risks, concentration risk in AI models
Regulatory Approach to AI in Finance	Precautionary approach with strict compliance requirements	Innovation-first approach with post-implementation oversight	Balanced approach focusing on financial inclusion with regulatory flexibility

Table 6.4: Key Similarities in Regulatory Approaches: EU, US and India

6.7.1 Data Protection and Consumer Privacy

When it comes to the regulatory frameworks governing data protection and consumer privacy, researcher can say that the three key jurisdictions, the US, Europe, and India, all share characteristics and similarities in the protective and enhancement measures they put in place to guard both the personal data basis and take into account the consumer's right. The frameworks differ in approach and scope, however, they both fundamentally agree on a several fundamental principles.

1. General Data Protection Regulation 2018 (GDPR) - EU

Regarded as the epitome of secure data, the General Data Protection Regulation, or the GDPR for short, was put into place in the year of 2018. It establishes general principles for processing personal data, such as data minimization, purpose limitation and consent-based processing. In addition, the GDPR grants individuals an array of robust rights, which include the right to data portability as well as the right to be forgotten (GDPR, Art. 20) (Viswanath, Muthanna, & Jain, 2023).

These rules and clauses are designed to empower individuals to have more control over their own personal data. In addition, they make sure that the organizations that process this data work in a transparent and responsible manner.

2. California Consumer Privacy Act (CCPA) & American Data Privacy Protection Act (ADPPA) (Proposed 2022) - US

The approach that American regulations on the privacy of personal information have taken up until now has been laying down rules for specific sectors of the economy, such as health (HIPAA) or finance (GLBA). Bringing the United States one step closer to the model of the GDPR, the California Consumer Privacy Act (CCPA) and the soon to be proposed American Data Privacy Protection Act (ADPPA) grant consumers other more enhanced rights such as the right to opt-out of data sharing and the right to access the personal data collected by the corporations. The ADPPA, although not yet fully

enacted, aims to provide more comprehensive protections at the federal level, covering various aspects of data collection and processing, similar to the GDPR

3. Digital Personal Data Protection (DPDP) Act 2023 - India

India's Digital Personal Data Protection (DPDP) Act, passed in 2023, shares many similarities with the GDPR, though it is narrower in scope. The DPDP Act mandates that companies obtain explicit consent before processing personal data and requires data fiduciaries to adhere to principles like purpose limitation and data minimization (Viswanath, Muthanna, & Jain, 2023)

However, the DPDP Act introduces the novel concept of deemed consent, allowing data processing for certain purposes without explicit user consent, which distinguishes it from the stricter GDPR standards (Viswanath, Muthanna, & Jain, 2023)

Alignment Across Frameworks

All three jurisdictions—EU, US and India—align on key objectives:

- **Consent and Transparency**: Each framework emphasizes the importance of obtaining consent before processing personal data and maintaining transparency in data handling practices.
- **Consumer Rights**: Users have the right to access, correct, or delete their data across all three jurisdictions, though the GDPR offers the most comprehensive protections, such as the right to be forgotten.
- **Data Breach Notifications**: All frameworks require entities to report data breaches, though the specifics of these requirements, such as the timeframe and thresholds for reporting, vary (Viswanath, Muthanna, & Jain, 2023)

While the specific provisions differ, the overarching goal of these regulations is to protect personal data and strengthen consumer privacy, reflecting a growing global consensus on the importance of data protection in the digital age.

6.7.2 Financial Stability and Risk Mitigation

AI-driven fintech introduces both opportunities and risks to financial stability, which is a shared concern across regulatory frameworks in the EU, US and India. While AI technologies enhance efficiency and risk management in areas like fraud detection and

trading, they also bring potential risks, such as model risk, overreliance and concentration risks, that need to be mitigated.

By using Artificial Intelligence (AI) in automating risk management, organizations can also improve the efficiency of fraud detection, credit decisions and market forecasts. Nonetheless, it also implies that if the AI models are poorly designed or use biased data that can lead to risks as well. All regions have expressed a concern on this matter, noting that AI-driven models may contribute to financial instability if they fail to detect outlier events, or if they are improperly or mistakenly used (Financial Stability Board, 2024).

Additionally, these leaders are bothered by the idea of model risk as well, which can be seen as where data is of poor quality or if AI algorithms are not fully translucent, and can also result in poor decision making concerning financial risk. The AI Act in the EU directly deals with this problem by setting strict rules and guidelines for high risk AI systems, systems like the ones used in financial markets, so that they are accurate in their decision making and that they aren't hiding anything from us. In the United States regulators such as the Federal Reserve stress the importance of model validation in order to avoid what AI systems can do for systemic risk (Financial Stability Oversight Council, 2024) (Klein & Lee, 2024) (Danielsson & Uthemann, 2024).

In addition, concentration is a major common risk. This is the risk that if AI is used by a large number of financial institutions the models that they use could all be very similar, this means that they would all react in the same way to a particular event, this could then amplified and cause an extremely large risk. A huge villain of the global financial crisis has been uniformity in risk models because of these problems market crashes happen. Moreover, trading or credit decisions by many different institutions that all use pretty much the same algorithms could compound the problem. Emphasis has been made by regulatory bodies both in the EU and in India of the need for scenario analyses that ascertain how an AI system might behave in a stressed market (Klein & Lee, 2024) (Treacy & Qemali, 2024).

In dealing with these risks, what regulators all over the globe are advocating is a very firm risk governance framework. The European Union is mandating strong governance of AI technologies through the Artificial Intelligence Act (AI Act), while India is instituting guidelines to ensure that AI-driven financial systems are robust to-market fluctuations and cybersecurity risks, with the help of the Reserve Bank of India (RBI). To mirror these efforts in the US, the Financial Stability Oversight Council (FSOC) is using its member agencies to explore how they can strengthen regulatory oversight of

Artificial Intelligence (AI) applications in the financial industry (CEPR, 2024) (Leitner, Singh, van der Kraaij, & Zsámboki, 2024) (Treacy & Qemali, 2024).

Financial markets can gain much from A.I., but to get there, the vulnerabilities have to be managed. EU, US and Indian regulatory frameworks have a common concern about how to address model risk, systemic vulnerabilities and transparency, and governance requirements.

6.8 KEY DIFFERENCES IN REGULATORY APPROACHES: EU, US AND INDIA

Regulatory approaches to AI in fintech differ across the EU, US, and India, shaped by their legal philosophies and economic priorities. The EU adopts a precautionary principle, prioritizing risk management and consumer protection before widespread AI adoption. The US follows an innovation-first approach, fostering technological advancements with a relatively flexible regulatory landscape. Meanwhile, India balances innovation with financial inclusion, ensuring fintech growth expands access to financial services while maintaining necessary safeguards. These differences lead to unique jurisdictional challenges. The EU's extraterritorial data protection laws (such as GDPR) impose strict cross-border compliance requirements. The US faces regulatory fragmentation, where fintech firms must navigate a complex landscape of state and federal laws. India's DPDP Act, 2023, eases some data transfer restrictions but still requires compliance with international privacy standards. These variations highlight the need for greater cross-jurisdictional cooperation to facilitate seamless AI-driven financial services across borders.

6.8.1 Approach to Innovation and Regulation

The distinct legal, economic and cultural contexts in Europe, US and India have influenced the regulation in FinTech and innovations and reflect their vision and strategy in term of the development of these industries. A stark disparity in how these countries balance innovation with regulation focuses the European Union on a precautionary principle, the United States on an innovation-first approach, and India on financial inclusion.

1. EU: Precautionary Principle

The regulatory landscape in the EU is structured as a precautionary structure to innovation. This is to say that new technology, especially in finance and AI, is held back to prevent any potential risks from emerging before they are fully understood. An example for this would be the AI Act which breaks AI systems into different risk categories and be required to go through strict examination if it is classified as high risk, like those systems for credit scoring and trading. The focus should be on ensuring that any new innovations within the fintech sector should not be eroding consumer protection or financial stability. The principle of precaution asks us to look at new technologies to make sure they are in step with our values and have the kind of regulations around them that the users get comfortable with before they get widely deployed (Ahern, 2021) (European Banking Authority [EBA], n.d.).

2. US: Innovation-First Approach

Contrarily, the United States commences a more innovation-friendly regulatory protocol. Though the country encourages the use of gadgets, the regulatory landscape often lags behind. The Federal Reserve, and the Federal Trade Commission (FTC) are agencies that watch over fintech the priority is fostering innovation and competition, rather instead of creating an excessive regulatory structure early on. The framework operating within the US, alternatively, is characterized by a strong emphasis on fostering innovation and entrepreneurship in industries, such as technology, reactor or our financial industry, that are traditionally more open to self-regulation. One example of this is the use of regulatory sandboxes that allow fintech firms to test new products and services without having to put in place time-consuming compliance measures. The concept with this approach is to try to balance the inherent freedom of the market and this later-stage oversight (Zander, 2010).

3. India: Financial Inclusion

India has a unique approach due to its emphasis on financial inclusion, which impacts its regulatory approach. To encourage the growth of the fintech industry and to ensure that the fintech innovation extends access to banking and financial services especially in the rural areas and to the not so privileged the Reserve Bank of India (RBI) had launched several initiatives. The Pradhan Mantri Jan Dhan Yojana and the Unified Payments Interface (UPI) are an example of how use fintech to promote inclusion, but also making sure that safeguards are in place. Facilitating innovation while also mitigating risks to financial stability, the National Strategy for Financial Inclusion (NSFI) takes a further aim at these points by recognizing that regulatory sandboxes is the opportunity to know that regulation and supervision continue to be part of the

equation (RBI, 2024) (Jain, 2023). Therefore, India's regulatory model simultaneously delivers innovation with deep intent to expand access of financial services in rural and remote, unbanked areas of the country.

The precautionary principle of the EU is an endeavor to try and maintain safety in the market by trying to limit risks before they happen. However, US focuses on innovation first and allows technology to grow without heavy initial regulation and India focuses on fintech innovation to promote financial inclusion by means of flexible frameworks to manage the innovation and risk. Such discrepancies highlight the differing priorities and challenges that each region faces, which in turn influences their regulatory responses to the development of fintech and artificial intelligence.

6.8.2 Jurisdictional Challenges

It is complex to navigate jurisdictional challenges navigating jurisdictional challenges in cross-border AI-driven financial operations, especially dealing with different regulatory frameworks in regions like the EU, US and India. Due to individual jurisdictions having their own unique approaches to AI, data protection and financial regulation the conflicts and difficulty with compliance may arise.

1. European Union (EU): Extraterritoriality and Data Protection

The General Data Protection Regulation, known as the GDPR, is a major regulation that enforces standardized data rights to protect the citizens of the European Union. The GDPR does not only govern companies located inside the EU, but also any company backward or forward processing any EU citizen's personal data. The fact that the GDPR is not limited to EU borders but any US fintech companies who's customers are in the EU also is subject to GDPR is an example of the GDPR's territorial reach. Because of the requirements associated with data transfers that have been put into place by the GDPR, cross-border operations may be more difficult for companies in the field of AI driven financial services. The newly proposed AI Act adds even more levels of complexity through the compliance burden by requiring international firms to comply with strict compliance requirements regarding of algorithmic transparency and risk assessments. This is going to make it even more difficult to manage operations in different jurisdictions (Deloitte, 2024) (Bromberg, Godwin, & Ramsay, 2018).

2. United States: Fragmented and Sectoral Approach

The US presents a patchwork of regulatory bodies, as different aspects of data protection and fintech are addressed individually in various federal and state laws.

Unlike the GDPR's uniform framework, the US relies on sector-specific regulations. For example, the California Consumer Privacy Act (CCPA) imposes strict data protection requirements in California, while other states may have different or less stringent regulations. This fragmented approach creates jurisdictional conflicts when US fintech firms engage in cross-border operations, as they must navigate both domestic inconsistencies and international regulations, such as GDPR compliance. Additionally, the Federal Trade Commission (FTC) and other federal agencies oversee parts of the fintech industry, but their sectoral focus makes it difficult for firms to manage cross-border compliance consistently (Bromberg, Godwin, & Ramsay, 2018)

3. India: Cross-Border Data Transfers under the DPDP Act

India's Digital Personal Data Protection (DPDP) Act, 2023, unlike earlier drafts, does not mandate data localization. The final version allows for cross-border data transfers to countries designated as "trusted" by the Indian government, thus easing some of the earlier concerns about strict localization requirements. However, Indian fintech firms must still comply with stringent data protection standards when handling sensitive data. This creates a jurisdictional challenge when Indian companies operate in foreign markets like the EU, where data transfer restrictions under the GDPR are more rigid. The Reserve Bank of India (RBI) also plays a crucial role in regulating fintech, ensuring that AI-driven financial services meet both domestic and international compliance requirements (Deloitte, 2024)

4. Cross-Jurisdictional Cooperation

A significant challenge across all regions is the lack of harmonized regulations for cross-border AI-driven financial operations. While the EU has stringent, unified frameworks like the GDPR, the US and India face fragmentation and a need for clearer coordination across jurisdictions. This complicates efforts to streamline compliance for companies operating in multiple regions. Collaborative frameworks, such as mutual recognition agreements or international regulatory sandboxes, may help alleviate some of these challenges, but they remain underdeveloped (Bromberg, Godwin, & Ramsay, 2018). Cross-border AI-driven fintech operations face jurisdictional challenges due to regulatory fragmentation and differing standards across the EU, US and India. Companies must develop robust compliance strategies to navigate the complex web of legal requirements in these regions.

6.9 LESSONS FOR INDIA FROM THE EU AND US APPROACHES

AI Regulation Aspect	EU AI Act (2024) - Legal Provisions	US AI Bill of Rights (2022) - Guidelines
Algorithmic Bias & Fairness	Article 10: High-risk AI must use bias-free, high-quality datasets. Article 14: Requires human oversight to prevent discriminatory outcomes.	Principle 2: AI must be designed to eliminate bias and ensure fairness.
Transparency & Explainability	Article 13: High-risk AI must provide clear documentation on its purpose and functioning. Article 52: Users must be informed when interacting with AI systems.	Principle 4: AI systems must disclose their presence and explain their decisions.
Blackbox Problem (AI Opacity)	Article 15: High-risk AI must provide sufficient documentation to ensure traceability and transparency.	Principle 1: AI should undergo rigorous testing and be publicly evaluated to ensure transparency and safety.
Data Privacy & Protection	Article 5: Prohibits AI practices posing unacceptable risks, including unauthorized personal data processing. Article 10: High-risk AI must align with GDPR data governance principles.	Principle 3: AI must provide users control over their data and ensure strong privacy protections.
Liability & Accountability	Article 99: Imposes penalties on companies deploying non-compliant high-risk AI.	Federal Trade Commission (FTC) AI Guidelines: Imposes financial penalties for AI consumer protection violations.

Table 6.5: AI Regulation Aspect: EU and US Approaches

6.9.1 Adopting Regulatory Best Practices

India can draw significant lessons from both the EU and US in adopting regulatory best practices for AI-driven fintech, balancing innovation with oversight and consumer protection.

1. Risk-Based Approach (EU)

One of the key takeaways from the EU's AI Act is its risk-based regulatory approach. The EU categorizes AI applications based on risk levels—minimal, limited, high and unacceptable—and applies different regulatory obligations depending on the risk involved. This tailored approach allows innovation in low-risk areas while ensuring stringent oversight for high-risk applications like those used in financial services. India could adopt a similar framework, particularly as fintech innovations involving AI grow. By doing so, India could better address systemic financial risks without stifling innovation (Krishnamurthy & Khandelwal, 2024)

2. Regulatory Sandboxes (US)

The US's innovation-first approach, especially its use of regulatory sandboxes, provides a flexible environment for fintech firms to test new technologies without facing immediate heavy regulatory burdens. These sandboxes allow fintech startups to

experiment with AI-driven solutions under regulatory supervision, fostering innovation while ensuring consumer protection. India has already begun to explore such initiatives under the Reserve Bank of India's regulatory sandbox framework, but further expanding these sandboxes to include AI-driven financial services could enhance the country's regulatory flexibility and promote responsible innovation (Engler, 2023) (Toms, Simon, & Kamyar, 2023)

3. Data Privacy and Security (EU & US)

Both the EU's GDPR and the US's sectoral approach to data privacy emphasize the importance of protecting consumer data. The GDPR sets a high standard for data protection, including rights such as data portability and the right to be forgotten. The US, while more fragmented, has specific sectoral regulations like the California Consumer Privacy Act (CCPA), which focuses on data protection in technology-driven sectors. India's Digital Personal Data Protection (DPDP) Act follows a similar consent-based approach, but can further enhance its data privacy protections by implementing more robust data security standards and algorithmic transparency requirements (Kakoti & Singh, 2024) (Engler, 2023)

4. Governance and Compliance (EU)

The EU's focus on AI governance, as highlighted in the AI Act and the Digital Operational Resilience Act (DORA), stresses the importance of continuous monitoring, risk assessment and compliance mechanisms. These governance structures ensure that AI models in fintech are transparent, explainable and aligned with financial stability goals. Indian regulators, such as the Reserve Bank of India, could adopt similar continuous governance frameworks to ensure that AI models used in credit scoring, lending and fraud detection are not only effective but also accountable (Toms, Simon, & Kamyar, 2023) (PwC, 2024). By adopting best practices from the EU and US, such as a risk-based approach, regulatory sandboxes and stronger data protection measures, India can enhance its AI regulatory framework while promoting fintech innovation.

6.9.2 Enhancing India's AI and Fintech Framework: Recommendations Based on International Examples

India's burgeoning fintech and AI ecosystems are poised for exponential growth. However, to ensure that this growth is both sustainable and responsible, India can draw several key lessons from the regulatory frameworks of the EU and US. Here are some recommendations based on these international examples:

1. Strengthening Data Privacy and Protection

Both the EU's GDPR and the US's sectoral regulations highlight the importance of robust data protection frameworks. The Digital Personal Data Protection (DPDP) Act, 2023 is a solid starting point, but India can enhance its framework by incorporating stricter data minimization and accountability principles. The GDPR's right to be forgotten and data portability provisions could serve as models for enhancing individual control over personal data. Additionally, implementing data localization policies similar to those discussed in earlier drafts of the DPDP Act could help secure sensitive financial data processed by AI systems, particularly in fintech services (Bagai, Uppal, & Baidwan, 2024) (Jain, Kumar, & Khurana, 2024)

2. Risk-Based Regulation for AI

Adopting a risk-based regulatory approach like the EU's AI Act would allow India to regulate AI technologies based on their potential risks. High-risk AI systems used in credit scoring**,** fraud detection and trading algorithms could be subject to stringent regulatory requirements, ensuring they meet transparency, accountability and fairness standards. This approach would help mitigate the risks associated with AI without stifling innovation in lower-risk areas (Singh, 2024)

3. Expanding Regulatory Sandboxes

India has already introduced regulatory sandboxes to foster fintech innovation under the supervision of the Reserve Bank of India (RBI). Drawing from the US and UK examples, India could further expand these sandboxes to include AI-driven fintech products. This would provide a controlled environment for fintech firms to test their AI models while ensuring compliance with evolving regulations. Sandboxes encourage innovation by allowing startups to refine their products without facing the full brunt of regulatory restrictions initially (Bagai, Uppal, & Baidwan, 2024) (Singh, 2024)

4. Ethical AI and Governance

The EU's focus on ethical AI through initiatives like the AI Act and the proposed Digital Operational Resilience Act (DORA) emphasizes the importance of fairness, accountability and transparency in AI systems. India could adopt similar governance structures to ensure that AI systems used in fintech are not only effective but also aligned with ethical standards. Establishing AI ethics councils and frameworks for monitoring AI model behavior would ensure responsible innovation (Mohanty & Sahu, 2024) (Bagai, Uppal, & Baidwan, 2024)

5. Cross-Border Data Transfers

Given India's ambition to expand its fintech services globally, the country can benefit from harmonizing data transfer standards with other major economies like the EU and the US. India's recent policy shift away from strict data localization to allowing cross-border data transfers under the DPDP Act marks a step in the right direction. However, adopting a framework similar to the GDPR's adequacy decisions could ensure smoother cross-border data flows without compromising privacy (Jain, Kumar, & Khurana, 2024) (Mohanty & Sahu, 2024). By integrating these international best practices, India can create a regulatory framework that balances innovation**,** consumer protection and financial stability, while encouraging the responsible growth of its AI and fintech sectors.

6.10 CONCLUSION

In conclusion, this chapter provided a comparative analysis of AI regulations in fintech across the EU, US, and India**,** highlighting their distinct approaches. The EU follows a comprehensive, risk-based regulatory model, prioritizing transparency, accountability, and consumer protection through laws like the GDPR and AI Act, setting a global benchmark for ethical AI governance. In contrast, the US adopts an innovation-driven, sector-specific approach**,** encouraging technological advancements while addressing fairness and safety through initiatives like the Blueprint for an AI Bill of Rights**.** India, positioned between these models, incorporates elements from both frameworks, with laws such as the Digital Personal Data Protection (DPDP) Act, 2023, and sectoral regulations by the RBI, aiming to balance innovation with financial inclusion and data protection. However, the lack of AI-specific regulations in India underscores the need for a more structured and unified legal framework to manage AI-driven fintech effectively. This analysis underscores how regulatory frameworks are shaped by regional priorities, offering insights into best practices while identifying areas where India can refine its approach to AI regulation in fintech.

Building on this comparative analysis, the next chapter, "Chapter 7: Conclusion and Recommendations", will synthesize the key findings from previous chapters to propose actionable recommendations. These will focus on bridging the regulatory gaps in India's AI and Fintech ecosystem by incorporating global best practices while aligning with local requirements. The chapter will also outline a comprehensive policy framework aimed at fostering innovation, ensuring ethical AI deployment, and safeguarding consumer interests in a rapidly evolving financial landscape.

CHAPTER 7

CONCLUSION AND RECOMMENDATIONS

7.1 CONCLUSION

Integrating artificial intelligence (AI) into the financial technology (FinTech) sector represents a transformative shift in the modern financial landscape, bringing unprecedented opportunities alongside complex legal and ethical challenges. This thesis undertook a comprehensive comparative analysis of how India, the European Union (EU), and the United States (US) are addressing these challenges within their respective legal frameworks. The findings underscore that as AI-driven financial systems continue to evolve, innovation must be matched by rigorous regulatory oversight, ethical safeguards, and a steadfast commitment to consumer rights. In essence, the promise of AI in FinTech can only be realized sustainably if accompanied by clear rules and principles that ensure technology serves the public interest rather than undermines it. The convergence of finance and AI demands not just technological acumen but also a reimagining of legal norms to keep pace with the rapid changes, ensuring that financial innovation does not outstrip the frameworks designed to govern it. This research highlights that legal responses to AI in FinTech vary significantly across jurisdictions, reflecting different stages of regulatory maturity and policy priorities. The EU has taken a proactive, comprehensive stance which is exemplified by instruments like the General Data Protection Regulation (GDPR) and the EU AI Act that emphasizes on risk-based approach that prioritizes transparency, accountability and consumer protection. The United States, by contrast has favoured an innovation-driven, sector-specific approach rather than one overarching AI law, it employs targeted regulations and agency guidelines to address the AI's impact in financial services, which is coupled with initiatives like the Blueprint for an AI Bill of Rights to guide ethical use of AI. India has found itself as positioned between these models. On one hand, India is drawing from the global best practices i.e. for instance, enacting the Digital Personal Data Protection Act, 2023 for data privacy and issuing sectoral guidelines through the Reserve Bank of India (RBI) which aims to balance the technological innovation with the financial inclusion and data protection. On the other hand, India lacks dedicated AI-specific legislation that results in a fragmented framework where existing financial, data and cyber laws are stretched to cover AI scenarios. These differences in regulatory approach are not merely academic alone but they also carry real-world implications for cross-border fintech operations, investor

confidence and consumer protection. The comparative lens of this thesis reveals that each jurisdiction's approach is shaped by its own normative values and policy objectives which the EU's emphasis on fundamental rights and risk mitigation, the US's emphasis on market innovation and self-regulation, and India's focus on growth and inclusion and still yet all face a common challenge of keeping the regulation as dynamic and adaptive as the technology itself. A major finding of this study is the sheer complexity of crafting legal frameworks for AI in FinTech, given the multifaceted challenges the technology poses. AI-driven financial systems amplify longstanding issues like the data privacy and security, while also introducing a new dilemmas around algorithmic decision-making, bias and accountability. Opaque "black box" AI models often defy easy explanation which makes it difficult for consumers or the regulators for even to understand how decisions (such as a loan approval or fraud flagging) are made. This opacity raises an serious concerns about fairness and also due process.

Currently, both the US and EU attempt to address such issues through existing laws such as American consumers might invoke the Fair Credit Reporting Act, and Europeans might rely on the GDPR provisions that requires the demand for the clarity on automated decisions. However, these mechanisms are only a start. The lack of built-in transparency in AI systems means that neither customers nor regulators can fully scrutinize the outcomes of a gap that undermines the accountability and trust. When errors or biases occur, the law struggles with assigning the liability part. As illustrated by incidents like the 2010 "flash crash" where the algorithmic trading programs have caused a rapid market collapse that AI can trigger cascading failures with systemic consequences, yet legal accountability remains murky. Such events spotlight the urgent need for legal clarity on responsibility and also redress in an age where autonomous algorithms can drive billion-dollar decisions. In the absence of clear rules, financial firms deploying AI run heightened legal risks and consumers may be left with vulnerable to unfair or opaque practices. AI algorithms which is trained on historical financial data can also inadvertently perpetuate or even exacerbate biases. For example, systematically disadvantaging certain minority groups in credit scoring or fraud detection. Such outcomes will offend the core normative commitment to the equality embedded in most of legal systems and thus underscoring that technological advancement must not come at the cost of societal values. Ensuring that AI-driven decisions align with principles of fairness requires a deliberate intervention.

Data inputs must be scrutinized for biases, and decision-making processes need to be made as transparent as possible. In this regard, explainable AI (XAI) has emerged as a crucial concept that aims to make the AI's inner workings interpretable to humans. By

enhancing transparency, XAI can also help regulators and affected individuals understand why an algorithm arrived at a particular conclusion and thereby facilitating accountability and contestability. This thesis found that explainability and ethical design are not merely an technical add-ons but also an essential components of good AI governance in finance. They help ensure that AI systems uphold the individual rights and public trust which echoes the calls in the EU's AI Act for requirements around non-discrimination, human oversight, and fairness in high-risk AI applications. In essence, a normative framework is emerging globally that demands AI be not only effective but also the legal systems will need to do incorporate these principles to remain legitimate and effective in the fintech context.

Another central insight of this research is the importance of balancing innovation with the regulation. FinTech innovation driven by AI holds an immense promise, from expanding financial inclusion through automated credit underwriting also to improving efficiency with robo-advisors and algorithmic trading. But an unchecked innovation can also introduce instability and cause consumer harms. The United States often gives innovation the benefit of the doubt and intervening primarily when clear harm materializes, whereas the EU tends to regulate the pre-emptively to curb potential risks and India's evolving framework seeks a middle ground. This means India can adopt global best practices such as the EU's emphasis on data protection and accountability, and adapt them to local needs, avoiding the mistakes others have made. As noted in this thesis, the Indian regulatory strategy could evolve into a hybrid model that safeguards the consumer interests and also financial stability without unduly hampering innovation. Such type of balanced approach is critical for building a resilient FinTech ecosystem that leverages the AI for growth and also inclusion while maintaining public trust.

The policy implications which emerge from this comparative study are profound, extending from domestic law-making to an international coordination. At the domestic level, one clear implication is that the India (and indeed other countries in similar positions) would benefit from developing a more unified and AI-specific regulatory framework for FinTech. Currently, Indian fintech companies must navigate a patchwork of laws that ranges from banking regulations and payment system rules to data protection statutes to which none of them were originally designed with AI in mind. In parallel, existing laws and regulations ought to be modernized to account for AI-driven risks. Financial regulations like the RBI Act or the Securities laws may need amendments to cover AI-based services and clarify the powers of regulators over algorithmic systems. Likewise, consumer protection laws should evolve to ensure AI-

driven financial services are covered by rules on fair treatment and redress, recognizing that an algorithm's actions can harm consumers just as much as a human's. Policymakers are called to anticipate how emerging technologies like blockchain and smart contracts will intersect with AI in finance, so that legal frameworks remain agile and future-proof. Notably, this study observed that the pace of technological change necessitates continuous regulatory learning and adaptation and regulators may need to adopt sandbox approaches and iterative rule-making, allowing them to respond promptly to innovation without sacrificing oversight. The legal and policy toolkit for AI in FinTech must be both comprehensive and flexible keeping a setting firm principles and boundaries, yet nimble enough to evolve as the technology and its uses continuously change.

Platforms such as the G20, the Financial Stability Board (FSB) and global standard-setting organizations are identified as crucial venues for forging consensus on AI governance principles in finance. By sharing best practices and aligning standards regulators can be more effectively oversee the AI-driven finance that operates globally. Collaborative efforts could lead to the development of international guidelines or even treaties that ensure AI applications in banking, payments, or investment are subject to consistent oversight no matter where they function. This would not only ease compliance for FinTech firms operating internationally but also close loopholes that bad actors might exploit by moving operations to lightly regulated jurisdictions. Crucially, the study also points to the need for empowering stakeholders across the board as part of the governance solution. Law and regulation alone will not suffice if the individuals and institutions who design, deploy and are affected by AI in FinTech are not actively involved in its oversight. This means financial regulators have to build their technical capacity to understand the AI systems, so they can effectively supervise complex algorithms and enforce rules.

Looking forward, the conclusion of this thesis reflects on future pathways and the imperative to manage systemic risks. One of the sobering lessons of AI integration in finance is that while it can make an individual firms more efficient, it can also introduce new forms of systemic vulnerability. As AI models become ubiquitous in credit scoring, trading, and risk management, there is a potential for correlated failures and if many institutions rely on similar algorithms or data and those algorithms behave unexpectedly, a single point of failure could ripple across the entire financial system. Financial regulators thus therefore must broaden their mandate to include oversight of algorithmic risks at a macro-prudential level. This study notes that international standard-setters like the Bank for International Settlements (BIS) and the International

Organization of Securities Commissions (IOSCO) have already started discussing such measures, recognizing that preventing AI-driven instability is now part of maintaining overall financial stability. In the Indian context, safeguarding against systemic risks might involve the RBI and other regulators conducting stress tests on AI algorithms used by banks and NBFCs, or requiring firms to have fallback plans if their automated systems malfunction. Ensuring financial stability in the age of AI will require novel tools and close coordination among regulators globally, since systemic shocks can be transmitted instantaneously through digital networks. Yet, these preventative efforts must be balanced with the awareness that over-regulation could hamper the beneficial systemic impacts of AI such as improved risk detection and efficiency gains that strengthen the financial system.

In conclusion, the integration of AI into FinTech is both a test and an opportunity for legal systems worldwide. It tests the adaptability of laws and regulations in the face of transformative technology and it also offers an opportunity to craft frameworks that can harness AI's benefits while curbing its perils. This thesis's comparative exploration of India, the EU, and the US shows that while there is no one-size-fits-all solution, there are common threads emerging: the need for clarity in accountability, the enforcement of ethical principles, the balancing of innovation with risk mitigation, and the value of collaborative governance across borders. Addressing the normative, legal and policy implications of AI in finance is not a one-time project but an ongoing journey whereas one will require vigilance, flexibility and foresight from lawmakers, regulators and industry alike. For India, a key takeaway is the importance of proactively shaping its regulatory landscape in dialogue with global developments, rather than reacting belatedly to problems after they arise. By enacting forward-looking policies and embracing international best practices, India can not only safeguard its consumers and financial markets but also position itself as a leader in responsible AI-driven innovation. Globally, the continued exchange of ideas and coordination through regulatory dialogues, standard-setting and perhaps even new international agreements will be pivotal in ensuring that AI-enhanced financial systems remain fair, transparent, and resilient. In summation, the future of FinTech with AI will be defined not just by algorithms and data, but by the legal policy we make today. A coherent, inclusive and principled approach to AI regulation in finance will help secure a future where technology serves society in the financial realm, bolstering trust and stability while fostering innovation for the benefit of all.

7.1.1 SUMMARY OF FINDINGS

1. The Complexities of Legal Frameworks

The regulatory approaches for India, the EU, and the US exist at different stages of maturity. In terms of the most mature regulation, the EU is leading the way with its proactive nature. In contrast, India's data protection framework is new with a high-level of focus—this is exemplified by the Digital Personal Data Protection (DPDP) Act, 2023. Although the United States has targeted regulations that are applied as part of a sector-specific approach and a more state-driven than federal one, it has no central government regulatory approach for AI technologies in place at the present time. These differences highlight just how important it is for the world to come together to work on solving jurisdictional conflict and cross-border problem, which operation globally is the biggest solution.

2. Key Legal and Ethical Challenges

Artificial intelligence (AI) driven FinTech systems poses a number of challenges such as requirement of data privacy, security, lack of transparency, opaque algorithmic biases and lack of robust liability frameworks. This problem is escalated with the 'black box' nature of AI systems, because in circumstances such as a financial error, or a course of action that was found to be discriminatory, it is difficult to assess who is to be held accountable. Moreover, the proliferation of technologies like quantum computing and blockchain only increases the intricacy of enforcement, requiring a perpetual amendment to regulations.

3. Balancing Innovation and Regulation

This research emphasizes the need for a balanced approach between innovation and protecting consumer interests and financial stability. The early-stage regulatory framework in India provides an excellent chance to glean lessons from the EU and US models regarding what works and what doesn't. It allows for the local adaptation of a global legal structure that can adequately meet the regulatory challenges of the day.

4. A Call for International Collaboration

Financial systems operating in an AI-driven manner exist in a borderless environment, making international collaboration essential to achieve regulatory harmony, share best practices, and resolve cross-border concerns like data flows and jurisdictional clashes. Collaboration can be fostered by platforms such as the G20 and Financial Stability Board.

5. Empowering Stakeholders

From this study, a crucial lesson learned is the rising need for stakeholder empowerment. This group includes not just consumers but also regulators and financial institutions that have a say in how AI should be governed. These stakeholders must be strengthened so they can manage the complicated business of AI governance. It is essential to build trust and ensure that equitable outcomes are reached when creating public awareness campaigns, when building the capacity of initiatives, and when forming inclusive processes of policy-making.

7.2 RECOMMENDATIONS

This thesis responded to the detailed challenges and opportunities associated with the certain dynamic AI in FinTech sector. In so doing, it formulated a set of comprehensive recommendations to build a well-functioning regulatory ecosystem for AI in FinTech. These recommendations aim to fill the legal, ethical, and technological voids researcher have identified while also encouraging innovation and ensuring consumer protection.

At the core of these suggestions is the **"Artificial Intelligence in Financial Technology Regulation Act, 2025,"** a proposed framework for governing the use of AI and financial technology together in our financial systems. Moreover, the researcher has proposed some more targeted measures to strengthen the regulatory landscape. These include:

2. Blockchain-Smart Contract Compliance Framework

This framework guarantees for blockchain-based smart contracts in financial technology (Fintech) legal recognition, openness and dispute resolution systems. Combining consumer protections, interoperability rules and auditing systems helps to build confidence, compliance and alignment with world regulatory policies.

3. Amendments to various existing laws, such as:

i. **IT Act, 2000**

   The amendments address the escalating dangers presented by AI-powered cybercrimes. They provide clear definitions, set out legal liabilities and establish penalties for using AI unlawfully. This creates a framework that makes not just the operators but also the developers and even end users of AI much more responsible for any cyber harms that might come from their AI-driven actions.

ii. RBI Act, 1934

To ensure responsible AI integration in financial services, these amendments bring AI-driven financial systems under RBI oversight, mandating registration, transparency, and consumer protection. By regulating algorithmic trading, credit scoring, and fraud detection, the framework balances innovation with accountability, mitigating systemic risks while fostering trust in AI-driven finance.

iii. Consumer Protection Act, 2019

To safeguard consumer rights in AI-driven services, these amendments introduce transparency, bias audits, and grievance redressal mechanisms. By ensuring explainability, the right to contest AI decisions, and proactive consumer awareness initiatives, the framework enhances trust, fairness, and accountability in AI-powered platforms.

4. International Harmonization

To facilitate secure cross-border AI deployment, this framework aligns India's regulations with global standards, ensuring seamless data exchange, AI transparency, and mutual recognition of certifications. By fostering international collaboration in research, dispute resolution and governance, it strengthens consumer protection while promoting India's leadership in AI-driven FinTech.

5. AI Transparency and Accountability

To ensure fairness and trust in AI-driven financial decisions, this framework mandates Explainable AI (XAI) standards and independent algorithm audits. By establishing a regulatory body for oversight, it enhances transparency, reduces biases and holds AI platforms accountable for ethical and accurate decision-making.

6. Strengthening Data Privacy and Protection

To safeguard consumer data in AI-driven financial systems, this framework aligns with the DPDP Act, 2023, mandating encryption, consent mechanisms and breach notifications. By regulating data localization and cross-border transfers, it ensures compliance with privacy laws while fostering trust in AI-powered services.

7. Encouraging Innovation

To drive AI and blockchain advancements in FinTech, this framework expands the RBI's regulatory sandbox, enabling controlled experimentation with AI-driven solutions. By offering tax incentives, funding R&D and supporting start-ups, it fosters innovation while ensuring regulatory compliance and consumer protection.

The next parts lay out these recommendations in detail, starting with the draft of the proposed Artificial Intelligence in Financial Technology Regulation Act, 2025 and concluding with Encouraging Innovations.

RECOMMENDATION 1: ARTIFICIAL INTELLIGENCE IN FINANCIAL TECHNOLOGY REGULATION ACT, 2025

CHAPTER I: PRELIMINARY

SECTION 1: SHORT TITLE, EXTENT, AND COMMENCEMENT

1. **Short Title**: This legislation shall be referred to as the "Artificial Intelligence in Financial Technology Regulation Act, 2025", abbreviated as the "AI in FinTech Act, 2025".
2. **Extent**: This Act extends to the whole of the Republic of India, including all states and union territories.
3. **Commencement**: The provisions of this Act shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint. Different dates may be appointed for different provisions of this Act. It is possible that different provisions of the Act might be made to 'commence' on different dates, which allows for a phased and prioritized approach to regulatory integration. The 'commencement phase,' if we may coin that term, would focus on building foundational infrastructure, on standing up the AI in FinTech Regulatory Authority (AIFRA), and on initiating the registration and certification process for existing, AI-driven financial systems. "Existing" means those systems that were in place before this Act was signed into law. This preparatory phase will be executed in such a way as to ensure that the subsequent phases are achieved with maximum clarity, minimum disruption, and sufficient efficiency to maintain the financial ecosystem's integrity.

Phase 1: Following from 6 Months of Enactment

(a) Establish the Authority of AI in FinTech Regulation (AIFRA) and its pivotal divisions (e.g., Division of AI Governance).

(b) Inform about necessary registration and certification provisions that pertain to already deployed AI systems.

Phase 2: Within 1 Year of Enactment

(a) Certify for transparency and compliance all AI-driven systems in financial operations.

(b) Publish guidelines for regulatory sandboxes, including blockchain-based AI projects and smart contracts.

(c) Commence in earnest consumer education concerning the new AI-driven financial services.

Phase 3: Within 2 Years of Enactment

(a) Impose penalties for failing to comply with AI certification, transparency, and bias-detection rules.

(b) Obtain international data-sharing agreements and develop collaborations to harmonize ethical standards.

(c) Broaden the regulatory framework to encompass quantum computing and new AI technologies.

Phase 4: Annual Evaluation and Revision

(a) Perform yearly evaluations of regulatory provisions to incorporate technological advancements and emerging challenges.

(b) Present yearly reports by AIFRA to Parliament on the governance of AI in FinTech.

Explanation:

- **Short Title**: The short title "Artificial Intelligence in Financial Technology Regulation Act, 2025" unambiguously designates the Act, making it straightforward to cite and refer to in legal and professional contexts.
- **Extent**: Saying that the Act applies to all parts of India guarantees that its provisions have the same effect in all kinds of jurisdictions across the country. This ensures consistency; it ensures that the same kind of regulation happens in all places where AI in Fintech is used in all the different kinds of jurisdictions we have in India.
- **Commencement**: Enabling the Central Government to appoint various commencement dates for different provisions allows the implementation process to be flexible. This approach permits a staged rollout, matching the

varied readiness of the numerous sectors and stakeholders to comply with the new rules and regulations.

SECTION 2: DEFINITIONS — In this Act, unless the context otherwise requires:

(1) Artificial Intelligence (AI): They can perceive, learn, and reason. Also, they can assist in decision-making, especially where output depends heavily on the learning from past experiences. Technologies that fall under AI include machine learning, natural language processing, and predictive analytics.

(2) Financial Technology (FinTech): The incorporation of modern technology into financial services; a subdivision of AI, blockchain, and the internet of things (IoT), with the aim to make financial operations run more smoothly and efficiently.

(3) Blockchain: A blockchain is a type of decentralized and immutable digital ledger that records transactions securely, transparently, and without the need of intermediaries.

(4) Smart Contract: A digital agreement that self-executes in accordance with the pre-set terms and conditions coded onto a blockchain, enforcing those terms automatically when pre-defined conditions are fulfilled.

(5) Explainable AI (XAI): AI systems built to give clear, understandable, and interpretable explanations of their decision-making processes.

(6) High-Risk AI Systems: AI systems that, because of their effect on financial stability or consumer rights, need to be held to a higher standard of regulatory oversight than what is normal, including systems used in credit scoring, detecting fraud, and algorithmic trading.

(7) Regulatory Sandbox: The Reserve Bank of India (RBI) establishes a controlled environment in which to test and validate innovative, AI-driven financial products, services, or business models. Office of Supervision manages this under the watchful eye of the regulator.

(8) Consumer: A single person or organization that employs financial products or services supplied by artificial intelligence-driven FinTech platforms.

(9) Bias in AI: Any systemic error or prejudice in AI systems that yields unfair or discriminatory outcomes, especially in financial decision-making contexts.

(10) Algorithmic Trading: The use of AI algorithms to handle financial trades at extraordinarily rapid speeds, based on a combination of real-time market conditions and pre-determined criteria.

(11) Data Protection: The safeguarding of personal and financial information processed by AI-driven FinTech platforms to ensure compliance with privacy regulations, including the DPDP Act, 2023.

(12) Data Localization: The requirement that sensitive financial data collected by AI systems be stored and processed within the territorial jurisdiction of India.

(13) Personal Data: Any information that relates to an identified or identifiable individual, including financial details, transactional data, and biometric identifiers.

(14) Cross-Border Data Flow: The transfer of personal or financial data across international borders by AI-driven systems, subject to regulatory approval and compliance with applicable laws.

(15) Liability: The legal responsibility of FinTech platforms, developers, or operators of AI systems for errors, fraud, or damages caused by the deployment of AI technologies.

(16) Digital Payment System: A technology-enabled platform that facilitates the transfer of funds electronically between individuals or entities.

(17) Fraud Detection System: An AI-powered system designed to identify and mitigate fraudulent activities within financial transactions.

(18) Risk Assessment: The evaluation of potential risks associated with AI-driven financial operations, including economic, ethical, and legal implications.

(19) Transparency: The principle of making the inner workings, decisions, and data processing methodologies of AI systems clear and comprehensible to users and regulators.

(20) Ethical AI: The development and deployment of AI technologies in a manner that aligns with societal values, fairness, and the protection of consumer rights.

Explanation

- The detailed and numerous definitions gives a clear and unequivocal notion on the crucial AI in FinTech notion that will abate any form of perplexity among the Act and therefore empowering the Act efficiency.
- Including terms like Bias in AI, Ethical AI, and Transparency reflects the focus on consumer rights and fairness.
- Definitions like Regulatory Sandbox and Cross-Border Data Flow align with modern regulatory needs and global interoperability.

CHAPTER II: SCOPE AND OBJECTIVES

SECTION 3: SCOPE AND APPLICABILITY

1. **Scope of the Act:**

   (a) All entities in India that use Artificial Intelligence (AI) for financial purposes are governed by this Act.

   (b) It includes banks, Non-Banking Financial Companies (NBFCs), digital payment platforms, peer-to-peer lending platforms, cryptocurrency exchanges, and other financial institutions utilizing AI in their operations.

   (c) The AI systems that this statute governs are utilized in:

      (i) Loan disbursement and scoring of credit.

      (ii) Trading and investment management by means of algorithms.

      (iii) Detection and prevention of fraud.

      (iv) Customer service automation and digital payment systems.

      (v) Financial systems based on blockchain, inclusive of smart contracts and DeFi (Decentralized Finance).

2. **Exemptions:**

   (a) The Act does not pertain to AI programs applied solely for back-office operations that do not engage consumers directly. It does apply, however, to back-office AI that has any impact on financial stability or consumer data security.

   (b) Entities working exclusively in the realm of experimental or research-focused AI systems that are under a regulatory sandbox may not have to follow many compliance requirements. These entities can be exempted from certain compliance requirements as long as they meet some conditions laid out by the Regulatory Authority.

SECTION 4: OBJECTIVES — The primary objectives of this Act are:

1. **Regulation of AI-Driven Financial Systems**: To craft a solid legal framework that governs the use of AI technologies in the financial sector so that they are used, in essence, to serve human and societal values.
2. **Consumer Protection and Fairness**: To maintain consumer rights and prevent algorithmic bias. Ensuring transparency in AI-driven decisions. And providing grievance redressal and dispute resolution.
3. **Data Protection and Privacy**: To guarantee compliance with the Digital Personal Data Protection (DPDP) Act, 2023, through the enforcement of

stringent directives regulating the gathering, safekeeping, processing, and transference of data by artificial intelligence (AI)-enhanced banking and financial services platforms.

4. **Mitigation of Risks and Liabilities:**
   (a) To uncover, evaluate, and lessen the risks tied to AI in FinTech, such as those related to financial inaccuracies, falsehoods, and cross-border complexities.
   (b) To delineate the liability in cases of financial fraud or system failure tied to AI.
5. **Harmonization with Global Standards**: To synchronize India's regulatory framework with the international standard, especially the ones set by the EU AI Act and other global regulatory frameworks, which promotes international cooperation and innovation.
6. **Encouraging Innovation**: To promote the development and adoption of new technologies, such as artificial intelligence, through regulatory "sandboxes", financial, and other support, and by ensuring compliance with legal and ethical standards.
7. **Blockchain and Smart Contracts**: To confer legal authenticity and structures upon financial transactions and smart contracts based on blockchain technology. This also involves tackling and resolving policy issues related to blockchain and smart contracts.
8. **Transparency and Explainability**: To require standards for Explainable AI (XAI) to be used in financial decision-making systems. This will ensure that both users and regulators are able to understand the decisions being made by AI-driven systems and to audit the rationale for those decisions.
9. **Establishment of Regulatory Oversight**: Creating an authoritative body for the AI in FinTech responsible for regulatory oversight, including compliance and enforcement, of this Act.

Explanation

- **Scope:** Unambiguously delineates the entities and activities regulated by the Act, guaranteeing far-reaching jurisdiction tempered by sensible exemptions that foster innovation.
- **Objectives:** Concentrates on achieving equilibrium between regulation and innovation, tackling risks, and ensuring consumer rights are protected. It resonates with India's data protection aims and is consistent with global best practices, making it not only a visionary but also a practical piece of legislation.

CHAPTER III: REGULATORY FRAMEWORKS

SECTION 5: HIGH-RISK AI SYSTEMS

1. **Definition of High-Risk AI Systems:**

   (a) AI systems that, because of what they do, how they're used, or how they might affect people, present the kinds of significant dangers that could threaten financial stability, consumer rights, or ethical standards.

   (b) Examples include AI systems used in:

   (i) **Credit Scoring and Loan Approvals:** Automated decision-making regarding the assessments of creditworthiness.

   (ii) **Fraud Detection and Prevention:** Systems using artificial intelligence monitor financial transactions for erroneous activities.

   (iii) **Algorithmic Trading:** High-frequency trading systems that can affect market volatility.

   (iv) **Insurance Underwriting:** Systems that determine who can get insurance, and at what price.

   (v) **Decentralized Finance (DeFi):** AI systems powered by blockchain facilitating decentralized financial transactions.

2. **Obligations for High-Risk AI Systems** — Entities deploying high-risk AI systems must:

   (a) **Perform Risk Evaluation:**

   (i) Assess threats inherent in the use of AI solutions, particularly when it comes to finances, operations, and ethics.

   (ii) Provide a comprehensive risk report to the AIFRA (AI in FinTech Regulatory Authority) prior to deployment.

   (b) **Obtain Certification:** Obtain certification from AIFRA that verifies adherence to regulatory standards, encompassing safety, transparency, and accountability.

   (c) **Implement Mitigation Measures:** Introduce safeguards to reduce risks, like frequent audits, supervision by humans, and mechanisms for Explainable AI (XAI).

   (d) **Ensure Explainability:** Give clear and open justifications for every decision an AI system makes, especially when it has profound implications for someone's life (e.g., denying credit, rejecting an insurance claim).

3. **Auditing and Monitoring Requirements:**

   (a) **Internal Audits:** Organizations must carry out periodic audits to evaluate conformity with ethical, legal, and technical standards.

   (b) **Third-Party Audits:** High-risk AI systems should have regular independent audits performed on them by certified third-party agencies.

   (c) **Regulatory Oversight:** AIFRA shall keep a watch on high-risk systems through regular checks and through the collection of data.

4. **Prohibited Practices:**

   (a) The high-risk AI systems must be compliant with the requirements. No high-risk AI that is non-compliant and non-certified shall be deployed.

   (b) In high-stakes situations, you can't use "black-box" opaque AI models that have no explainability.

   (c) Discriminatory practices or biases in financial decision-making that AI systems produce are prohibited.

5. **Consumer Safeguards:**

   (a) **Right to Explanation:** Individuals affected by high-risk AI decisions have the right to ask for comprehensive accounts and the particulars of the data used in the decision-making process.

   (b) **Redressal Mechanisms:** Set up unambiguous pathways for consumers to dispute AI-generated choices and obtain correction or remuneration.

   (c) **Bias Mitigation:** Require the application of bias-detection tools to guarantee fair and equal results from AI systems.

6. **Regulatory Sandbox Testing for High-Risk Systems:** Any entity that intends to roll out high-risk AI systems must first run those systems through the RBI's Regulatory Sandbox Environment, demonstrating not just safety but effectiveness as well, before going for a full scale development.

7. **Penalties for Non-Compliance:**

   (a) Entities using high-risk AI systems that are either uncertified or do not comply with regulations shall face:

      (i) Fines up to ₹1 crore for initial violations.

      (ii) Operating licenses suspended for repeated violations.

      (iii) Criminal accountability for intentional violations that yield economic damage to consumers.

Explanation

This section provides a sturdy framework for managing high-risk AI systems. Some pivotal points to note are:

- **Pre-emptive Measures:** Emphasis on risk assessments and certification ensures potential issues are addressed before deployment.
- **Consumer Protection:** Right to explanation and redressal mechanisms promote fairness and accountability.
- **Innovation with Safety:** Regulatory sandbox testing supports innovation while ensuring compliance and safety.
- **Prohibited Practices:** The prohibition of black-box AI and discriminatory algorithms is compatible with what is ethical.

SECTION 6: LICENSING AND REGISTRATION

1. **Licensing and Registration Required by Act:**

   (a) All entities using Artificial Intelligence (AI) systems for financial technology operations must acquire a license from the AI in FinTech Regulatory Authority (AIFRA) before they can deploy such systems.

   (b) It is imperative to ensure transparency, accountability, and regulatory compliance that these entities and their AI systems register.

2. **Eligibility Criteria for Licensing**—Entities seeking to obtain a license must:

   (a) Exist as an entity that is fully functional within India.

   (b) Show that the entities are compliant with the data protection laws, which include the Digital Personal Data Protection (DPDP) Act, 2023.

   (c) Deliver an all-inclusive report that describes the AI system's operations, designated applications, evaluated risks, and protective measures.

   (d) Provide evidence of strong data storage and protection, along with Explainable AI compliance.

   (e) Undergo a preliminary evaluation and examination by AIFRA.

3. **Registration Process:**

   (a) **Step 1:** Submit an application to AIFRA, including:

      (i) Specifics of the entity's legal form.

      (ii) Documentation of the AI system's architecture and intended applications.

      (iii) A report that assesses the potential risks, including ethical, legal, and financial ones.

   (b) **Step 2:** Pay the required registration fee, which will be set according to the scope and intricacy of the AI system.

   (c) **Step 3:** Wait for certification after AIFRA conducts review and approval.

   (d) **Step 4:** A unique license number will be awarded to successful applicants, good for five years and renewable upon verification of compliance.

4. **Obligations Post-Registration**—Entities must provide AIFRA with updates concerning:
   (a) Any substantial amendments to the AI framework.
   (b) Breaches, fraud, or mistakes caused by the AI system that lead to incidents of any kind.
   (c) Annual compliance audits, which outline how well the system works and whether it complies with the various regulations.
5. **Exemptions:**
   (a) Systems of artificial intelligence deployed solely for the purposes of research and experiment and in a regulatory sandbox environment may not have to obtain full licenses provided that:
      (i) The systems are non-commercial while being tested.
      (ii) They function beneath rigid supervision from AIFRA.
6. **Revocation and Suspension of Licenses:**
   (a) If any of the following conditions exist, the licenses may be suspended or revoked:
      (i) The organization does not meet regulatory requirements.
      (ii) Significant harm or bias is found to have been caused by the AI system.
      (iii) Annual audits reveal persistent non-compliance or violations of ethical standards.
7. **Public Registry of Licensed Entities:**
   (a) AIFRA shall maintain a public registry of all licensed entities and their AI systems to promote transparency.
   (b) The registry shall include:
      (i) The name and details of the entity.
      (ii) The type and purpose of the AI system.
      (iii) Certification status and renewal dates.
8. **Penalties for Non-Compliance**—Entities operating unlicensed AI systems shall face:
   (a) A penalty of up to ₹50 lakh for the first offense.
   (b) Suspension of operations until compliance is achieved.
   (c) Criminal liability for repeated violations leading to consumer harm.

Explanation

- **Purpose of Licensing and Registration:** Ensures that only compliant and safe AI systems operate in the financial sector, protecting consumer interests and financial stability.

- **Transparency:** A public registry builds trust and accountability, allowing consumers and regulators to verify the legitimacy of AI-powered financial platforms.
- **Adaptability:** Exemptions for sandbox testing encourage innovation without compromising oversight.
- **Enforcement Mechanism:** Clear penalties and the revocation process deter non-compliance and unethical practices.

SECTION 7: AUDITS AND MONITORING REQUIREMENTS

1. **Mandatory Audits for AI Systems:**
   (a) All AI systems deployed in financial operations must undergo periodic audits to ensure compliance with legal, ethical, and technical standards.
   (b) Audits must address:
      (i) Data protection and privacy adherence.
      (ii) Transparency and Explainable AI (XAI) compliance.
      (iii) Risk mitigation measures for algorithmic bias and systemic errors.
2. **Types of Audits:**
   (a) **Internal Audits:** Conducted by the entity's compliance team on a quarterly basis to ensure day-to-day adherence to regulatory requirements.
   (b) **Third-Party Audits:**
      (i) Entities must engage certified independent audit firms for an annual audit of their AI systems.
      (ii) The AI in FinTech Regulatory Authority (AIFRA) must receive the audit report within 30 days of completion.
   (c) **Special Audits**—AIFRA may direct that special audits be conducted in the following circumstances:
      (i) Non-compliance and consumer grievances that were reported.
      (ii) Systemic failures or fraud are suspected.
3. **Key Audit Parameters:**
   (a) **Algorithmic Transparency:** Auditors must assess the AI system's explainability and decision-making processes.
   (b) **Data Usage Compliance:** Ensure compliance with the DPDP Act, 2023, especially with respect to data collection, processing, and storage.
   (c) **Bias Detection:** Evaluate the mechanism for possible prejudices or discriminatory activities in the financial decision-making processes.

(d) **Error and Failure Analysis:** Examine logs for system errors, failures, and their fixes.

(e) **Security Protocols:** Assess how strong the cybersecurity measures are at preventing unauthorized access or breaches.

4. **Monitoring by AIFRA**—AIFRA shall establish a dedicated **Monitoring and Compliance Division** to:

(a) Examine yearly and extraordinary audit reports that entities submit.

(b) Perform unannounced checks and in-person oversight of AI systems deemed most likely to pose risks.

(c) Keeping a compliance database that tracks the performance and any incidents linked to AI systems that are registered.

5. **Audit Certification:**

(a) Entities will be awarded an AI Compliance Certificate for successful completion of the audit. This Certificate is valid for one year.

(b) This certificate's renewal depends on audits that are yet to be completed and on compliance with a set of rules that might change.

6. **Audit Failures and Non-Compliance:**

(a) If an audit shows major non-compliance, AIFRA might:

(i) Issue a compliance notice, requiring corrective actions to be taken within a set timeframe.

(ii) Impose penalties or suspend licenses for repeated violations.

(b) If entities do not fix the problems pointed out in audits, they may be suspended from operating or have their licenses taken away.

7. **Technology Upgrades and Monitoring:**

(a) Any significant upgrades or changes to their AI systems must be reported to AIFRA by entities.

(b) Systems with changes might need to be re-audited and re-certified prior to being put back into operation.

8. **Reporting of Incidents:**

(a) To AIFRA, entities must report the following within 48 hours:

(i) Consumer information involved in data breaches.

(ii) Major system breakdowns or flaws.

(iii) Fraud or misconduct associated with AI systems.

9. **Public Reporting:**

(a) An annual State of AI in FinTech Report shall be published by AIFRA, which will provide comprehensive details on:

(i) Trends in compliance.

(ii) Outcomes of audits throughout the industry.

(iii) Main difficulties and regulations update.

10. **Penalties for Non-Compliance:**

(a) Not conducting required audits or not submitting reports shall result in:

(i) A penalty of ₹25 lakh for initial infringements.

(ii) Increased fines for repeated violations.

(iii) License suspension for entities displaying persistent non-compliance.

Explanation

- **Purpose of Audits:** Ensures AI systems in financial operations are transparent, fair, and secure, reducing risks to consumers and financial stability.
- **Monitoring Mechanisms:** Continuous oversight by AIFRA ensures compliance and identifies risks early.
- **Consumer Confidence:** Public reporting and mandatory certifications build trust in AI-powered financial systems.
- **Proactive Measures:** Requiring entities to report incidents promptly ensures quick regulatory intervention.

CHAPTER IV: DATA PROTECTION AND PRIVACY

SECTION 8: DATA PROTECTION AND PRIVACY

1. **Alignment with Existing Laws:** All entities utilizing AI in financial technology must adhere to the provisions of the Digital Personal Data Protection (DPDP) Act, 2023 and other relevant data protection laws.
2. **Consumer Consent:**

(a) Entities must obtain explicit, informed consent from users before collecting, processing, or sharing their personal or financial data.

(b) Consent must be:

(i) Specific to the purpose of data usage.

(ii) Revocable by the user at any point.

3. **Data Minimization:**

(a) Entities shall collect only the minimum amount of data required to achieve the intended purpose of the AI system.

(b) Unnecessary data storage and processing are strictly prohibited.

4. **Data Localization:** Sensitive financial data of Indian consumers must be stored and processed within India, in compliance with localization requirements under the DPDP Act, 2023.
5. **Cross-Border Data Transfers:**
   (a) Entities must obtain prior approval from the **AI in FinTech Regulatory Authority (AIFRA)** for transferring personal or financial data outside India.
   (b) Such transfers shall be permitted only if the recipient country provides equivalent data protection standards.
6. **Data Security Measures:**
   (a) Entities must implement robust cybersecurity measures to protect consumer data, including:
      (i) End-to-end encryption of sensitive information.
      (ii) Regular security audits to identify and address vulnerabilities.
      (iii) Multi-factor authentication for access to critical systems.
7. **Rights of Consumers**—Consumers shall have the right to:
      (a) Access their data processed by AI systems.
      (b) Correct their inaccurate data.
      (c) Upon request, delete their data, complying with legal and regulatory mandates.
      (d) Get an accounting of how decisions made by AI affect their financial situation.
8. **Transparency in Data Usage**—Entities must disclose to consumers:
      (a) The type of data being collected.
      (b) The purpose of data processing.
      (c) If and for what purpose the data will be shared with third parties.
9. **Data Breach Notification**—In the event of a data breach:
      (a) If a breach occurs, entities must alert AIFRA and impacted consumers within 48 hours of becoming aware of the breach.
      (b) The notification shall include:
         (i) The breach's nature and extent.
         (ii) Steps taken to mitigate the risk.
         (iii) Steps consumers can take to safeguard themselves
10. **Audit and Compliance:**
    (a) Conducting regular data audits is necessary to guarantee that privacy laws are upheld.
    (b) AIFRA shall receive submission of audit reports on an annual basis.

11. **Penalties for Data Violations:**
    (a) Data protection and privacy requirement non-compliance shall result in:
        (i) Penalties can go as high as ₹1 crore for violations like data breaches or sharing information without the user's permission.
        (ii) Increased consequences for offenders who repeatedly violate or breach secure, sensitive data.
    (b) Criminal liability could attach in instances of intentional negligence or fraudulent schemes involving consumer data.
12. **Consumer Awareness Initiatives:** AIFRA shall conduct periodic campaigns to educate consumers on their data rights and protections under this Act.

Explanation

- **Consumer-Centric Approach:** Emphasis on informed consent, transparency, and user rights ensures that data protection is at the forefront of AI-driven financial systems.
- **Alignment with Global Standards:** Localization and cross-border data transfer requirements align with international best practices while safeguarding national interests.
- **Proactive Security Measures:** Breach notifications and audits provide a robust framework for addressing data security risks.
- **Accountability:** Penalties for violations ensure that entities prioritize consumer data protection.

CHAPTER V: BLOCKCHAIN AND SMART CONTRACTS

SECTION 9: BLOCKCHAIN AND SMART CONTRACTS

1. **Legal Recognition of Blockchain:**
    (a) Transactions and records based on blockchain technology shall be legally recognized under this Act, provided that they meet the qualifications specified by the authority established in this Act.
    (b) This acknowledgment encompasses financial dealings, data storage, and the carrying out of smart contracts.
2. **Definition and Scope of Smart Contracts:**
    (a) Self-executing digital agreements in which the terms are encoded in a blockchain are called smart contracts.
    (b) This Act applies to smart contracts used in:

(i) Loans, insurance, and investment contracts are all financial agreements.

(ii) Payments and remittances that are automated.

(iii) Platforms for lending directly between individuals and for decentralized finance.

3. **Mandatory Compliance for Smart Contracts**—All smart contracts must:

(a) Be auditable and transparent.

(b) Embed dispute resolution clauses within the code or govern them via external mechanisms.

(c) Before deploying in financial systems, AIFRA must review and certify it.

4. **Dispute Resolution Mechanisms:**

(a) Disputes that come up from smart contracts shall be addressed through:

(i) Mechanisms for minor dispute arbitration based on blockchain technology.

(ii) Established legal routes for complex or unresolved matters.

(b) AIFRA will set up a Smart Contract Dispute Resolution Cell (SCDRC) to take care of grievances and arbitration demands.

5. **Immutability and Error Handling:**

(a) Provisions must be included to:

(i) Correct mistakes in contract execution, such as wrong inputs or coding errors.

(ii) Limited mutability is allowed under certain specified conditions and requires AIFRA approval.

(b) In cases of fraud or error, a mechanism can be introduced that rolls back the affected transactions.

6. **Auditing and Certification of Blockchain Systems:**

(a) Financial operational blockchain systems require:

(i) Technical audits carried out on a regular basis to guarantee safety and regulatory compliance.

(ii) Certification by independent third-party auditors validated by AIFRA.

(b) Annual submission of certification reports to AIFRA is required.

7. **Data Security and Privacy:**

(a) Data security and compliance with the Digital Personal Data Protection (DPDP) Act, 2023, are must for blockchain systems.

(b) The blockchain must be a very secure platform. Sensibly sensitive data placed therein must be encrypted and accessible only to a limited number of authorized personnel.

8. **Interoperability Standards:** Blockchain systems must adhere to interoperability standards established by AIFRA to facilitate seamless integration across platforms and jurisdictions.
9. **Penalties for Non-Compliance:**
   (a) Entities that deploy smart contracts or blockchain systems that do not comply with the required regulations shall face:
      (i) Fines of up to ₹50 lakh for initial violations.
      (ii) For repeated violations, operations may be suspended.
      (iii) Criminal responsibility where there is deliberate deception or fraudulent use of the blockchain technology.
10. **Encouraging Blockchain Innovation:**
    (a) The AIFRA shall incentivize innovation in blockchain technology—this encompasses tax benefits and funding support for start-ups in the space.
    (b) New blockchain solutions will be able to test their products in regulatory sandboxes under controlled conditions.
11. **Consumer Protection**—Consumers using blockchain-powered financial systems shall be entitled to:
    (a) Clear information about how smart contracts work and the risks they involve.
    (b) Ways to communicate grievances and seek redressal.
    (c) Safeguards against deceptive practices or wrongful dealings.

Explanation

- **Legal Recognition:** Establishing the legal validity of blockchain and smart contracts ensures their integration into India's financial and legal systems.
- **Consumer Safeguards:** Including error-handling mechanisms and grievance redressal enhances trust in blockchain-based systems.
- **Promoting Innovation:** Encouraging blockchain technology through sandboxes and incentives balances regulation with innovation.
- **Accountability:** Auditing, certification, and penalties deter misuse and ensure compliance.

CHAPTER VI: CONSUMER PROTECTION

SECTION 10: CONSUMER PROTECTION

1. **Right to Explanation:**

   (a) Individuals affected by AI-powered fiscal determinations, like the approving of loans or scoring of credit, shall have the right to request:

   (i) The rationale behind the decision is explained.

   (ii) Access to the data that was utilized in making the decision.

   (b) The explanation must be given in clear and understandable language within 15 working days of the application's submission.

2. **Prevention of Algorithmic Bias:**

   (a) Financial operations AI systems must be designed and assessed to remove from them any discriminatory practices based on:

   (i) Gender, caste, religion, ethnicity, disability, or socioeconomic status.

   (b) Entities shall employ algorithms for finding bias to guarantee the fairness and equity of decision-making.

3. **Grievance Redressal Mechanisms:**

   (a) Dedicated grievance redressal cells must be established by entities to resolve consumer complaints related to:

   (i) Financial errors driven by AI.

   (ii) Fraud or misuse of consumer data.

   (iii) Outcomes that are discriminatory or biased.

   (b) Must grievances be resolved within 30 days if they are to be escalated to the AI in FinTech Regulatory Authority (AIFRA)

4. **Data Privacy and Security:**

   (a) Consumers shall have the right to:

   (i) Approve or disapprove the acquiring of their personal and financial data by AI systems.

   (ii) Withdraw consent for data usage at any time, provided there aren't any legal obligations to retain the data.

   (b) Entities must inform consumers of data breaches that involve their information within 48 hours.

5. **Proactive Consumer Education**—AIFRA, in collaboration with licensed entities, shall:

   (a) Conduct awareness campaigns periodically on the rights of consumers in AI-driven financial services.

   (b) Issue guides and frequently asked questions to enlighten consumers about AI systems and the effects they have.

6. **Protection from Fraud and Errors:**
   (a) Consumers shall be entitled to compensation for financial harm they suffer that is caused by:
      (i) Errors in AI decision-making.
      (ii) Activities that AI systems help make fraudulent.
   (b) Compensation claims must be processed within 60 days of filing with the concerned entity or AIFRA.
7. **Transparency Requirements**—Entities must disclose to consumers:
   (a) The manner in which their data is being collected, processed and utilized.
   (b) If and when data is shared with third parties, what do they share and why?
   (c) The hazards and constraints of employing AI-powered financial services.
8. **Consumer-Centric AI Development:**
   (a) When developing AI systems, you must concentrate on augmenting the user experience, guaranteeing simplicity, and cultivating trust.
   (b) Consumer feedback loops will be integrated into system updates and improvements.
9. **Prohibition of Predatory Practices:**
   (a) Consumers must not be exploited by AI systems, which includes:
      (i) Providing loans with concealed conditions or with excessively high-interest rates
      (ii) Practices, manipulative in nature, directed at susceptible groups.
10. **Penalties for Consumer Rights Violations:**
   (a) Under this Act, entities that infringe upon consumer rights shall face:
      (i) Fines reaching as high as ₹1 crore for serious infringements.
      (ii) Licenses may be revoked for being persistently non-compliant.
   (b) In cases of intentional fraud or damage, criminal responsibility.
11. **Consumer Protection Ombudsman**—AIFRA shall appoint a **Consumer Protection Ombudsman** to:
   (a) Resolve the unresolved consumer complaints.
   (b) Ensure adherence to consumer protection provisions.
   (c) Suggest punishments or remedial actions for violators.

Explanation

- **Empowerment of Consumers:** Rights such as explanation, transparency, and grievance redressal ensure that consumers remain at the center of AI-driven financial systems.
- **Bias Prevention:** Proactive measures to prevent algorithmic bias foster trust and inclusivity.

- **Quick and Effective Remedies:** The establishment of redressal mechanisms and the Ombudsman ensures swift resolution of consumer issues.
- **Transparency and Accountability:** Disclosure requirements and anti-predatory practices safeguard consumers from exploitation.

CHAPTER VII: PROMOTING INNOVATION AND TESTING

SECTION 11: INNOVATION AND TESTING

1. **Establishment of Regulatory Sandboxes:**
   (a) There shall be established a dedicated Regulatory Sandbox Framework by the AI in FinTech Regulatory Authority (AIFRA). This Framework will focus on supporting innovation in AI-driven financial technologies.
   (b) The environment for testing shall be controlled, and the sandbox shall provide it.
      (i) Credit scoring, fraud detection, and algorithmic trading now have new AI algorithms.
      (ii) Financial systems and smart contracts based on blockchain technology.
      (iii) Tools for consumer service powered by artificial intelligence, like chatbots and virtual assistants.
2. **Eligibility for Participation in the Sandbox:**
   (a) Startups, financial institutions, and technology developers wishing to test new, innovative AI solutions can apply.
   (b) Eligibility criteria include:
      (i) A clear proposal shows how this innovation could really impact things.
      (ii) Adherence to fundamental consumer protection and data privacy standards.
      (iii) A risk assessment report that outlines the safeguards that will be employed during testing.
3. **Sandbox Testing Process:**
   (a) Phase 1: Application and Approval: Entities must present a comprehensive application to AIFRA, detailing technical specifications, aims, and a plan for testing.

(b) Phase 2: Testing Period:

(i) Entities that have received approval shall carry out tests in the sandbox and under the supervision of AIFRA.

(ii) The testing phase must not last longer than 12 months unless an extension is granted under truly exceptional circumstances.

(c) Phase 3: Evaluation and Reporting: AIFRA requires entities to provide a final report that details the outcomes, any encountered challenges, and the compliance measures taken during the testing.

4. **Flexibility in Regulations for Sandbox Participants:**

(a) Temporary exemptions from certain regulatory requirements may be granted to entities in the sandbox, under the condition that:

(i) The measures for consumer protection are not compromised.

(ii) Standards for data privacy are adhered to.

(b) Testing period exemptions shall be allowed for only the duration of the testing period.

5. **Encouraging Collaboration**—The sandbox framework shall promote collaboration between:

(a) Institution of finance and technology start-ups.

(b) Researchers in academia and developers in financial technology.

(c) Standards to be harmonized by domestic and international regulators.

6. **Innovation Incentives:**

(a) Incentives shall be provided by AIFRA to encourage innovation in AI-driven financial systems, which shall include:

(i) Benefits in taxation for organizations participating in sandbox testing.

(ii) Availability of funds and grants for promising projects.

(iii) Acknowledgment and credentials for fruitful innovations.

7. **Monitoring and Evaluation:**

(a) The sandbox activities must be continuously supervised by AIFRA to:

(i) Ensure adherence to safety and ethical standards.

(ii) Identify possible risks and aspects of the regulatory structure that could be improved.

(b) Insights and best practices shall be shared in annual reports on sandbox outcomes.

8. **Transition from Sandbox to Full Deployment**—Entities demonstrating successful outcomes in the sandbox may transition to full deployment by:

(a) Applying for the certification and licensing under this Act.

(b) Carrying out the recommendations of AIFRA to correct detected risks or problems.

9. **International Collaboration**—AIFRA shall collaborate with global regulatory bodies to:
   (a) Assist in testing AI-based financial technologies across borders.
   (b) Set interoperability standards for AI systems and blockchain networks.
   (c) Share best practices and insights about regulatory sandbox frameworks.
10. **Penalties for Non-Compliance in the Sandbox**—Entities violating sandbox rules or failing to address identified risks shall face:
    (a) Entities will be suspended immediately from the sandbox.
    (b) For intentional violations, fines can go up to ₹25 lakh.
    (c) Future participation in the sandbox may be jeopardized if found ineligible.

Explanation

- **Promotes Innovation:** Regulatory sandboxes provide a safe space for developing and testing new technologies without immediate regulatory constraints.
- **Support for Startups:** Offering tax benefits and funding incentives encourages small players to participate and innovate.
- **Regulatory Oversight:** Continuous monitoring ensures that sandbox activities align with ethical, legal, and safety standards.
- **Global Integration:** Encouraging cross-border collaboration enhances India's competitiveness in the global FinTech ecosystem.

SECTION 12: ENFORCEMENT AND PENALTIES

1. **Establishment of Enforcement Mechanisms:**
   (a) The **AI in FinTech Regulatory Authority (AIFRA)** shall be empowered to:
      (i) Monitor compliance with this Act.
      (ii) Look into infringements or contraventions by organizations using AI technologies in their financial operations.
      (iii) Apply penalties and sanctions to achieve compliance.
2. **Categories of Violations:** Violations under this Act shall be classified into the following categories:
   (a) **Minor Violations:** Lapses in procedure, delays in reporting, or failure to present necessary documentation.

(b) **Major Violations:** Not following the audit requirements, breaching data privacy, or failing to meet consumer protection standards.

(c) **Severe Violations:** Use of AI systems without the proper licenses, deceptive practices, or behaviours that cause meaningful damage to the consumer or the economy.

3. **Penalties for Minor Violations:**

(a) Entities committing minor violations shall face:

(i) A notice of warning and rectification.

(ii) For repeated offenses, fines can total as much as ₹10 lakh.

4. **Penalties for Major Violations:**

(a) Major violations will subject entities to:

(i) Penalties between ₹25 lakh and ₹1 crore, depending on how severe the infringement is and its consequences.

(ii) The entity's license or registration may be temporarily suspended.

(iii) Compliance training that is mandatory for the entity's leadership and employees.

5. **Penalties for Severe Violations:**

(a) Serious breaches will lead to:

(i) For first offenses, fines may reach as high as ₹5 crore.

(ii) The entity's license shall be permanently revoked for repeated offenses.

(iii) Individuals guilty of committing deliberate fraud or misconduct face criminal liability, including a potential prison sentence of up to 3 years.

6. **Enforcement Actions by AIFRA:**

(a) **Inspections and Investigations:** AIFRA may conduct surprise inspections and may initiate investigations into suspected violations.

(b) **Freezing Operations:** AIFRA shall have the authority to freeze the operations of entities that are not in compliance, doing so to prevent any further detriment or violations.

(c) **Public Disclosure:** Information about significant and serious breaches will be made public in AIFRA's yearly compliance report, in the interest of transparency and to deter wrongdoing.

7. **Appeals Mechanism:**

   (a) This Act allows entities that have been penalized to appeal to the Appellate Tribunal for AI in FinTech. They have 30 days from receiving the penalty order to do so.

   (b) The Tribunal shall adjudicate appeals within 60 days and may uphold, modify, or overturn the penalties imposed by AIFRA. The Tribunal shall hear appeals and shall make decisions in 60 days and may uphold penalties, modify penalties, or overturn penalties.

8. **Whistle-blower Protections:** Individuals who report violations of this Act are shielded from retaliation under AIFRA's Whistle-blower Protection Framework.

9. **Incentives for Voluntary Disclosure:**

   (a) Entities that are not compliant or have breaches that they want to remedy can report these matters to AIFRA.

      (i) Lower penalties if they take corrective actions quickly.

      (ii) Waivers for self-reported minor violations that are first-time occurrences

10. **Penalties for Obstruction of Enforcement:**

    (a) Entities obstructing AIFRA's inspections or investigations shall face:

       (i) Fines up to ₹50 lakh.

       (ii) Individuals who take obstructive actions will face additional penalties.

11. **Consumer Compensation:**

    (a) Responsible entities that violate laws in serious ways causing consumer harm shall:

       (i) Within 60 days of making a determination, compensate money to harmed customers.

       (ii) Set up a fund for restitution to remedy the extensive damage done by systemic failures.

12. **Continuous Monitoring and Evaluation:**

    (a) AIFRA shall establish a Compliance Monitoring Division to:

       (i) Adhere to and monitor compliance trends in the industry

       (ii) Provide updated rules and recommendations derived from observed patterns of non-compliance.

Explanation

- **Graduated Penalties:** Categorizing violations ensures proportional responses, deterring misconduct without stifling innovation.

- **Transparency and Accountability:** Public disclosure of major violations builds consumer trust and sets an example for other entities.
- **Appeals and Protections:** An appeals mechanism and whistle-blower protections safeguard fairness and encourage accountability.
- **Restitution Measures:** Consumer compensation mechanisms emphasize the consumer-first approach of this Act.

CHAPTER VIII: ESTABLISHMENT AND GOVERNANCE

SECTION 13: AI IN FINTECH REGULATORY AUTHORITY (AIFRA)

1. **Establishment of the Authority:**
   (a) AI in FinTech regulatory authority must be established with a dedicated regulator under India's finance ministry.
   (b) AIFRA shall function as an autonomous authority with the mandate to regulate, monitor, and enforce compliance under this Act.
2. **Composition of AIFRA:**
   (a) **Chairperson:** A person with specialized knowledge in financial technologies, named by the Central Government.
   (b) **Members:**
      (i) Delegates from the Reserve Bank of India (RBI).
      (ii) Expert authorities in AI, blockchain, and cybersecurity.
      (iii) Professionals in law with knowledge in the fields of finance and technology.
      (iv) Advocates for consumer rights.
   (c) **Tenure:** A member shall get to serve a term of five years and can opt for one renewal as a second term.
3. **Functions and Responsibilities of AIFRA:**
   (a) **Regulation and Oversight:**
      (i) Formulate and enforce regulatory benchmarks for artificial intelligence in financial operations.
      (ii) Certify and license organizations that are implementing AI systems within FinTech.
   (b) **Monitoring and Compliance:**
      (i) Carry out audits and inspections of registered entities to ensure adherence to regulations and compliance.
      (ii) Keep a compliance register that the public can access.

(c) **Dispute Resolution:** Serve as an appellate body for resolving disputes pertaining to artificial intelligence systems and smart contracts.

(d) **Policy Development:** Propose changes to this Act and other relevant laws that would resolve new problems—problems that artificial intelligence and its fintech offspring are creating in our economy and daily lives.

(e) **Consumer Protection:** Ensure fair and decent treatment for consumers impacted by AI systems and address their grievances.

4. **Powers of AIFRA:**

(a) **Rulemaking Authority:** Under this Act, they are to make rules, guidelines, and standards.

(b) **Enforcement Actions:** Levy monetary fines, cancel operating licenses, and begin court proceedings against organizations that fail to comply.

(c) **Investigative Powers:**

(i) Carry out inquiries into alleged breaches or systemic faults.

(ii) Demand documents and issue summons to entities under investigation.

(d) **Advisory Role:** Offer authoritative guidance to the Central Government concerning policies that pertain to AI in financial systems.

5. **Funding and Resources:**

(a) AIFRA shall be funded through:

(i) Grants dispensed by the central government.

(ii) Licensing and penalties fees collected.

(b) To carry out its mandate, the authority may employ as needed technical and legal experts.

6. **Technology Infrastructure:**

(a) Establish advanced monitoring tools for:

(i) Financial systems driven by AI must be tracked in real time.

(ii) Analyzing trends in the performance and compliance of algorithms.

(b) Keep a secure repository of data for details provided by registered entities.

7. **Collaboration with Other Authorities**—AIFRA shall work in collaboration with:

(a) Regulatory sandbox initiatives from the Reserve Bank of India (RBI).

(b) Ministry of Electronics and Information Technology (MeitY) regarding technical standards related to artificial intelligence.

(c) Authorities for addressing consumer complaints and resolving consumer grievances.

8. **Public Reporting and Transparency**—Publish an **Annual Report** detailing:
   (a) The condition of artificial intelligence in financial technology, which comprises compliance innovations and trends.
   (b) Enforcement actions taken and major violations.
   (c) Policy recommendations for the government and industry.
9. **Innovation and Research Support:**
   (a) Establish a **Center for AI in FinTech Innovation (CAIFI)** to:
      (i) Foster research and development in ethical AI and blockchain technologies.
      (ii) Organize workshops, conferences, and capacity-building programs for industry stakeholders.
10. **Accountability of AIFRA:**
   (a) The Central Government shall hold AIFRA accountable by:
      (i) Its functioning is subject to periodic audits.
      (ii) If challenged, its decisions may be reviewed by an independent appellate authority.

Explanation

- **Focused Governance:** AIFRA's establishment ensures a specialized, centralized approach to regulating AI in FinTech.
- **Expert-Led Composition:** Including diverse experts ensures a balance between technical, legal, and consumer perspectives.
- **Transparency and Innovation:** Public reporting and the promotion of innovation foster trust and industry growth.
- **Proactive Role:** AIFRA's ability to collaborate with other authorities and recommend policy updates ensures adaptability to technological advancements.

CHAPTER IV: MISCELLANEOUS PROVISIONS

SECTION 14: POWER TO MAKE RULES AND REGULATIONS

1. **Authority to Make Rules:** The Central Government, in consultation with the **AI in FinTech Regulatory Authority (AIFRA)**, shall have the power to make rules and regulations for carrying out the provisions of this Act.
2. **Scope of Rulemaking**—The rules and regulations may address, but are not limited to:
   (a) **Licensing and Registration:** Processes for application, authorization, reapproval, and license revocation.

(b) **Audit and Compliance Standards:** Directives for regular audits, certifications, and oversight of AI systems.

(c) **Consumer Protection Mechanisms:** Grievance redressal frameworks, compensation procedures, and the transparent functioning of these mechanisms ensure consumer protection.

(d) **Regulatory Sandbox Framework:** Rules governing eligibility, operational guidelines, and outcomes for sandbox participants.

(e) **Blockchain and Smart Contracts:** Standards for resolution of disagreements, management of mistakes, and interoperability.

(f) **Data Protection and Privacy:** The AI systems will follow specific data handling protocols to comply with the DPDP Act, 2023.

(g) **Penalties and Enforcement:** Specific schedules delineating the fines and actions for slight, serious, and grievous breaches.

(h) **Emerging Technologies:** Regulations for incorporating and controlling innovations not explicitly discussed in this Act.

3. **Consultative Process:**

(a) AIFRA must set up a consultative process with stakeholders, who include:

(i) Institutions that deal with finance, developers of technology, and groups that advocate for consumer rights.

(ii) Experts in AI, blockchain, and data protection from academia and the legal field.

(b) Public comments shall be obtained on draft rules before they are finalized.

4. **Publication and Notification:**

(a) This section shall have all rules and regulations formulated under it:

(i) Must be published in the Official Gazette.

(ii) Become effective on the date indicated in the notification.

5. **Periodic Review and Updates:**

(a) AIFRA shall periodically review the rules and regulations, at a minimum, once every three years, to address:

(i) Technological advancements.

(ii) Evolving industry practices.

(iii) Global regulatory standards.

6. **Binding Nature of Regulations:**

(a) The rules and regulations made under this section shall have mandatory effect on:

(i) All organizations and persons covered by this Act.

(ii) Organizations working under exemptions made in Section 21.

7. **Rulemaking in Exceptional Cases:**

   (a) In rare circumstances, the Central Government may shorten the rulemaking process to allow for immediate formulation of essential regulations when:

   (i) There is an immediate need for regulatory action to protect financial stability and consumer safety.

   (ii) There are new technologies or use cases that are significantly impacting the operations of FinTech firms.

8. **Judicial Review:** The rules and regulations that are made under this section will be subject to judicial review. This means they will be checked to see if they are in accord with the constitutional principles and this Act.

Explanation

- **Comprehensive Rulemaking Authority:** Allows flexibility in addressing current and emerging challenges, ensuring the Act remains relevant.
- **Stakeholder Involvement:** Promotes inclusivity and transparency in the regulatory process.
- **Periodic Updates:** Ensures adaptability to evolving technologies and industry needs.
- **Binding Nature:** Reinforces the enforceability of the Act's provisions.

SECTION 15: AMENDMENT OF EXISTING LAWS

1. **Objective of Amendments:**

   (a) Harmonize current legal frameworks to align them with the provisions of this Act, ensuring an all-encompassing regulation of AI in fintech

   (b) To tackle potential legal shortcomings that may stem from AI system integration in FinTech.

2. **Identification of Relevant Laws for Amendment:**

   (a) The laws and regulations listed below may be changed to include provisions that are aligned with this Act:

   (i) **Information Technology Act, 2000**: Inclusion of provisions for AI-specific cybercrime, algorithmic transparency, and liability in AI-driven transactions.

   (ii) **Reserve Bank of India Act, 1934**: An expansion of regulatory jurisdiction of the RBI that encompasses AI-empowered financial arrangements.

   (iii) **Consumer Protection Act, 2019**: This law adds consumer rights that pertain to Explainable AI (XAI) and also provides for grievance redressal in connection with AI-based decisions.

(iv) **Payment and Settlement Systems Act, 2007**: Inclusion of directives for payment systems driven by AI, for detecting fraud, and for auditing algorithms.

(v) **Companies Act, 2013**: Introduction of requirements for corporate accountability in the deployment of AI technologies.

3. **Procedure for Amendments:**

(a) The Central Government, in cooperation with pertinent ministries and regulatory bodies, will prepare amendments to the specified laws.

(b) Drafted amendments shall be:

(i) Published for public consultation.

(ii) Based on stakeholder feedback, revised and polished.

(c) Amendments that are final must be presented to Parliament so that they can be approved.

4. **Integration of AI-Specific Clauses:**

(a) Provisions shall be included in amendments for:

(i) Artificial Intelligence (AI) systems and their range of definitions in the realm of financial applications.

(ii) Mechanisms to hold accountable the people or organizations responsible for mistakes or biases in AI systems.

(iii) Adherence to data protection standards established in the DPDP Act, 2023.

(iv) Definite liability structures concerning financial decisions and frauds induced by AI.

5. **Harmonization with Global Standards:** International best practices must be followed when aligning amendments, and those amendments must ensure cooperation and innovation across borders. The alignment must especially involve the EU AI Act and other global frameworks, which represent leading-edge practices and standards.

6. **Timeline for Implementation:**

(a) Existing laws may be amended and shall be finalized and notified within 18 months from the date of enforcement of this Act.

(b) Affected entities shall have a 12-month grace period following the effective date of the amendment to ensure compliance.

7. **Monitoring and Review of Amendments:**

(a) AIFRA shall regularly assess how effective the amendments are and shall recommend further changes if they find them necessary.

(b) The Central Government shall receive every year reports on the effects of these amendments.

Explanation

- **Purpose:** Ensures that existing laws are updated to account for the unique challenges posed by AI in financial technology.
- **Comprehensive Approach:** Covers all major laws impacted by AI and FinTech integration, from cybersecurity to consumer protection.
- **Stakeholder Involvement:** Ensures amendments are practical, effective, and widely accepted.
- **Adaptability:** Provisions for periodic review allow the legal framework to evolve with technological advancements.

SECTION 16: PROTECTION OF ACTIONS TAKEN IN GOOD FAITH

1. **Immunity for Regulatory Actions:**
   (a) No suit, prosecution, or other legal proceeding shall be maintained against:
      (i) The Central Government.
      (ii) The **AI in FinTech Regulatory Authority (AIFRA)**, its officers, or employees.
      (iii) Any person acting under the authority or direction of AIFRA.
   (b) This immunity pertains to actions taken in good faith while fulfilling the duties or exercising the powers conferred by this Act.
2. **Scope of Protection:**
   (a) This section covers the following actions:
      (i) Licenses, certifications, or approvals issued.
      (ii) Penalties and compliance measures enforced.
      (iii) Conducting and performing inspections, audits, or investigations.
      (iv) Decisions made by regulators, which can include any of the following: granting approvals, suspending licenses, or revoking licenses.
      (v) Suggestions for changes or updates to legal and policy frameworks.
3. **Exclusions from Protection:**
   (a) Immunity shall not apply in cases where:
      (i) The action was taken with malicious intent.
      (ii) Gross negligence or wilful misconduct can be proven.
      (iii) An official acted outside the scope of authority assigned under this Act.

4. **Good Faith Presumption:** Under this Act, any action taken shall be presumed to be in good faith. The presumption may be rebutted only by proof, which must be shown to a judge that the action was not taken in good faith. The judge will determine the good faith of the acts alleged as a violation of this Act.
5. **Mechanism for Addressing Grievances Against Officials:**
   (a) If a party claims that an act was not performed in good faith, they may:
      (i) Submit a grievance to the Internal Oversight Committee (IOC), which AIFRA has set up.
      (ii) Seek judicial review in a court of law after exhausting administrative remedies.
6. **Protection for Stakeholders**—Protection under this section extends to:
   (a) Entities and individuals who comply with directives issued under this Act, provided their compliance was based on good faith reliance on such directives.
   (b) Experts, advisors, or consultants engaged by AIFRA in regulatory, investigative, or advisory roles.
7. **Accountability Mechanisms:**
   (a) While this section grants immunity, AIFRA shall maintain mechanisms to:
      (i) Review complaints against misuse of power by its officers or employees.
      (ii) Penalize officials found guilty of misconduct or gross negligence.

Explanation

- **Encourages Proactive Regulation:** Immunity ensures that regulators and officials can perform their duties without fear of litigation, provided their actions are in good faith.
- **Balance Between Protection and Accountability:** By excluding malicious intent or gross negligence from immunity, the section maintains checks on regulatory overreach.
- **Grievance Mechanisms:** Provides recourse for individuals or entities that feel wronged by regulatory actions, ensuring fairness.

SECTION 17: CONFIDENTIALITY OF INFORMATION

1. **Obligation to Maintain Confidentiality:**
   (a) Any information submitted to the **AI in FinTech Regulatory Authority (AIFRA)** by entities, individuals, or stakeholders under this Act shall be treated as confidential.

(b) Such information shall not be disclosed, shared, or published without explicit consent from the submitting party, except as provided under this section.

2. **Permissible Disclosures:**

(a) The following circumstances exist in which AIFRA may disclose confidential information:

(i) For investigation or enforcement purposes, to law enforcement agencies or other regulatory bodies.

(ii) Under legal obligations or court orders.

(iii) For the purposes of policymaking or administration, to the Central Government or the appropriate state governments.

(iv) In a form that maintains anonymity or aggregates enough data to prevent the identification of any individual or entity, for the purposes of research, reporting, or serving the public interest.

3. **Scope of Confidential Information:**

(a) Confidential information includes, but is not limited to:

(i) Technical and operational specifics of AI systems.

(ii) Intellectual property and proprietary algorithms.

(iii) Audited or compliance-checked financial and consumer record data.

(iv) Reports on incidents involving data breaches, system failures, or fraud.

4. **Data Handling and Storage:**

(a) AIFRA will create secure systems and protocols to ensure:

(i) Keeping sensitive data secure.

(ii) Limiting access to only those individuals who are authorized.

(iii) Preventing unauthorized access, breaches, or leaks.

5. **Non-Disclosure Agreements (NDAs):** AIFRA employees, contractors, and third-party consultants must sign NDAs promising the confidentiality of information they access in the course of their work.

6. **Penalties for Breach of Confidentiality:**

(a) Any individual convicted of improperly revealing confidential information shall face:

(i) Fines up to ₹50 lakh.

(ii) For breaches that are deliberate and malicious, criminal liability of up to two years in prison.

(b) For intentional breaches or those caused by negligence, entities found responsible may face:

(i) Fines up to ₹2 crore.

(ii) Their license under this Act being suspended or revoked.

7. **Consumer Protection in Confidentiality:**

   (a) Entities submitting consumer personal data to AIFRA shall do so under the provisions of the Digital Personal Data Protection (DPDP) Act, 2023.

   (b) Consumers shall have the right to:

   (i) Understand how their data is utilized or shared

   (ii) Object to or restrict the sharing of their data, unless mandated by law.

8. **Audit of Confidentiality Practices:**

   (a) AIFRA shall perform consistent audits of its data management and confidentiality practices to confirm adherence to compliance and security requirements.

   (b) An independent, third party auditor shall verify these practices every year.

9. **Whistle-blower Protections:** Individuals who blow the whistle on breaches of confidentiality occurring within AIFRA or among regulated entities will be safeguarded under the AIFRA Whistle-blower Protection Framework.

Explanation

- **Strict Confidentiality:** Ensures sensitive data remains secure, promoting trust between regulated entities, consumers, and the regulatory authority.
- **Permissible Disclosures:** Strikes a balance between confidentiality and necessary information sharing for enforcement and policy purposes.
- **Accountability and Penalties:** Provides robust mechanisms to deter breaches and hold violators accountable.
- **Consumer-Centric Approach:** Aligns with the DPDP Act, ensuring consumer data is prioritized and protected.

SECTION 18: APPEALS AND ADJUDICATION

1. **Right to Appeal:**

   (a) Any individual, entity, or stakeholder displeased by a decision, order, or penalty handed down by the AI in FinTech Regulatory Authority (AIFRA) under this Act shall have the right to appeal.

   (b) Appeals must be filed within 30 days of the decision or penalty notice being received.

2. **Appellate Tribunal for AI in FinTech (ATAF):**

(a) The Central Government shall create the Appellate Tribunal for AI in FinTech (ATAF) to hear and resolve appeals regarding this Act.

(b) **Composition:**

(i) Chairperson: A former judge of either the High Court or the Supreme Court.

(ii) Members:

(a) An expert in financial technology or AI systems.

(b) An experienced legal professional whose expertise extends to the areas of technology and finance law.

3. **Jurisdiction of ATAF**—ATAF shall have jurisdiction to:

(a) Hear appeals against orders issued by AIFRA.

(b) Settle disputes that occur under this Act, including those that pertain to:

(i) Licensing and certification.

(ii) Penalties for non-compliance.

(iii) Consumer grievances escalated beyond AIFRA.

4. **Adjudication Procedure:**

(a) Appeals must be filed in the required format and accompanied by all pertinent paperwork.

(b) ATAF shall ensure:

(i) A fair and transparent hearing process.

(ii) Resolution of appeals within 60 days from the date of filing, barring exceptional circumstances.

(c) Decisions of ATAF shall be binding on all parties and enforceable as per the provisions of this Act.

5. **Appeal to Higher Courts:**

(a) Parties dissatisfied with the decision of ATAF may appeal to the appropriate High Court within 60 days of the Tribunal's decision.

(b) Appeals to the High Court shall be limited to substantial questions of law.

6. **Alternate Dispute Resolution (ADR):**

(a) ATAF may recommend mediation or arbitration for resolving disputes, particularly in cases involving:

(i) Consumer grievances against AI-driven financial decisions.

(ii) Disputes between entities operating under this Act.

(b) ADR proceedings shall be concluded within 90 days, with outcomes enforceable under this Act.

7. **Enforcement of Tribunal Decisions:**
   (a) AIFRA shall be responsible for implementing the orders and decisions of ATAF.
   (b) Non-compliance with ATAF orders shall result in penalties or further legal actions as prescribed under this Act.
8. **Costs and Fees:**
   (a) ATAF may award costs to the winning party in appeals, considering the merits of the case and the conduct of parties during the proceedings.
   (b) Filing fees for appeals shall be prescribed and kept nominal to ensure accessibility.
9. **Transparency and Accountability:**
   (a) ATAF shall publish an annual report summarizing:
      (i) The number and types of appeals filed.
      (ii) The nature of disputes resolved.
      (iii) Trends and insights to inform policy development.
10. **Grievance Monitoring and Feedback:** ATAF shall maintain a grievance monitoring system to track unresolved disputes and consumer feedback on the adjudication process.

Explanation

- **Comprehensive Appeal Mechanism:** Ensures that aggrieved parties have a structured and efficient process to challenge regulatory decisions.
- **Expert-Led Adjudication:** The composition of ATAF ensures a balance of legal, technical, and financial expertise in resolving disputes.
- **Fair and Timely Resolution:** Defined timelines for hearings and decisions promote trust in the regulatory framework.
- **Transparency:** Publishing annual reports ensures public accountability and provides insights for improving the adjudication process.

SECTION 19: OFFENSES BY CORPORATIONS

1. **Corporate Accountability:**
   (a) If an offense under this Act is committed by a corporation, the company, along with any individual responsible for its management and operations, shall be deemed liable.
   (b) This includes directors, managers, officers, and other employees involved in the decision-making processes leading to the offense.

2. **Extent of Liability:**

(a) The liability of a corporation shall include:

(i) Financial penalties specified under this Act.

(ii) Licenses issued under this Act may be suspended or revoked.

(iii) Any civil liabilities that come about because of the offense.

3. **Liability of Responsible Individuals:**

(a) Individuals who oversee and are responsible for the running of the corporation's business will also be held personally liable unless they can prove:

(i) The crime was carried out without their awareness.

(ii) They took due diligence to prevent the offense.

4. **Exceptions:**

(a) No liability shall attach to individuals who:

(i) Were not engaged in the particular decision-making that resulted in the offense.

(ii) Can show proactive initiatives to make sure this Act is complied with.

5. **Offenses Involving AI Systems:**

(a) Specific violations pertinent to the use of AI systems encompass:

(i) Employment of non-compliant or uncertified AI technologies.

(ii) Fraudulent purposes for which AI algorithms are deliberately manipulated or tampered with.

(iii) Implementation of AI systems that result in considerable monetary damage to consumers or pose broad systemic threats to the financial sector.

6. **Enhanced Penalties for Wilful Violations:**

(a) Corporations committing deliberate violations shall face:

(i) Penalties up to ₹5 crore.

(ii) Criminal responsibility, including a prison term of as long as five years for individuals involved.

(b) If the offense causes substantial consumer damage or results in serious financial disruption, AIFRA might propose tougher consequences, such as banning the company from doing business.

7. **Reporting of Corporate Offenses:**

(a) Any offenses, violations, or breaches committed by their AI systems shall be reported by corporations to the AI in FinTech Regulatory Authority (AIFRA) within 48 hours of detection.

(b) Failure to report will constitute an additional offense, which comes with stiffer penalties.

8. **Whistle-blower Protections for Employees:**

   (a) Under this Act, whistle-blowers are protected when they report to us the offenses committed by their corporations.

   (b) Additional penalties, including suspension of licenses, shall be faced by corporations that retaliate against whistle-blowers.

9. **Restitution for Affected Consumers:**

   (a) Corporations that are found guilty must make repayment to affected consumers, comprising:

      (i) Monetary compensation for the damages done.

      (ii) Measures to rectify errors caused by their AI systems.

10. **Corporate Compliance Programs:**

    (a) Internal compliance programs must be put into place by corporations to prevent offenses. These programs must do the following:

       (i) Consistent training of the personnel concerning the stipulations of this Act.

       (ii) Regular audits of AI systems to identify risks and mitigate them.

       (iii) Appointing a compliance officer responsible for ensuring adherence to the Act.

11. **Repeat Offenses and Escalation:**

    (a) Corporations committing repeat offenses within five years shall:

       (i) Be subject to fines that equal double the amount of the original penalty.

       (ii) Be subject to oversight that is much stricter, including audits that are mandatory and conducted every month.

       (iii) Be risked of getting suspension of operations for up to two years.

Explanation

- **Corporate Accountability:** Ensures that corporations cannot escape responsibility for violations committed through their AI systems.
- **Balance Between Liability and Exceptions:** Protects individuals who have exercised due diligence while holding negligent parties accountable.
- **Consumer-Centric Approach:** Mandates restitution for consumers, ensuring they are not left to bear the consequences of corporate violations.
- **Deterrence:** Enhanced penalties for willful violations and repeat offenses discourage non-compliance.

CHAPTER X: SPECIAL PROVISIONS

SECTION 20: PROVISIONS FOR RESEARCH AND DEVELOPMENT

1. **Promotion of Ethical AI and Blockchain Research:**
   (a) The Central Government, together with the AI in FinTech Regulatory Authority (AIFRA), will take the lead in establishing initiatives that promote research and development in:
      (i) Ethical AI systems for financial applications.
      (ii) Solutions based on blockchain for secure and transparent financial operations.
      (iii) Frameworks for mitigating risks related to artificial intelligence (AI)-driven financial technologies.
2. **Establishment of Research Centers:**
   (a) The creation of dedicated Centers for AI and Blockchain Innovation shall be supported by AIFRA in collaboration with:
      (i) Research institutions and universities.
      (ii) Leaders in AI and FinTech industries.
      (iii) Worldwide technological entities.
3. **Incentives for Innovation:**
   (a) The following incentives shall be provided by the Central Government to encourage R&D:
      (i) **Tax Benefits:** Entities investing in AI and blockchain research can receive tax exemptions.
      (ii) **Grants and Funding:** Money grants to new businesses, universities, and other entities that allow them to carry out their research work on potentially pathbreaking AI systems.
      (iii) **Patent Support:** Assistance with filing for patents on new inventions in artificial intelligence and blockchain technology.
4. **R&D Partnerships:**
   (a) Foster collaborations between the public and private sectors to:
      (i) Create advanced AI systems for FinTech.
      (ii) Test blockchain solutions in regulatory sandboxes.
      (iii) Exchange knowledge and best practices through cooperative platforms.
5. **Fostering International Collaboration**—AIFRA shall:
   (a) Partner with global regulatory bodies and research institutions to harmonize standards.

(b) Facilitate knowledge exchange on emerging AI and blockchain technologies.

(c) Promote cross-border research projects in AI-driven financial technologies.

6. **Ethical and Inclusive Innovation:**

(a) R&D programs shall prioritize:

(i) The development of Explainable AI (XAI) for financial decision-making.

(ii) Tools to identify and mitigate algorithmic biases.

(iii) Accessible AI solutions for underserved populations, promoting financial inclusion.

7. **Monitoring and Evaluation of R&D Initiatives:**

(a) AIFRA shall establish a dedicated **R&D Oversight Committee** to:

(i) Oversee the advancement and influence of financed endeavours.

(ii) Assess the results of research projects every year.

(iii) Suggest policy refinements to manage the movement of technology.

8. **Publication of Research Outcomes:**

(a) Must publish key findings, to the maximum extent possible and consistent with applicable laws, which do not reveal any proprietary or sensitive information.

(i) Contribute to the extensive reservoir of knowledge.

(ii) Stimulate further innovation in AI and blockchain technology.

9. **Creation of a National AI and Blockchain Repository:**

(a) AIFRA will keep a repository of:

(i) Academic articles, patents, and case studies concerning artificial intelligence and blockchain technology within the realm of financial technology.

(ii) Best practices ensuring the ethical and transparent deployment of these technologies.

(iii) Tools and frameworks that are open source to speed up and boost innovation.

10. **Encouragement for Start-ups and SMEs:**

(a) The following special initiatives shall be implemented to support start-ups and small and medium enterprises (SMEs):

(i) Lower costs for taking part in regulatory sandboxes.

(ii) Grants and resources will be made available with priority access to very high-potential projects.

(iii) Programs for the mentorship of industry experts.

11. **Annual Innovation Report:**

(a) The Annual Innovation Report detailing the following shall be published by AIFRA:

(i) Significant research advancements and how they are shaping the FinTech ecosystem.

(ii) AI and blockchain adoption trends.

(iii) Suggestions for upcoming R&D priorities.

Explanation

- **Focus on Ethical Innovation:** Encourages the development of AI systems that are transparent, fair, and inclusive.
- **Resource Allocation:** Provides financial and structural support for R&D, ensuring India remains a leader in AI and blockchain innovation.
- **Global Competitiveness:** International collaboration positions India as a hub for cutting-edge research in FinTech technologies.
- **Accountability and Transparency:** Monitoring mechanisms and publication of research outcomes ensure effective utilization of resources.

SECTION 21: POWER TO EXEMPT CERTAIN ENTITIES

1. **Authority to Grant Exemptions:** The Central Government, in consultation with the **AI in FinTech Regulatory Authority (AIFRA)**, may exempt specific entities or categories of AI systems from compliance with certain provisions of this Act.
2. **Criteria for Exemptions**—Exemptions may be granted if:

   (a) The system or entity serves mostly in a capacity that is non-commercial or experimental. It may serve in a capacity for research, such as in an academic setting, or in some other non-commercial role.

   (b) Compliance would require these entities—start-ups, for example, or small-scale enterprises—that lack the financial means to pay for compliance, to bear a cost that is out of line with their size and resources.

   (c) The exemption serves the public interest, including progress in financial inclusion and ethical AI innovation.
3. **Categories of Exemptions:**

   (a) **Regulatory Sandbox Participants:** Entities that are testing AI-driven financial solutions under the regulatory sandbox framework may get some exemptions from full compliance during the testing phase.

(b) **Academic and Non-Profit Entities:** Research institutions and non-profits that use AI systems for educational or social welfare reasons may be eligible for exemptions.

(c) **Low-Risk AI Systems:** These systems are recognized as having little impact on either financial stability or consumer rights. As such, they may face relaxed regulatory requirements.

4. **Duration of Exemptions:**

(a) Exemptions shall be granted for a stipulated period that does not exceed two years. They may be renewed, however, and in those instances, the exemption authority would undoubtedly conduct a compliance review.

(b) AIFRA may at any time revoke exemptions when the requisite conditions are found to be in violation.

5. **Application Process for Exemptions:**

(a) Organizations wanting exemptions must file a formal application with AIFRA that includes:

(i) A complete account of the intended usage of the AI system and a detailed description of what it is.

(ii) Justifications for the exemption request.

(iii) Proof of Evidence that the minimum regulatory standards are being complied with.

(b) AIFRA will make a decision on the application within 60 days of submission.

6. **Conditions Attached to Exemptions:**

(a) Exempted entities must:

(i) Comply with fundamental data security and consumer protection regulations.

(ii) Send regular updates to AIFRA about how the systems are being used and the impact of their AI systems.

(b) Exemptions might involve particular conditions that address risk or ensure transparency.

7. **Public Disclosure of Exemptions:**

(a) AIFRA will uphold an accessible public registry that contains all exemptions it grants, and this will be explicated in detail.

(i) The name and type of the exempted entity or system.

(ii) Exempt provisions and duration of the exemption.

(iii) The conditions to which the exemption is attached.

8. **Revocation of Exemptions:**
   (a) Exemptions may be revoked if:
      (i) The exemption conditions are not satisfied by the entity.
      (ii) The exempted systems pose unforeseen risks to the stability of the financial sector, consumer safety, or data privacy.
   (b) Affected entities may appeal the decision to revoke their authority to the Appellate Tribunal for AI in FinTech (ATAF) within 30 days.
9. **Review of Exemption Policy:** Yearly review shall be conducted by AIFRA on exemption policies to ensure they are consistent with technological progress and the goals of regulation.

Explanation

- **Flexibility for Innovation:** Provides room for experimentation and innovation while maintaining safeguards for consumer protection and financial stability.
- **Support for Small Players:** Startups, SMEs, and non-profits benefit from relaxed regulations, fostering growth and innovation in FinTech.
- **Accountability and Transparency:** Public disclosure and reporting requirements ensure exemptions are granted responsibly and are subject to oversight.
- **Dynamic Policy:** Regular reviews allow exemption policies to adapt to the evolving needs of the industry.

SECTION 22: TRANSITIONAL PROVISIONS

1. **Application to Existing Entities and AI Systems:**
   (a) All entities using AI systems for financial operations prior to this Act's commencement must comply with this Act's provisions within a stipulated time.
   (b) This includes entities operating:
      (i) AI-driven financial platforms.
      (ii) Systems based on blockchain technology for the purposes of payments or maintaining financial records
      (iii) AI systems with a high risk used for credit scoring, fraud detection, and algorithmic trading.
2. **Registration and Licensing Grace Period:**
   (a) Existing entities shall:

(i) Within six months of the Act coming into force, apply for registration and licensing with the AI in Fintech Regulatory Authority (AIFRA).

(ii) Ensure compliance to all functional, data security, and consumer protection laws within one year of the Act's commencement

3. **Certification for Deployed AI Systems:**

(a) AI systems already in use must:

(i) Have an audit conducted and obtain AIFRA certification within 12 months of the Act's commencement.

(ii) Put into effect any recommendations given during the certification process within three months of receiving the associated feedback.

4. **Provisions for Ongoing Contracts:**

(a) Financial contracts that were executed using artificial intelligence or blockchain prior to the enactment of this law shall remain valid

(b) Nevertheless, these contracts must adhere to the provisions laid out in this Act when it comes to future changes or renewals.

5. **Phased Implementation for High-Risk Systems:**

(a) High-risk AI system operators are to submit a risk remediation plan to AIFRA. They have six months from the Act's start date to comply.

(b) The compliance timeline may be extended by AIFRA for high-risk systems when the entity shows that it is making a good faith effort to remedy known problems.

6. **Capacity Building for Compliance:**

(a) AIFRA shall provide:

(i) Entities moving to the regulatory framework require guidance documents, FAQs, and compliance checklists.

(ii) Workshops and training sessions to aid organizations in comprehending and executing the Act's requirements.

7. **Regulatory Sandbox Integration:** Under the regulatory sandbox, entities having difficulty meeting compliance deadlines may apply to operate for an additional six months, subject to AIFRA's approval.

8. **Reporting Requirements During Transition:**

(a) Quarterly progress reports shall be submitted to AIFRA by entities. The reports shall detail:

(i) Actions undertaken to achieve compliance.

(ii) Problems faced and suggested remedies.

9. **Penalties for Non-Compliance During Transition:**

   (a) Entities that do not meet transitional deadlines and lack valid reasons shall face:

      (i) First-time lapses receive warnings and rectification notices.

      (ii) Fines up to ₹10 lakh for repeated failures.

      (iii) Willful or prolonged noncompliance resulting in suspension of operations.

10. **Review of Transitional Provisions:**

    (a) Six months after the Act comes into effect, AIFRA will carry out a review of transitional progress to:

      (i) Identify challenges faced by entities.

      (ii) If necessary, make clarifications about issues or extend timelines.

Explanation

- **Smooth Transition:** Ensures existing entities have sufficient time to align with the new regulatory framework without disrupting their operations.
- **Support for Stakeholders:** Provides tools and guidance to help entities navigate compliance requirements.
- **Fair Enforcement:** Balances strict compliance with flexibility for entities genuinely working toward adherence.

CHAPTER XI: CONCLUDING PROVISIONS

SECTION 23: REMOVAL OF DIFFICULTIES

1. **Authority to Address Implementation Challenges:** If any difficulty arises in implementing the provisions of this Act, the Central Government may, by notification in the Official Gazette, take necessary actions to resolve such difficulties.
2. **Scope of Authority:**

   (a) This section gives authority to:

      (i) Clarify any unclear parts of provisions that are open to interpretation or that seem to apply in more than one way.

      (ii) Issue additional rules or guidelines to deal with unexpected problems.

      (iii) Change deadlines for compliance or enforcement when starting to implement things.

3. **Timeline for Exercise of Power:** The powers under this section shall be exercisable only within two years from the date of the Act's commencement.
4. **Consultative Process:** The Central Government shall consult with the **AI in FinTech Regulatory Authority (AIFRA)** and other relevant stakeholders before issuing notifications under this section.
5. **Transparency in Decision-Making:**
   (a) Under this section, all decisions and notifications made shall be:
      (i) Issued in the Official Gazette.
      (ii) Made public using the AIFRA website, with an exhaustive explanation of the rationale for the action.

SECTION 24: REPEAL AND SAVINGS

1. **Repeal of Inconsistent Provisions:**
   (a) Any provisions of existing laws or regulations inconsistent with the provisions of this Act shall stand repealed upon its commencement.
   (b) This encompasses provisions in any law that governs the financial system, AI technologies, or data protection if those provisions conflict with this Act.
2. **Savings Clause:**
   (a) Notwithstanding the repeal of inconsistent provisions:
      (i) Actions undertaken, licenses issued, penalties enforced, or contracts signed under the provisions that have been revoked shall continue to be valid.
      (ii) Entities must continue to observe and uphold all obligations under the laws that have been repealed until the provisions of this Act that correspond to those repealed laws are enforced.
3. **Preservation of Consumer Rights:** Nothing in this Act shall adversely affect the rights of consumers protected under other laws unless explicitly stated in this Act.
4. **Continuity of Proceedings:** Legal proceedings initiated under the repealed provisions before the commencement of this Act shall continue as if the provisions had not been repealed.
5. **Notification of Repeal:** The Central Government shall notify the specific provisions being repealed within six months of the Act's commencement.

Explanation

- **Section 23: Removal of Difficulties** ensures adaptability and flexibility during the initial phase of implementation, addressing unforeseen challenges efficiently.
- **Section 24: Repeal and Savings** provides clarity on the transition from existing laws to the new framework, preserving ongoing actions and protecting consumer rights.

RECOMMENDATION 2: BLOCKCHAIN-SMART CONTRACT COMPLIANCE FRAMEWORK

Objective: To establish a comprehensive policy framework that addresses the unique challenges of blockchain and smart contract applications in financial technology, ensuring legal recognition, transparency, and harmonization with existing laws.

KEY COMPONENTS OF THIS FRAMEWORK

1. **Legal Recognition of Smart Contracts**
   (a) Amend the Indian Contract Act, 1872, to statutorily acknowledge smart contracts as legally enforceable contracts.
   (b) Define enforceability criteria, which include:
      (i) Execution of terms encoded on blockchain is automatic.
      (ii) Proof of Evidence for mutual consent demonstrated through digital signatures.
2. **Transparency Standards for Blockchain Systems**
   (a) Ensure public disclosures are mandatory for financial blockchain projects, which should cover:
      (i) Consensus mechanisms (e.g., Proof of Stake, Proof of Work).
      (ii) Decision-making protocols and governance structures.
   (b) Mandate that all blockchain systems keep audit logs that cannot be changed and can be seen by regulators when necessary.
3. **Smart Contract Dispute Resolution Mechanism**
   (a) Create a hybrid framework for resolving disputes that combines:
      (i) For minor disputes, arbitration using blockchain technology allows for inexpensive and speedy resolution.
      (ii) Conventional legal remedies for intricate disputes that necessitate judicial involvement.

(b) Include provisions for disputes that arise in multiple jurisdictions, so they conform to the global standards of arbitration.

4. **Auditing and Certification of Smart Contracts**

   (a) Establish a Smart Contract Certification Program under the AI in FinTech Regulatory Authority (AIFRA):

      (i) Ensure that contracts comply with data protection, consumer protection, and anti-fraud standards.

      (ii) Require regular audits by external firms to uncover any weaknesses or programming mistakes.

5. **Data Protection and Privacy in Blockchain**

   (a) Align blockchain data usage with the Digital Personal Data Protection (DPDP) Act, 2023, including:

      (i) Personal and sensitive data could be encrypted and stored on-chain.

      (ii) Explicit consumer consent for data storage and transaction recording.

      (iii) Provisions for data sharing with select parties without compromising the integrity of the blockchain.

6. **Interoperability Standards**

   (a) Develop interoperability standards to enable blockchain systems to integrate seamlessly with traditional financial systems and other blockchain networks.

   (b) Align interoperability measures with international best practices to facilitate cross-border blockchain operations.

7. **Mechanisms for Error Handling and Amendments**

   (a) Define circumstances under which a smart contract can be amended or rolled back:

      (i) Coding errors or bugs causing significant financial harm.

      (ii) Evidence of fraud or coercion during contract execution.

   (b) Introduce a Rollback Protocol requiring regulatory approval for amendments to blockchain records.

8. **Consumer Safeguards and Education**

   (a) Mandate disclosures for smart contract users, including:

      (i) Risks associated with automation and immutability.

      (ii) Potential liabilities and remedies in case of system failures or fraud.

   (b) Launch consumer awareness programs to educate the public about blockchain and smart contract technologies.

9. **Collaboration with International Frameworks**
   (a) Establish cross-border compliance protocols with frameworks like the EU Blockchain Strategy and US Smart Contract Governance models.
   (b) Promote international agreements for mutual recognition of blockchain certifications and dispute resolution mechanisms.
10. **Penalties for Non-Compliance**
    (a) Impose penalties for entities deploying non-compliant blockchain systems or smart contracts, including:
        (i) Fines up to ₹5 crore for significant violations.
        (ii) Suspension of licenses for repeated offenses.
        (iii) Criminal liability for deliberate misuse of blockchain technologies.

IMPLEMENTATION ROADMAP

1. **Phase 1: Legislative Amendments**
   (a) Amend the Indian Contract Act, 1872, and other relevant laws to include blockchain-specific provisions.
   (b) Establish the Smart Contract Certification Program under AIFRA.
2. **Phase 2: Infrastructure Development**
   (a) Set up technical infrastructure for auditing and certifying blockchain systems.
   (b) Develop interoperability and rollback protocols.
3. **Phase 3: Regulatory and Consumer Integration**
   (a) Roll out consumer education initiatives.
   (b) Implement cross-border agreements for harmonized blockchain governance.
4. **Phase 4: Review and Optimization**
   (a) Conduct an annual review of the framework to address emerging challenges and incorporate technological advancements.

Expected Outcomes

1. Legal clarity and recognition for blockchain and smart contract applications.
2. Improved trust and transparency in blockchain-powered financial systems.
3. Enhanced consumer protection and dispute resolution mechanisms.
4. Alignment with global blockchain governance standards, fostering international collaboration.

RECOMMENDATION 3: IT ACT, 2000 (AS AMENDED IN THE YEAR 2008): INCLUSION OF AI-SPECIFIC CYBERCRIME AND FRAUD PROVISIONS

I. PROPOSED DEFINITIONS FOR INCLUSION IN THE IT ACT, 2000

1. **AI System**

   (a) **Definition:** "AI System" refers to any software, algorithm, or model, including machine learning, neural networks, or natural language processing, designed to perform tasks autonomously or with minimal human intervention, including decision-making, prediction, classification, or data processing.

   (b) **Illustration:**

   (i) A credit-scoring algorithm analyzing user financial data.

   (ii) A chatbot resolving customer service queries.

2. **AI-Generated Content**

   (a) **Definition:** "AI-Generated Content" refers to any text, image, audio, video, or other form of media created or significantly altered by an AI system, which may include synthetic content, deepfakes, or augmented content.

   (b) **Illustration:**

   (i) A video manipulated using deepfake technology to mimic a public figure's speech.

   (ii) Text generated by AI for advertising or social media posts.

3. **Autonomous Systems**

   (a) **Definition:** "Autonomous Systems" refer to self-executing AI systems capable of making decisions and performing tasks without direct human oversight, including systems deployed in financial, operational, or decision-making roles.

   (b) **Illustration:**

   (i) An algorithmic trading system executing stock trades based on market trends.

   (ii) A drone delivering packages based on pre-programmed instructions.

4. **Malicious AI Activities**

   (a) **Definition:** "Malicious AI Activities" refer to the use of AI systems to intentionally cause harm, deceive, or manipulate individuals or entities, including but not limited to:

   (i) Creating phishing scams using AI-generated content.

   (ii) Developing AI systems for cyberattacks, such as automated hacking tools or AI-powered malware.

(b) **Illustration:**

(i) An AI system generating targeted phishing emails to steal user credentials.

(ii) AI-powered bots spreading misinformation or propaganda.

5. **AI-Driven Cybercrime**

(a) **Definition:** "AI-Driven Cybercrime" refers to any offense committed under this Act using AI systems to automate, enhance, or disguise malicious activities, including hacking, identity theft, data breaches, or fraud.

(b) **Illustration:**

(i) Using an AI bot to breach a financial institution's security system.

(ii) Employing AI to mimic legitimate voices in a social engineering scam.

6. **Explainable AI (XAI)**

(a) Definition: "Explainable AI" refers to AI systems designed to provide transparent, understandable, and interpretable outputs or decisions, enabling users and regulators to comprehend the reasoning and data used by the AI system.

(b) Illustration: An AI credit scoring system explaining the criteria used to deny or approve a loan application.

7. **Adversarial Attacks on AI**

(a) Definition: "Adversarial Attacks on AI" refer to actions designed to deceive, manipulate, or exploit vulnerabilities in AI systems, causing them to produce incorrect or unintended results.

(b) Illustration: Injecting misleading data into an AI fraud detection system to bypass security measures.

Rationale for Inclusion

- **Clarity in Scope:** Introducing precise definitions ensures that the IT Act explicitly addresses emerging AI-related issues.
- **Legal Enforcement:** Provides a clear framework for identifying and prosecuting AI-driven cybercrimes.
- **Global Alignment:** Aligns with international frameworks that have started defining and addressing AI systems and cybercrimes.

II. PROPOSED PROVISION: LIABILITY FOR AI-GENERATED CYBERCRIMES

To be included as a new section under the **IT Act, 2000**, addressing liability for cybercrimes involving AI systems.

SECTION XX: LIABILITY FOR AI-GENERATED CYBERCRIMES

1. **Liability of Developers and Operators**

   (a) Developers and operators of AI systems shall be held liable if:

   (i) The AI system is deliberately designed to commit or facilitate cybercrimes, such as phishing, identity theft, or data breaches.

   (ii) The developer or operator fails to incorporate necessary safeguards, resulting in foreseeable misuse of the system.

   (iii) The system is deployed without proper testing, auditing, or certification, causing harm to users or third parties.

   (b) Illustration:

   (i) A developer creates an AI-powered bot that mimics human voices for fraudulent financial transactions.

   (ii) An operator knowingly deploys an AI tool designed to scrape sensitive personal data from websites.

2. **Liability of End Users**

   (a) Users of AI systems shall be held accountable if:

   (i) They intentionally exploit AI systems to commit fraud, deception, or cyberattacks.

   (ii) They modify or manipulate AI systems for malicious purposes, bypassing safeguards.

   (b) Illustration:

   (i) A user deploys an AI system to create deepfakes used for blackmail.

   (ii) A financial analyst uses an AI-powered trading bot to manipulate stock prices illegally.

3. **Shared Liability in Collaborative Systems**

   (a) When multiple parties are involved in the deployment of an AI system, liability shall be apportioned based on:

   (i) The degree of control exercised by each party over the system.

   (ii) The specific role played by each party in the crime (e.g., design, deployment, or use).

   (iii) Negligence or failure to comply with regulatory standards.

4. **Burden of Proof and Safe Harbor**

   (a) Developers, operators, or users may avoid liability by demonstrating:

   (i) They exercised due diligence in the design, testing, and deployment of the AI system.

   (ii) Adequate safeguards were implemented to prevent misuse.

(iii) The misuse of the system was unforeseen and beyond their reasonable control.

(b) Illustration: A company proves that its AI chatbot used in phishing scams was hacked by an unauthorized third party.

5. **Enhanced Liability for Rogue AI Systems**

   (a) Developers or operators of rogue AI systems—intentionally designed for illegal activities—shall face:

   (i) Fines up to ₹5 crore.

   (ii) Criminal liability, including imprisonment of up to five years.

   (iii) Permanent disqualification from developing or operating AI systems in regulated sectors.

6. **Regulatory Obligations for Developers and Operators**

   (a) Developers and operators must:

   (i) Register AI systems deployed in financial or sensitive operations with the **AI in FinTech Regulatory Authority (AIFRA)**.

   (ii) Maintain detailed audit logs and records of system performance and decision-making processes.

   (iii) Notify regulators of any breaches or suspected misuse of their AI systems within 48 hours.

7. **Penalties for Non-Compliance**

   (a) Failure to comply with safeguards, reporting, or certification requirements shall result in:

   (i) Fines up to ₹2 crore for first offenses.

   (ii) Higher penalties for repeated violations or cases involving consumer harm.

   (iii) Suspension of licenses for deploying AI systems in regulated industries.

Rationale for Inclusion

- **Accountability:** Ensures developers, operators, and users are held responsible for malicious or negligent use of AI systems.
- **Deterrence:** Penalizing rogue systems discourages the creation and use of harmful AI applications.
- **Consumer Protection:** Establishes a clear framework for restitution and legal recourse for victims of AI-related cybercrimes.

III. PROPOSED PROVISION: MANDATORY REPORTING OF AI-DRIVEN CYBER INCIDENTS

To be included as a new section under the **IT Act, 2000**, addressing the obligation to report AI-driven cybercrimes and incidents.

SECTION XX: MANDATORY REPORTING OF AI-DRIVEN CYBER INCIDENTS

1. **Obligation to Report**: Any individual, organization, or entity deploying AI systems must report cyber incidents involving their systems to the **Indian Computer Emergency Response Team (CERT-In)** within **48 hours** of detection.
   (a) Cyber incidents subject to reporting include:
      (i) Data breaches caused by or involving AI systems.
      (ii) Unauthorized access or exploitation of AI systems.
      (iii) AI-driven phishing, fraud, or misinformation campaigns.
      (iv) Malfunction or unintended outcomes in AI systems leading to financial harm or security risks.
2. **Scope of Reporting**
   (a) Entities must include the following details in their report:
      (i) Nature and scope of the incident.
      (ii) Affected systems, users, and data.
      (iii) Steps taken to mitigate the incident.
      (iv) Potential risks or impacts arising from the incident.
   (b) Illustration:
      (i) A bank using an AI fraud detection system must report a breach where hackers bypass the AI system to siphon customer funds.
      (ii) A platform deploying an AI chatbot must report if the bot is exploited to execute phishing attacks.
3. **Exemptions and Anonymity**
   (a) Reporting requirements may be relaxed for:
      (i) Non-commercial AI systems used in research or education, provided there is no material harm.
   (b) CERT-In may allow anonymized reporting for incidents that do not involve personal data breaches.
4. **Responsibilities of CERT-In**
   (a) CERT-In shall:
      (i) Acknowledge and respond to incident reports within 24 hours.

(ii) Provide technical assistance to affected entities to mitigate risks.

(iii) Maintain a database of reported incidents to track trends and recommend policy updates.

(iv) Publish periodic reports on AI-driven cyber incidents, excluding sensitive or identifying information.

5. **Penalties for Failure to Report**

(a) Entities failing to report cyber incidents involving AI systems shall face:

(i) Fines up to ₹50 lakh for first offenses.

(ii) Higher fines and potential criminal liability for repeated or deliberate failures to report.

(b) Illustration: A FinTech company failing to report an AI system malfunction that caused financial losses to consumers would be liable.

6. **Whistle-blower Protections**

(a) Employees or third parties reporting unreported incidents shall be protected under the **Whistle-blower Protection Framework**, ensuring:

(i) Anonymity and protection from retaliation.

(ii) Rewards or recognition for reporting critical vulnerabilities or breaches.

7. **Collaboration with International Bodies**

(a) CERT-In shall share information on significant AI-driven cyber incidents with:

(i) International counterparts under global cybersecurity frameworks.

(ii) Multilateral forums addressing AI governance and cybercrime.

8. **Proactive Incident Response Guidelines**

(a) CERT-In, in consultation with the AI in FinTech Regulatory Authority (AIFRA), shall:

(i) Develop and disseminate guidelines for preventing and managing AI-driven cyber incidents.

(ii) Conduct workshops and training sessions for entities deploying AI systems.

Rationale for Inclusion

- **Early Mitigation:** Ensures timely reporting and action to minimize harm from AI-driven cyber incidents.
- **Accountability:** Encourages entities to proactively monitor and secure their AI systems.
- **Global Alignment:** Harmonizes India's approach with international best practices for cybersecurity and incident reporting.

IV. PROPOSED AMENDMENTS: AI-SPECIFIC PENALTIES

AMENDMENT TO SECTION 66: PENALTIES FOR CYBERCRIMES INVOLVING AI

1. **Higher Penalties for AI-Driven Cybercrimes**

(a) Existing Provision: Section 66 prescribes penalties for unauthorized access, data theft, and other computer-related offenses.

(b) Proposed Amendment: Amend Section 66 to impose enhanced penalties for cybercrimes committed using AI systems, such as:

(i) Phishing campaigns powered by AI-generated content.

(ii) Deepfake technology used for fraud or defamation.

(iii) Automated attacks leveraging AI algorithms to exploit vulnerabilities.

(c) Penalties:

(i) First Offense: Fine up to ₹2 crore and/or imprisonment of up to 5 years.

(ii) Repeat Offenses: Fine up to ₹5 crore and/or imprisonment of up to 7 years.

(d) Illustration: A person deploying an AI bot to execute large-scale phishing scams targeting financial institutions would face these enhanced penalties.

V. NEW CLAUSE: OFFENSES INVOLVING AUTONOMOUS AI SYSTEMS

1. Introduction of New clause under Section 66B of IT Act, 2000 (As Amended in 2008): Crimes Involving Autonomous AI Systems

(a) Definition: Crimes involving autonomous AI systems refer to offenses committed directly or indirectly through self-operating AI systems without direct human intervention at the time of the offense.

(b) Liability for Operators: Operators of autonomous AI systems shall be held accountable if the system commits a crime, including:

(i) Fraudulent financial transactions.

(ii) Data breaches or identity theft.

(iii) Harm caused by AI-driven misinformation or manipulation.

(c) **Operators must demonstrate that:**

(i) Necessary safeguards were implemented to prevent such crimes.

(ii) The incident was beyond their reasonable control to avoid liability.

(d) Liability for Developers: Developers of rogue autonomous AI systems—designed intentionally for illegal activities—shall be directly liable for the crimes committed by the system.

(e) Penalties:

(i) For Operators: Fine up to ₹3 crore and/or imprisonment of up to 6 years for negligence leading to AI system misuse.

(ii) For Developers: Fine up to ₹7 crore and/or imprisonment of up to 10 years for deliberate creation of rogue AI systems.

(f) Illustration:

(i) A developer creating an autonomous AI system designed to infiltrate banking systems and steal customer data would face these penalties.

(ii) An operator deploying an AI-powered trading bot that causes market manipulation without safeguards would also be held accountable.

VI. NEW CLAUSE: STRICT LIABILITY FOR ROGUE AI SYSTEMS

1. Section 66C: Strict Liability for Rogue AI Systems

(a) Definition: Rogue AI systems are those intentionally designed or programmed to violate laws or commit crimes autonomously.

(b) Provisions: Developers, deployers, and collaborators involved in creating rogue AI systems shall face:

(i) Criminal liability, including imprisonment of up to 10 years.

(ii) Permanent disqualification from developing or deploying AI systems in India.

(a) Affected parties shall have the right to seek compensation from liable entities.

VII. PROVISIONS FOR RESTITUTION AND REHABILITATION

1. Restitution for Victims of AI-Driven Crimes

(a) Entities or individuals convicted under Section 66 for AI-driven crimes shall be required to:

(i) Compensate affected victims for financial losses and damages.

(ii) Pay additional penalties to a government-managed Cybersecurity Rehabilitation Fund to aid victims of cybercrimes.

Rationale for Inclusion

- **Enhanced Accountability:** Encourages developers, operators, and users to implement stronger safeguards for AI systems.

- **Deterrence:** Higher penalties deter malicious actors from using AI systems for illegal activities.
- **Consumer Protection:** Introduces restitution mechanisms to compensate victims and promote trust in AI technologies.
- **Alignment with Global Standards:** Recognizes the unique risks posed by autonomous AI systems, aligning India's legal framework with international best practices.

RECOMMENDATION 4: PROPOSED AMENDMENTS TO THE RBI ACT, 1934: INCLUSION OF AI-DRIVEN FINANCIAL SYSTEMS

I. NEW SECTION: AI-DRIVEN FINANCIAL SYSTEMS UNDER RBI OVERSIGHT

SECTION XX: REGULATION OF AI-DRIVEN FINANCIAL SYSTEMS

1. **Definition and Scope**

   (a) AI-Driven Financial Systems: Financial services or operations powered by artificial intelligence, including:

   (i) Algorithmic trading platforms.

   (ii) Robo-advisors offering automated investment advice.

   (iii) AI systems for credit scoring, fraud detection, and risk assessment.

   (iv) Blockchain-based financial systems, including smart contract applications.

   (b) Scope: Includes all banks, non-banking financial companies (NBFCs), and payment system providers using AI systems in their operations.

2. **Mandatory Registration and Certification**

   (a) Entities deploying AI-driven financial systems must:

   (i) Register such systems with the **Reserve Bank of India (RBI)**.

   (ii) Obtain a compliance certificate from the RBI or a designated certifying body before deployment.

   (b) Certification requirements include:

   (i) Ensuring the system is Explainable AI (XAI) compliant.

   (ii) Bias detection and mitigation protocols.

   (iii) Robust fraud detection and error-handling mechanisms.

3. **AI Governance Framework**

   (a) RBI shall establish an **AI Governance Division** responsible for:

(i) Monitoring the deployment and performance of AI systems in financial operations.

(ii) Conducting periodic audits to ensure compliance with regulatory standards.

(iii) Investigating cases of systemic risk, fraud, or breaches caused by AI systems.

4. **Algorithmic Trading Regulation**

(a) Entities using AI in algorithmic trading must:

(i)Pre-register trading algorithms with the RBI.

(ii) Provide detailed documentation on algorithm logic, risk controls, and back testing results.

(ii) Ensure real-time monitoring of trading activities to prevent market manipulation or excessive volatility.

5. **Credit Scoring and Lending Standards**

(a) AI systems used for credit scoring must:

(i) Provide transparent and explainable decision-making criteria.

(ii) Allow consumers the right to contest AI-driven credit decisions.

(iii) Ensure no discriminatory practices based on gender, caste, religion, or other protected characteristics.

(b) Banks and NBFCs must conduct periodic audits of AI-based credit scoring systems to detect and mitigate algorithmic biases.

6. **Fraud Detection and Risk Mitigation**

(a) Entities using AI for fraud detection must:

(i) Implement AI models capable of identifying and reporting fraudulent activities in real time.

(ii) Share data on detected fraud patterns with the RBI to build a centralized fraud detection database.

(iii) Notify the RBI of any breaches or fraudulent activities involving AI systems within 24 hours.

7. **Consumer Protection Measures**

(a) AI systems in financial operations must comply with:

(i) Consumer grievance redressal mechanisms as prescribed by the RBI.

(ii) Data protection requirements under the Digital Personal Data Protection (DPDP) Act, 2023.

(b) Consumers must be informed about the use of AI in financial services and their rights, including contesting decisions.

8. **Risk Assessment Framework**

(a) Entities deploying AI systems must submit an annual AI Risk Assessment Report to the RBI, detailing:

(i) System performance, vulnerabilities, and compliance.

(ii) Measures taken to mitigate risks identified during audits or operations.

9. **Penalties for Non-Compliance**

(a) Non-compliance with the AI regulatory framework shall result in:

(i) Fines up to ₹10 crore for systemic risks or consumer harm.

(ii) Suspension of operations involving non-compliant AI systems.

(iii) Criminal liability for willful misconduct or fraud involving AI systems.

10. **Innovation and Collaboration**

(a) The RBI shall:

(i) Expand the scope of its regulatory sandbox to include AI-driven financial systems.

(ii) Collaborate with global regulatory bodies to harmonize standards for AI governance in FinTech.

(iii) Provide incentives for banks and NBFCs adopting ethical and innovative AI solutions.

Rationale for Inclusion

- **Enhanced Oversight:** Brings AI-driven financial systems under RBI's direct supervision, ensuring they align with regulatory standards.
- **Consumer Trust:** Ensures fairness, transparency, and accountability in AI-driven financial decisions.
- **Mitigation of Systemic Risks:** Reduces risks of market manipulation, algorithmic biases, and AI-related fraud.
- **Innovation Support:** Encourages responsible innovation while maintaining regulatory safeguards.

RECOMMENDATION 5: PROPOSED AMENDMENTS TO THE CONSUMER PROTECTION ACT, 2019

I. DISCLOSURE OF ALGORITHMIC BIASES

1. Amend Section 2(1)(f) Definition of Defects

(a) Include **algorithmic biases** within the definition of "defects" under goods and services.

(b) Proposed Definition: "Algorithmic Bias" refers to systemic errors or biases in AI systems that lead to unfair, discriminatory, or inaccurate outcomes, impacting consumers' rights or access to goods and services.

2. Proposed Obligations for AI Platforms:

1. Regular Bias Audits:

(a) AI platforms must conduct periodic audits to identify biases in their algorithms.

(b) Audits should assess whether the system disproportionately affects consumers based on protected characteristics (e.g., gender, caste, religion).

2. Disclosure Requirements:

(a) Audit findings must be shared with regulators and summarized in plain language for consumers.

(b) Platforms must publish a transparency report annually, highlighting:

(i) Bias mitigation efforts.

(ii) Outcomes of audits.

3. Illustration: A credit scoring platform using AI must disclose if its algorithm negatively affects credit approvals for specific consumer groups, even if unintentionally.

II. TRANSPARENCY IN AI DECISION-MAKING

1. Add new section: Duties of the Manufacturer or Service Provider

(a) Add a clause mandating **Explainable AI (XAI) standards** for AI platforms making financial or significant decisions.

2. Proposed Clause:

(b) Service providers deploying AI systems must:

(i) Provide clear and understandable explanations for automated decisions affecting consumers.

(ii) Ensure decisions are traceable and auditable to avoid arbitrary outcomes.

3. Illustration: If a loan application is rejected by an AI system, the platform must explain the reasons (e.g., low income, high debt) and suggest corrective actions the consumer can take.

III. RIGHT TO CONTEST AI DECISIONS

1. Add new section: Right to Information

(a) Expand the scope of consumers' rights to include:

(i) Right to Appeal AI Decisions: Consumers must have the ability to contest decisions made by AI systems and request a human review.

(ii) Access to AI Decision-Making Data: Consumers should be able to access the data and criteria used in AI decisions, provided it does not disclose proprietary algorithms.

2. **Proposed Implementation:**

(a) Platforms must establish an internal process to review and respond to consumer appeals within 15 days.

(b) In case of disputes, consumers can escalate the issue to regulatory bodies or grievance redressal forums.

3. Illustration: A consumer denied credit by an AI-driven system can request a review and access the decision criteria to understand and appeal the outcome.

IV.GRIEVANCE REDRESSAL MECHANISM FOR AI PLATFORMS

1. **Amend Section 9: Establishment of Grievance Redressal Mechanisms**

(a) Mandate AI-driven platforms to establish a dedicated AI Grievance Redressal Cell responsible for:

(i) Receiving and resolving complaints related to algorithmic decisions.

(ii) Ensuring disputes are resolved within 30 days.

2. **Proposed Clause:**

(a) Platforms must assign trained personnel to manage AI-related grievances and ensure transparency in the resolution process.

(b) Platforms failing to comply with grievance timelines will face penalties under Section 72 of the Act.

3. Illustration: A consumer lodging a complaint about unfair pricing on an e-commerce platform powered by AI must receive a resolution or a clear explanation within 30 days.

V. CONSUMER AWARENESS INITIATIVES

1. **Add new Section: Consumer Rights Advocacy**

(a) Add a mandate requiring AI platforms to:

(i) Conduct awareness campaigns to educate consumers about AI systems, their risks, and potential impacts.

(ii) Inform consumers of their rights under the Consumer Protection Act and other relevant laws.

2. **Proposed Implementation:**
   (a) Awareness materials must include:
      (i) Simple guides on how AI systems work.
      (ii) Steps to contest decisions and lodge complaints.
      (iii) Warnings about the limitations and risks of AI-based services.
3. **Illustration:** An AI-driven robo-advisory platform must educate users on how investment decisions are made, the risks involved, and how to raise disputes.

Expected Benefits

1. **Enhanced Consumer Trust:** Transparency and accountability in AI decision-making will build consumer confidence in AI platforms.
2. **Fairness in AI Operations:** Regular audits and the right to appeal ensure that algorithmic biases are identified and mitigated.
3. **Streamlined Grievance Redressal:** Dedicated mechanisms will make it easier for consumers to resolve disputes.
4. **Consumer Empowerment:** Awareness campaigns will help consumers make informed decisions and exercise their rights effectively.

RECOMMENDATION 6: INTERNATIONAL HARMONIZATION

I. DATA SHARING AGREEMENTS

1. **Objective:** To facilitate secure and regulated cross-border data sharing for AI-driven financial systems while ensuring compliance with global data protection standards.
2. **Proposed Recommendations:**
   (a) Negotiate **bilateral or multilateral agreements** with key jurisdictions like the EU and US to:
      (i) Enable seamless data exchange for AI-powered financial services.
      (ii) Harmonize data privacy standards to prevent conflicts between regulatory frameworks (e.g., GDPR, CCPA).
   (b) Include provisions for:
      (i) Data Localization Exceptions: Allow specific cross-border data transfers with adequate safeguards.
      (ii) Mutual Data Audits: Establish shared auditing protocols to verify compliance with data protection laws.

3. **Illustration:** An Indian FinTech company using an AI system to process international remittances can securely share and process customer data in Europe under GDPR-aligned rules.

II. GLOBAL STANDARDS FOR ALGORITHMIC TRANSPARENCY

1. **Objective:** To align Indian regulations with global standards, ensuring interoperability and trust in AI systems across jurisdictions.
2. **Proposed Recommendations:**
   (a) Collaborate with international bodies (e.g., ISO, OECD) to:
      (i) Adopt global standards for **Explainable AI (XAI)** in FinTech.
      (ii) Ensure uniform benchmarks for algorithmic transparency, fairness, and accountability.
   (b) Advocate for a **Global AI Regulatory Forum** to discuss and harmonize standards across countries.

3. Illustration: A global bank using an AI-powered credit scoring model can deploy the system in multiple jurisdictions without modifications, provided it meets global transparency standards.

III. MUTUAL RECOGNITION OF AI CERTIFICATIONS

1. **Objective:** To facilitate cross-border deployment of AI systems by recognizing certifications issued by foreign regulators.
2. **Proposed Recommendations:**
   (a) Establish a framework for **mutual recognition of AI certifications** with major jurisdictions.
   (b) Align certification criteria with international best practices, ensuring:
      (i) Compliance with data protection, bias detection, and risk mitigation standards.
      (ii) Interoperability of AI systems across borders.
3. **Illustration:** An AI system certified in the EU under its AI Act could be fast-tracked for deployment in India, and vice versa, if it meets equivalent regulatory standards.

IV. INTERNATIONAL AI RESEARCH COLLABORATION

1. **Objective:** To foster innovation and ethical governance through shared research and development.

2. **Proposed Recommendations:**

   (a) Partner with leading AI research institutions and regulatory bodies in the EU, US, and other regions to:

      (i) Share insights on algorithmic bias detection, fraud prevention, and risk management.

      (ii) Co-develop tools and frameworks for ethical AI deployment in FinTech.

   (b) Establish an **AI Research Fund** to support cross-border projects on:

      (i) Blockchain integration with AI.

      (ii) Risk assessment models for AI-powered financial systems.

3. **Illustration:** India collaborates with EU regulators to develop a tool for detecting biases in AI-based lending systems, which can be adopted globally.

V. CROSS-BORDER DISPUTE RESOLUTION

1. **Objective:** To provide a structured framework for resolving disputes arising from AI-driven financial operations involving multiple jurisdictions.
2. **Proposed Recommendations:**

   (a) Develop an international arbitration mechanism aligned with **UNCITRAL arbitration rules** to handle:

      (i) Disputes over AI system failures in cross-border transactions.

      (ii) Consumer complaints involving foreign AI platforms.

   (b) Advocate for an **International AI Dispute Resolution Body** to standardize arbitration rules for AI-related cases.

3. **Illustration:** A consumer in India experiencing losses from an AI-powered trading platform in the US could resolve the dispute through an internationally recognized arbitration framework.

VI. PARTICIPATION IN GLOBAL AI GOVERNANCE FORUMS

1. **Objective:** To position India as a leader in shaping global AI governance and FinTech innovation.
2. **Proposed Recommendations:**

   (a) Actively participate in international AI governance forums like the Global Partnership on AI (GPAI) and World Economic Forum's AI initiatives**.**

   (b) Advocate for ethical AI practices in FinTech, emphasizing:

      (i) Consumer protection.

      (ii) Risk mitigation.

      (iii) Cross-border interoperability.

3. **Illustration:** India co-chairs a GPAI working group to develop a global ethical AI framework for financial services.

Expected Benefits

1. **Seamless Global Operations:** Harmonization enables Indian FinTech companies to expand internationally without facing regulatory roadblocks.
2. **Enhanced Trust:** Adherence to global standards increases confidence in Indian AI systems among international partners and consumers.
3. **Innovation Boost:** Collaborative research and mutual recognition of certifications promote faster deployment of innovative AI solutions.
4. **Consumer Protection:** International dispute resolution mechanisms safeguard consumers across borders.
5. **Strategic Leadership:** Active participation in global forums positions India as a key player in shaping AI governance.

RECOMMENDATION 7: AI TRANSPARENCY AND ACCOUNTABILITY

I. IMPLEMENT EXPLAINABLE AI (XAI) STANDARDS

1. Objective: To ensure AI systems used in financial decision-making are transparent, understandable, and fair.

2. **Proposed Measures:**

(a) Mandating XAI Standards:

(i) AI platforms in FinTech must adopt Explainable AI (XAI) standards to ensure users and regulators can comprehend AI-driven decisions.

(ii) XAI frameworks should provide clear explanations for decisions like loan approvals, credit scoring, or investment recommendations.

(b) Auditable Decision Processes:

(i) AI systems must maintain logs of inputs, algorithms, and outputs, allowing independent audits of decisions.

(ii) Consumers must have access to simplified explanations of decisions affecting them.

3. **Benefits:**

(a) Reduces instances of discriminatory practices by ensuring fairness.

(b) Enhances trust in AI systems by making decision-making processes accessible to users.

II. SET UP A REGULATORY BODY TO AUDIT AI ALGORITHMS

1. Objective: To establish a mechanism for independent oversight of AI systems in FinTech to ensure accuracy, fairness, and transparency.

2. Proposed Regulatory Framework:

(a) Formation of the Regulatory Body:

(i) Create an AI Algorithm Auditing Authority (AIAAA) under the AI in FinTech Regulatory Authority (AIFRA).

(b) Key Responsibilities of AIAAA:

(i) Conduct bias audits and performance reviews of AI systems in FinTech.

(ii) Certify AI systems for compliance with transparency, fairness, and ethical standards.

(iii) Investigate consumer complaints about unfair or erroneous decisions by AI systems.

(c) Audit Frequency and Scope:

(i) Conduct annual audits of high-risk AI systems, such as those used in credit scoring and algorithmic trading.

(ii) Perform random inspections for low-risk AI systems.

3. Benefits:

(a) Prevents systemic risks arising from unregulated AI algorithms.

(b) Enhances accountability by holding entities deploying AI systems responsible for compliance.

RECOMMENDATION 8: STRENGTHENING DATA PRIVACY AND PROTECTION

I. ALIGNMENT WITH THE DPDP ACT, 2023

1. Objective: To ensure AI-driven systems comply with India's data privacy standards while addressing unique challenges posed by AI.

2. Proposed Measures:

(a) AI-Specific Data Privacy Provisions:

(i) Require AI systems to anonymize and encrypt consumer data during processing.

(ii) Mandate AI platforms to disclose how consumer data is used, stored, and shared.

(b) Alignment with DPDP Act—Ensure AI platforms comply with key DPDP Act requirements:

(i) Consent Mechanisms: Consumers must provide explicit consent for data usage in AI-driven financial systems.

(ii) Data Localization: Critical data used by AI systems must be stored within India, with restrictions on cross-border transfers.

(iii) Breach Notifications: AI platforms must notify consumers and regulators within 48 hours of data breaches.

II. MECHANISMS FOR CONSUMER CONSENT, LOCALIZATION, AND CROSS-BORDER DATA FLOW

1. Consumer Consent:

(a) Introduce dynamic consent mechanisms, allowing consumers to modify or revoke consent at any time.

(b) Provide clear options for opting out of AI-driven services without penalty.

2. Data Localization:

(a) Establish clear categories for sensitive and non-sensitive data to streamline compliance.

(b) Allow exemptions for global FinTech firms under strict conditions, such as adhering to DPDP-equivalent protections.

3. Cross-Border Data Flow: Develop a **Data Transfer Agreement Framework (DTAF)** aligned with GDPR and other international standards.

4. Benefits:

(a) Protects consumer data and privacy in an era of AI-driven automation.

(b) Encourages responsible data handling practices, building consumer trust.

RECOMMENDATION 9: ENCOURAGING INNOVATION

I. EXPAND THE SCOPE OF RBI'S REGULATORY SANDBOX

1. **Objective:** To foster experimentation and innovation while ensuring consumer safety and regulatory compliance.
2. **Proposed Expansion:**

(a) Inclusion of AI-Driven Blockchain Projects:

(i) Permit projects that integrate AI and blockchain in areas like:

(a) Fraud detection using AI algorithms on blockchain.

(b) Blockchain-based credit scoring systems using AI predictions.

(b) Smart Contract Testing:

(i) Allow testing of smart contracts that automate financial transactions, including:

(a) AI-powered dynamic interest rates.

(b) Automated insurance claims using smart contracts and AI assessment.

(c) Flexible Testing Environment:

(i) Enable start-ups and innovators to test systems under controlled environments with relaxed compliance for a fixed period.

(ii)Provide technical and legal support to participants in the sandbox.

II. INNOVATION INCENTIVES

1. Tax Incentives:

(a) Offer tax benefits to start-ups and established firms investing in AI research and blockchain development.

2. Funding for Research and Development (R&D):

(b) Establish an **AI Innovation Fund** to support R&D projects aimed at ethical and transparent AI solutions in FinTech.

Benefits of Encouraging Innovation

- Promotes cutting-edge solutions in FinTech that enhance efficiency and consumer experience.
- Positions India as a global leader in AI and blockchain innovation.
- Reduces barriers for start-ups and SMEs to test and deploy new technologies.

7.2.1 Future Research Directions

The rapidly changing world of AI and FinTech requires ongoing investigation to deal with new problems and prospects. Future research could centre on the influence of generative AI in financial decision-making, the part quantum computing could play in FinTech, and the ethical concerns surrounding systems of decentralized finance (DeFi). In summary, this thesis emphasizes the potential of AI to transform FinTech and addresses the urgent need for comprehensive legal structures to traverse this intricate environment. If stakeholders confront the challenges and seize the opportunities described, they can clear a path toward an inclusive, transparent, and sustainable financial future.

BIBLIOGRAPHY

BOOKS & EDITED BOOK CHAPTERS

1. Abbas, N. N., Ahmad, R., Qazi, S., & Ahmed, W. (2023). Impact of deepfake technology on fintech applications. In S. Saeed, A. Almuhaideb, N. Kumar, N. Zaman, & Y. Zikria (Eds.), *Handbook of research on cybersecurity issues and challenges for business and fintech applications* (pp. 225–242). IGI Global. https://doi.org/10.4018/978-1-6684-5284-4.ch012
2. Aggarwal, N. (2024). AI, fintech, and the evolving regulation of consumer financial privacy. In J. B. Bullock, M. MacCarthy, & K. Yeung (Eds.), *The Oxford handbook of AI governance* (online ed.). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197579329.013.51
3. Barezzani, S. (2024). Artificial Intelligence Act (AI Act) and the GDPR. In S. Jajodia, P. Samarati, & M. Yung (Eds.), *Encyclopedia of cryptography, security and privacy* (pp. 1–6). Springer. https://doi.org/10.1007/978-3-642-27739-9_1820-1
4. Basly, S. (2024). Artificial intelligence and the future of decentralized finance. In S. Basly (Ed.), *Decentralized finance (Financial Innovation and Technology Series)*. Springer. https://doi.org/10.1007/978-3-031-49515-1_10
5. Beck, A. D. (2021). The role of artificial intelligence in robo-advisory. In P. Scholz (Ed.), *Robo-advisory – Investing in the digital age* (pp. 227–243). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-40818-3_11
6. Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press. https://global.oup.com/academic/product/superintelligence-9780199678112?cc=in&lang=en&
7. Chakravaram, V., Ratnakaram, S., Vihari, N., & Tatikonda, N. (2020). The role of technologies on banking and insurance sectors in the digitalization and globalization era—A select study. In *Digital transformation in business and society*. Page (145-156) Springer. https://doi.org/10.1007/978-981-15-7234-0_12
8. Chen, K. (2018). Financial innovation and technology firms: A smart new world with machines. In *International Symposia in Economic Theory and Econometrics* (Vol. 25, pp. 279–292). Emerald Publishing. https://www.emerald.com/insight/content/doi/10.1108/s1571-038620180000025012/full/html
9. Dorfleitner, G., Hornuf, L., Schmitt, M., & Weber, M. (2017). *FinTech in Germany*. Springer. https://doi.org/10.1007/978-3-319-54666-7
10. Guo, H., & Polak, P. (2021). Artificial intelligence and financial technology (FinTech): How AI is being used under the pandemic. In V. Ratten & P. Jones (Eds.), *The fourth industrial revolution: Implementation of artificial intelligence for*

growing business success (pp. 169–186). Springer. https://doi.org/10.1007/978-3-030-65765-9_10

11. Huang, L., & Peissl, W. (2023). Artificial intelligence—A new knowledge and decision-making paradigm? In L. Hennen, J. Hahn, M. Ladikas, R. Lindner, W. Peissl, & R. van Est (Eds.), *Technology assessment in a globalized world* (pp. 205–221). Springer. https://doi.org/10.1007/978-3-031-10617-0_9
12. Kulhari, S. (2018). Data protection, privacy and identity: A complex triad. In *Building-blocks of a data protection revolution: The uneasy case for blockchain technology to secure privacy and identity* (pp. 123–140). Springer. https://www.jstor.org/stable/j.ctv941qz6.7
13. Ma, A. (2023). Blockchain-enabled smart legal contracts. In *Blockchain and smart contracts* (pp. 75–92). IntechOpen. https://doi.org/10.5772/intechopen.109041
14. Pasumarti, S. S. (2024). Legal implications of fintech. In C. M. Gupta & G. Kaur (Eds.), *E-banking, fintech & financial crimes* (pp. 231–245). Springer. https://doi.org/10.1007/978-3-031-67853-0_12
15. Perdana, A., Wang, T., & Arifin, S. (2024). Artificial intelligence in accounting: Ethical challenges and legal perspectives. In A. Perdana & T. Wang (Eds.), *Digital transformation in accounting and auditing* (pp. 215–233). Palgrave Macmillan. https://doi.org/10.1007/978-3-031-46209-2_11
16. Lui, C., & Ryder, N. (Eds.). (2023). *FinTech, artificial intelligence and the law: Regulation and crime prevention*. Routledge. https://www.routledge.com/9781032012469
17. Rupeika-Apoga, R., & Marano, P. (Eds.). (2022). *The risk landscape within FinTech and InsurTech business models.* MDPI Books. https://doi.org/10.3390/books978-3-0365-2773-4
18. Shackelford, S. J. (2021). Governing the Internet of Everything. In *Governing privacy in knowledge commons* (pp. 203–219). Cambridge University Press. https://doi.org/10.1017/9781108749978.009
19. Stahl, B. C. (2021). Addressing ethical issues in AI. In *Artificial intelligence for a better future* (pp. 73–82). SpringerBriefs in Research and Innovation Governance. https://doi.org/10.1007/978-3-030-69978-9_5
20. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.
21. Wischmeyer, T. (2020). Artificial intelligence and transparency: Opening the black box. In T. Wischmeyer & T. Rademacher (Eds.), *Regulating artificial intelligence* (pp. 63–83). Springer. https://doi.org/10.1007/978-3-030-32361-5_4
22. Yordanova, K., & Bertels, N. (2024). Regulating AI: Challenges and the way forward through regulatory sandboxes. In H. S. Antunes et al. (Eds.),

Multidisciplinary perspectives on artificial intelligence and the law (Law, Governance and Technology Series 58, pp. 445–462). Springer. https://doi.org/10.1007/978-3-031-41264-6_23

23. Zachariadis, M., & Ozcan, P. (2022). *Open banking: How platforms and the API economy change competition in financial services*. MIT Press. https://doi.org/10.7551/mitpress/13673.003.0007
24. Zander, J. (2010). *The application of the precautionary principle in practice*. Cambridge University Press.

JOURNAL ARTICLES

1. Abbas, S. G., Vaccari, I., Hussain, F., Zahid, S., Fayyaz, U. U., Shah, G. A., Bakhshi, T., & Cambiaso, E. (2021). Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach. *Sensors,* 21(14), 4816. https://doi.org/10.3390/s21144816
2. Ahern, D. (2021). Regulatory lag, regulatory friction and regulatory transition as fintech disenablers: Calibrating an EU response to the regulatory sandbox phenomenon. *European Business Organization Law Review*, 22, 395–432. https://doi.org/10.1007/s40804-021-00217-z
3. Aldboush, H. H. H., & Ferdous, M. (2023). Building trust in fintech: An analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. *International Journal of Financial Studies*, 11(3), 90. https://doi.org/10.3390/ijfs11030090
4. Alt, R., Beck, R., & Smits, M. (2018). Fintech and the transformation of the financial industry. *Electronic Markets*, 28(3), 235–243. https://doi.org/10.1007/s12525-018-0310-9
5. Anakpo, G., Xhate, Z., & Mishi, S. (2023). The policies, practices, and challenges of digital financial inclusion for sustainable development: The case of the developing economy. *FinTech*, 2(2), 327–343. https://doi.org/10.3390/fintech2020019
6. Anshari, M., Almunawar, M. N., & Masri, M. (2021). Financial technology with AI-enabled and ethical challenges. *Society,* 58, 189–195. https://doi.org/10.1007/s12115-021-00592-w
7. Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of fintech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47(4), 1271–1319. http://dx.doi.org/10.2139/ssrn.2676553

8. Ashta, A., & Herrmann, H. (2021). Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance. *Strategic Change*, 30(3), 211–222. https://doi.org/10.1002/jsc.2404
9. Asif, M. (2023). The impact of fintech and digital financial services on financial inclusion in India. *Journal of Risk and Financial Management*, 16(2), 122. https://doi.org/10.3390/jrfm16020122
10. Assenova, V. A., Best, J., Cagney, M., Ellenoff, D., Karas, K., Moon, J., Neiss, S., Suber, R., & Sorenson, O. (2016). The present and future of crowdfunding. *California Management Review,* 58(2), 125–135. https://doi.org/10.1525/cmr.2016.58.2.125
11. Azzutti, A., Ringe, W.-G., & Stiehl, H. S. (2024). Machine learning, market manipulation, and collusion on capital markets: Why the "black box" matters. *University of Pennsylvania Journal of International Law*, 45(1), 79–134. https://scholarship.law.upenn.edu/jil/vol45/iss1/3
12. Bahoo, S., Cucculelli, M., Goga, X., et al. (2024). Artificial intelligence in finance: A comprehensive review through bibliometric and content analysis. *SN Business & Economics*, 4, Article 23. https://doi.org/10.1007/s43546-023-00618-x
13. Balamurugan, M. (2024). AI vs. AI: The digital duel reshaping fraud detection. *European Journal of Computer Science and Information Technology*, 12(7), 12–20. https://doi.org/10.37745/ejcsit.2013/vol12n71220
14. Balayn, A., Lofi, C., & Houben, G. J. (2021). Managing bias and unfairness in data for decision support: A survey of machine-learning and data-engineering approaches to identify and mitigate bias and unfairness within data-management and analytics systems. *The VLDB Journal*, 30, 739–768. https://doi.org/10.1007/s00778-021-00671-8
15. Ballell, T. R. de L. H. (2019). Legal challenges of artificial intelligence: Modelling the disruptive features of emerging technologies and assessing their possible legal impact. *Uniform Law Review*, 24(2), 302–314. https://doi.org/10.1093/ulr/unz018
16. Bao, Y., Gong, W., & Yang, K. (2023). A literature review of human–AI synergy in decision making. *Systems*, 11(9), Article 442. https://doi.org/10.3390/systems11090442
17. Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing-attack detection techniques. *Telecommunication Systems*, 76(1), 139–154. https://doi.org/10.1007/s11235-020-00733-2
18. Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation. *Harvard Journal of Law & Technology*, 31(2), 889–938.

https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf

19. Bauer, P. W., & Hancock, D. (1995). Scale economies and technological change in Federal Reserve ACH payment processing. *Economic Review* (Federal Reserve Bank of Cleveland), 31(3), 14–29.
20. Belanche, D., Casaló, L. V., & Flavián, C. (2019). Artificial intelligence in fintech: Understanding robo-advisor adoption among customers. *Industrial Management & Data Systems,* 119(7), 1411–1430. https://doi.org/10.1108/IMDS-08-2018-0368
21. Bella, F. I. (2020). Optimization of Islamic peer-to-peer lending for micro and small enterprises. *Journal of Islamic Economic Laws*, 3(2), 108–123. https://doi.org/10.23917/jisel.v3i2.11337
22. Belli, L., Curzi, Y., & Gaspar, W. B. (2023). AI regulation in Brazil: Advancements, flows, and need to learn from the data-protection experience. *Computer Law & Security Review*, 48, 105767. https://doi.org/10.1016/j.clsr.2022.105767
23. Berg, T., Fuster, A., & Puri, M. (2022). Fintech lending. *Annual Review of Financial Economics*, 14, 187–207. https://doi.org/10.1146/annurev-financial-101521-112042
24. Berger, A. N., & Frame, W. S. (2007). Small business credit scoring and credit availability. *Journal of Small Business Management*, 45(1), 5–22. https://doi.org/10.1111/j.1540-627X.2007.00195.x
25. Bertino, E., Kundu, A., & Sura, Z. (2019). Data transparency with blockchain and AI ethics. *Journal of Data and Information Quality*, 11(4), Article 16. https://doi.org/10.1145/3312750
26. Bharanitharan, K., & Kaur, G. (2024). The development of AI regulations in fintech. *Journal of Informatics Education and Research*, 4(3), 640–641. https://doi.org/10.52783/jier.v4i3.1361
27. Bholat, D., & Susskind, D. (2021). The assessment: Artificial intelligence and financial services. *Oxford Review of Economic Policy*, 37(3), 417–434. https://doi.org/10.1093/oxrep/grab015
28. Bickley, S. J., & Torgler, B. (2023). Cognitive architectures for artificial-intelligence ethics. *AI & Society*, 38(2), 501–519. https://doi.org/10.1007/s00146-022-01452-9
29. Blythe, J. M., Sombatruang, N., & Johnson, S. D. (2019). What security features and crime-prevention advice is communicated in consumer IoT device manuals and support pages? *Journal of Cybersecurity*, 5(1), Article tyz005. https://doi.org/10.1093/cybsec/tyz005

30. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2), 213–238. https://doi.org/10.1257/jep.29.2.213
31. Bono, T., Croxson, K., & Giles, A. (2021). Algorithmic fairness in credit scoring. *Oxford Review of Economic Policy*, 37(3), 585–617. https://doi.org/10.1093/oxrep/grab020
32. Bredt, S. (2019). Artificial intelligence (AI) in the financial sector—Potential and public strategies. *Frontiers in Artificial Intelligence*, 2, Article 16. https://doi.org/10.3389/frai.2019.00016
33. Bromberg, L., Godwin, A., & Ramsay, I. (2018). Cross-border cooperation in financial regulation: Crossing the Fintech bridge. *Capital Markets Law Journal,* 13(1), 59–84. https://doi.org/10.1093/cmlj/kmx041
34. Brophy, J. E. (2020). Blockchain and insurance: A review for operations and regulation. *Journal of Financial Regulation & Compliance*, 28(2), 215–234. https://doi.org/10.1108/JFRC-09-2018-0127
35. Brożek, B., Furman, M., Jakubiec, M., & Tajsner, M. (2024). The black box problem revisited: Real and imaginary challenges for automated legal decision making. *Artificial Intelligence and Law*, 32, 427–440. https://doi.org/10.1007/s10506-023-09356-9
36. Brummer, C., & Yadav, Y. (2018). Fintech and the innovation trilemma. *Georgetown Law Journal*, 107(2), 235–307. https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/02/1Fintech-and-the-Innovation-Trilemma.pdf
37. Bruton, G. D., Khavul, S., Siegel, D., & Wright, M. (2015). New financial alternatives in seeding entrepreneurship: Microfinance, crowdfunding, and peer-to-peer innovations. *Entrepreneurship Theory and Practice*, 39(1), 9–26. https://doi.org/10.1111/etap.12143
38. Buiten, M., de Streel, A., & Peitz, M. (2023). The law and economics of AI liability. *Computer Law & Security Review*, 48, 105794. https://doi.org/10.1016/j.clsr.2023.105794
39. Cai, L. (2018). Disruption of financial intermediation by fintech: A review on crowdfunding and blockchain. *Accounting & Finance*, 58(4), 965–992. https://doi.org/10.1111/acfi.12405
40. Cath, C. (2018). Governing artificial intelligence: Ethical, legal and technical opportunities and challenges. Philosophical Transactions of the Royal Society A: Mathematical, *Physical and Engineering Sciences*, 376(2133), 20180080. https://doi.org/10.1098/rsta.2018.0080

41. Čerka, P., Grigiene, J., & Sirbikyte, G. (2015). Liability for damages caused by artificial intelligence. *Computer Law & Security Review*, 31(3), 376–389. https://doi.org/10.1016/j.clsr.2015.03.008
42. Chander, A. (2019). The Internet of Things: Both goods and services. World Trade Review, 18(S1), S9–S22. https://doi.org/10.1017/S1474745619000089
43. Chatterjee, S. (2023). E-contracts: Legal implications and regulatory challenges in the digital era. *International Journal of Creative Research Thoughts*, 11(12), Article IJCRT2312463. https://ijcrt.org/papers/IJCRT2312463.pdf
44. Cho, K. (2024). New sustainable fintech business models created by open-banking API platforms. *Sustainability*, 16(16), 7187. https://doi.org/10.3390/su16167187
45. Cioffi, R., Travaglioni, M., & Piscitelli, G. (2020). Artificial intelligence and machine-learning applications in smart production: Progress, trends, and directions. *Sustainability*, 12(2), 492. https://doi.org/10.3390/su12020492
46. Colombage, S. (2023). Financial technology (fintech) and sustainable financing: A new paradigm for risk management. *Journal of Risk and Financial Management*, 16(12), 502. https://doi.org/10.3390/jrfm16120502
47. Colombo, E., Mercorio, F., & Mezzanzanica, M. (2019). AI meets labour market: Exploring the link between automation and skills. *Information Economics and Policy*, 47, 27–37. https://doi.org/10.1016/j.infoecopol.2019.05.003
48. Cretarola, A., Figà-Talamanca, G., & Grunspan, C. (2021). Blockchain and cryptocurrencies: Economic and financial research. *Decisions in Economics and Finance*, 44, 141–167. https://doi.org/10.1007/s10203-021-00366-3
49. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review*, 2, 6–10. https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf
50. Cuccuru, P. (2017). Beyond bitcoin: An early overview on smart contracts. *International Journal of Law and Information Technology*, 25(3), 179–195. https://doi.org/10.1093/ijlit/eax003
51. Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2008). Past, present and future of mobile-payments research: A literature review. *Electronic Commerce Research and Applications*, 7(2), 165–181. https://doi.org/10.1016/j.elerap.2007.02.001
52. Das, S. R. (2019). The future of fintech. *Financial Management*, 48(4), 981–1007. https://doi.org/10.1111/fima.12297
53. de Almeida, P. G. R., dos Santos, C. D., & Farias, J. S. (2021). Artificial-intelligence regulation: A framework for governance. *Ethics and Information Technology*, 23, 505–525. https://doi.org/10.1007/s10676-021-09593-z

54. Du, H., & Le, D-P. (2022). A review of blockchain in fintech: Taxonomy, challenges, and future directions. *Cryptography*, 6(2), 18. https://doi.org/10.3390/cryptography6020018
55. Duffourc, M. N., & Gerke, S. (2023). The proposed EU directives for AI liability leave worrying gaps likely to impact medical AI. *NPJ Digital Medicine*, 6, Article 39. https://doi.org/10.1038/s41746-023-00823-w
56. El Hajj, M., & Hammoud, J. (2023). Unveiling the influence of artificial intelligence and machine learning on financial markets: A comprehensive analysis of AI applications in trading, risk-management, and financial operations. *Journal of Risk and Financial Management,* 16(10), 434. https://doi.org/10.3390/jrfm16100434
57. Fenwick, M., & Vermeulen, E. P. M. (2020). Banking and regulatory responses to fintech revisited—Building the sustainable financial-service "ecosystems" of tomorrow. *Singapore Journal of Legal Studies*, 2020, 165–189. https://doi.org/10.2307/27032605
58. Ferrara, E. (2024). Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies. *Sci,* 6(1), 3. https://doi.org/10.3390/sci6010003
59. Ferreira, F. G. D. C., Gandomi, A. H., & Cardoso, R. T. N. (2021). Artificial intelligence applied to stock-market trading: A review. *IEEE Access*, 9, 30898–30917. https://doi.org/10.1109/ACCESS.2021.3058133
60. FinTech (MDPI). (2023). *AI in the financial sector: Innovation and responsibility* [Special-issue editorial]. https://doi.org/10.3390/info15080432
61. Fuster, A., Plosser, M., Schnabl, P., & Vickery, J. (2019). The role of technology in mortgage lending. *Review of Financial Studies*, 32(5), 1854–1899. https://doi.org/10.1093/rfs/hhz018
62. Gaffar, H., & Albarashdi, S. (2024). Copyright protection for AI-generated works: Exploring originality and ownership in a digital landscape. *Asian Journal of International Law*, 14(2), 1–24. https://doi.org/10.1017/S2044251323000735
63. García-Corral, F. J., Cordero-García, J. A., de Pablo-Valenciano, J., & Uribe-Toril, J. (2022). A bibliometric review of cryptocurrencies: How have they grown? *Financial Innovation*, 8, Article 9. https://doi.org/10.1186/s40854-021-00306-5
64. Garcia, A. C. B., Garcia, M. G. P., & Rigobon, R. (2024). Algorithmic discrimination in the credit domain: What do we know about it? *AI & Society*, 39, 2059–2098. https://doi.org/10.1007/s00146-023-01676-3
65. Gaspar, R. M., & Oliveira, M. (2024). Robo-advising and investor profiling. *FinTech*, 3(1), 102–115. https://doi.org/10.3390/fintech3010007

66. Gasser, U. (2023). An EU landmark for AI governance. *Science*, 380(6651), 1203. https://doi.org/10.1126/science.adj1627
67. Georgieff, A., & Hyee, R. (2022). Artificial intelligence and employment: New cross-country evidence. *Frontiers in Artificial Intelligence*, 5, Article 832736. https://doi.org/10.3389/frai.2022.832736
68. Ghioni, R., Taddeo, M., & Floridi, L. (2024). Open-source intelligence and AI: A systematic review of the GELSI literature. *AI & Society*, 39, 2167–2192. https://doi.org/10.1007/s00146-023-01628-x
69. Giuffrida, I. (2019). Liability for AI decision-making: Some legal and ethical considerations. *Fordham Law Review,* 88(2), 439–478. https://ir.lawnet.fordham.edu/flr/vol88/iss2/3
70. Gomber, P., Koch, J.-A., & Siering, M. (2017). Digital finance and fintech: Current research and future research directions. *Journal of Business Economics*, 87(5), 537–580. https://doi.org/10.1007/s11573-017-0852-x
71. Gunning, D., Stefik, M., Choi, J., Miller, T., Stumpf, S., & Yang, G. Z. (2019). XAI—Explainable artificial intelligence. *Science Robotics*, 4(37), eaay7120. https://doi.org/10.1126/scirobotics.aay7120
72. Headinger, G., Cohen, L., & Gong, Z. (2024). Managing, preserving, and unlocking wealth through fintech. *Harvard Business School*. https://www.hbs.edu/faculty/Pages/item.aspx?num=66090
73. Hendershott, T., Zhang, X., Zhao, J. L., & Zheng, Z. (2021). Fintech as a game changer: Overview of research frontiers. *Information Systems Research*, 32(1), 1–17. https://doi.org/10.1287/isre.2021.0997
74. Hentzen, J. K., Hoffmann, A., Dolan, R., & Pala, E. (2022). Artificial intelligence in customer-facing financial services: A systematic literature review and agenda for future research. *International Journal of Bank Marketing*, 40(6), 1299–1336. https://doi.org/10.1108/IJBM-09-2021-0417
75. How, M. L., Cheah, S. M., Khor, A. C., & Chan, Y. J. (2020). Artificial-intelligence-enhanced predictive insights for advancing financial inclusion: A human-centric AI-thinking approach. *Big Data and Cognitive Computing*, 4(2), Article 11. https://doi.org/10.3390/bdcc4020008
76. Hua, X., Huang, Y., & Zheng, Y. (2019). Current practices, new insights, and emerging trends of financial technologies. *Industrial Management & Data Systems*, 119(7), 1401–1410. https://doi.org/10.1108/IMDS-08-2019-0431
77. Huynh, T. L. D., Hille, E., & Nasir, M. A. (2020). Diversification in the age of the 4th industrial revolution: The role of artificial intelligence, green bonds and

cryptocurrencies. *Technological Forecasting and Social Change*, 159, 120188. https://doi.org/10.1016/j.techfore.2020.120188

78. Ienca, M. (2023). On artificial intelligence and manipulation. *Topoi*, 42, 833–842. https://doi.org/10.1007/s11245-023-09940-3
79. ISACA. (2020). A fintech risk-assessment model. *ISACA Journal*, 2020(3). https://www.isaca.org/resources/isaca-journal/issues/2020/volume-3/a-fintech-risk-assessment-model
80. Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., … Shafiq, M. (2022). Detection of distributed denial-of-service (DDoS) attacks in IoT-based monitoring system of banking sector using machine-learning models. *Sustainability,* 14(14), 8374. https://doi.org/10.3390/su14148374
81. Jaswant, S., & Kale, P. (2022). Smart contracts and blockchain: Legal issues and implications for Indian contract law. *International Review of Law, Computers & Technology*, 36(2), 1–18. https://doi.org/10.1080/13600869.2021.1999312
82. Jiao, Z., Shahid, M. S., Mirza, N., & Tan, Z. (2021). Should the Fourth Industrial Revolution be widespread or confined geographically? *Technological Forecasting and Social Change*, 166, 120442. https://doi.org/10.1016/j.techfore.2020.120442
83. Judge, B., Nitzberg, M., & Russell, S. (2024). When code isn't law: Rethinking regulation for artificial intelligence. Policy and Society. *Advance online publication*. https://doi.org/10.1093/polsoc/puae020
84. Kapsis, I. (2020). Blockchain and cryptocurrencies: Essential tools in a two-tier financial system. *Capital Markets Law Journal*, 15(1), 18–47. https://doi.org/10.1093/cmlj/kmz025
85. Kayani, U., & Hasan, F. (2024). Unveiling cryptocurrency impact on financial markets and traditional banking systems. *Journal of Risk and Financial Management,* 17(2), 58. https://doi.org/10.3390/jrfm17020058
86. Kgoroeadira, R., Burke, A., & van Stel, A. (2019). Small business online loan crowdfunding: Who gets funded and what determines the rate of interest? *Small Business Economics,* 52(1), 67–87. https://doi.org/10.1007/s11187-017-9986-z
87. Khan, S. N., Loukil, F., Ghedira-Guegan, C., et al. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications,* 14, 2901–2925. https://doi.org/10.1007/s12083-021-01127-0
88. Khando, K., Islam, M. S., & Gao, S. (2023). The emerging technologies of digital payments and associated challenges: A systematic literature review. *Future Internet*, 15(1), 21. https://doi.org/10.3390/fi15010021

89. Kirakosyan, A. (2023). Intellectual property ownership of AI-generated content. *Digital Law Journal*, 4(3), Article e003. https://doi.org/10.38044/2686-9136-2023-4-3-3
90. Kumar, A., Sahoo, S., & Lim, W. M. (2020). A framework of mobile-banking adoption in India. *Journal of Open Innovation: Technology, Market, and Complexity*, 6(2), 40. https://doi.org/10.3390/joitmc6020040
91. Kramcsák, P. T. (2023). Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets? *Computer Law and Security Review*, https://doi.org/10.1016/j.clsr.2022.105765
92. Lee, J. (2020). Access to finance for artificial-intelligence regulation in the financial-services industry. *European Business Organization Law Review*, 21, 731–757. https://doi.org/10.1007/s40804-020-00200-0
93. Lenz, R. (2016). Peer-to-peer lending: Opportunities and risks. *European Journal of Risk Regulation*, 7(4), 688–700. https://doi.org/10.1017/S1867299X00010126
94. Li, X., & Zhang, Y. (2022). Financial-fraud detection based on machine learning: A systematic literature review. *Applied Sciences*, 12(19), 9637. https://doi.org/10.3390/app12199637
95. Lifshitz, L. R. (2024). Security-by-design. *Stanford Journal of Blockchain Law & Policy,* 7(1), 45–58. https://doi.org/10.2307/27180316
96. Lin, L., & Chen, C. (2020). The promise and perils of insurtech. *Singapore Journal of Legal Studies*, 2020(2), 212–231. https://doi.org/10.2139/ssrn.3463533
97. Lui, A., & Lamb, G. W. (2018). Artificial intelligence and augmented-intelligence collaboration: Regaining trust and confidence in the financial sector. *Information & Communications Technology Law*, 27(3), 267–283. https://doi.org/10.1080/13600834.2018.1488659
98. Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart-contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, 35, 233–243. https://doi.org/10.1016/j.tele.2018.10.004
99. Maier, E. (2016). Supply and demand on crowdlending platforms: Connecting small and medium-sized-enterprise borrowers and consumer investors. *Journal of Retailing and Consumer Services,* 33, 143–153. https://doi.org/10.1016/j.jretconser.2016.08.004
100. Manser Payne, E., Peltier, J. W., & Barger, V. A. (2018). Mobile banking and AI-enabled mobile banking: The differential effects of technological and non-technological factors on digital natives' perceptions and behaviour. *Journal of Research in Interactive Marketing,* 12(3), 328–346. https://doi.org/10.1108/JRIM-07-2018-0087

101. Maras, M.-H. (2015). Internet of Things: Security and privacy implications. *International Data Privacy Law*, 5(2), 99–104. https://doi.org/10.1093/idpl/ipv004
102. Merritt, C. G. (2023). A compulsory solution to the machine problem: Recognizing artificial intelligence as inventors in patent law. *Vanderbilt Journal of Entertainment & Technology Law,* 25(1), 211–246. https://scholarship.law.vanderbilt.edu/jetlaw/vol25/iss1/5
103. Mhlanga, D. (2020). Industry 4.0 in finance: The impact of artificial intelligence on digital financial inclusion. *International Journal of Financial Studies*, 8(3), 45. https://doi.org/10.3390/ijfs8030045
104. Milana, C., & Ashta, A. (2021). Artificial-intelligence techniques in finance and financial markets: A survey of the literature. *Strategic Change*, 30(3), 189–209. https://doi.org/10.1002/jsc.2403
105. Muthukannan, P., Tan, B., Gozman, D., & Johnson, L. (2020). The emergence of a fintech ecosystem: A case study of the Vizag FinTech Valley in India. *Information & Management,* 57(8), 103385. https://doi.org/10.1016/j.im.2020.103385
106. Neilson, B. (2023). Artificial-intelligence authoring financial recommendations: Comparative Australian evidence. *Journal of Financial Regulation,* 9(3), 395-420. https://doi.org/10.1093/jfr/fjad004
107. Nemitz, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. *Philosophical Transactions of the Royal Society A*, 376(2133), 20180089. https://doi.org/10.1098/rsta.2018.0089
108. Nguyen Thanh, B., Son, H. X., & Vo, D. T. H. (2024). Blockchain: The economic and financial institution for autonomous AI? *Journal of Risk and Financial Management*, 17(2), 54. https://doi.org/10.3390/jrfm17020054
109. Ní Loideáin, N., & Adams, R. (2020). From Alexa to Siri and the GDPR: The gendering of virtual personal assistants and the role of data-protection impact assessments. *Computer Law & Security Review*, 36, 105366. https://doi.org/10.1016/j.clsr.2019.105366
110. Noriega, J. P., Rivera, L. A., & Herrera, J. A. (2023). Machine learning for credit-risk prediction: A systematic literature review. *Data*, 8(11), 169. https://doi.org/10.3390/data8110169
111. Ntoutsi, E., Fafalios, P., Gadiraju, U., et al. (2020). Bias in data-driven artificial-intelligence systems: An introductory survey. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery,* 10(3), e1356. https://doi.org/10.1002/widm.1356

112. Olaiya, O. P., Adesoga, T. O., Pieterson, K., Obani, O. Q., & Adebayo, J. O. (2024). RegTech solutions: Enhancing compliance and risk management in the financial industry. *GSC Advanced Research and Reviews*, 20(2), 8–15. https://doi.org/10.30574/gscarr.2024.20.2.0295

113. Omarova, S. T. (2020). Technology v technocracy: FinTech as a regulatory challenge. *Journal of Financial Regulation*, 6(1), 75–124. https://doi.org/10.1093/jfr/fjaa004

114. Packin, N. G. (2018). RegTech, compliance, and the technology-judgment rule. *Chicago-Kent Law Review*, 93(3), 757–796. https://ssrn.com/abstract=3043021

115. Pagallo, U., Casanovas, P., & Madelin, R. (2019). The middle-out approach: Assessing models of legal governance in data protection, artificial intelligence, and the Web of Data. *Theory and Practice of Legislation*, 7(1), 1–25. https://doi.org/10.1080/20508840.2019.1664543

116. Paiva, F., Cardoso, R., Hanaoka, G., & Duarte, W. (2018). Decision-making for financial trading: A fusion approach of machine learning and portfolio selection. *Expert Systems with Applications*, 115, 582–599. https://doi.org/10.1016/j.eswa.2018.08.003

117. Pandey, D., & Raghunath, H. (2020). Stationing smart contract as a "contract": A case for interpretative reform of the Indian Contract Act, 1872. *NUJS Law Review*, 13(4), 1–27. https://nujslawreview.org/2021/01/12/stationing-smart-contract-as-a-contract-a-case-for-interpretative-reform-of-the-indian-contract-act-1872

118. Parminder, V., Shivinder, N., & Kiran, S. (2022). A thematic analysis of fintech influence on the banking industry. *Risks,* 10(10), 186. https://doi.org/10.3390/risks10100186

119. Patel, S. R., & Patil, R. (2022). An analysis of the fintech regulations in India. *Indian Journal of Integrated Research in Law*, 2(4), 1–18. https://ijirl.com/wp-content/uploads/2022/09/AN-ANALYSIS-OF-THE-FINTECH-REGULATIONS-IN-INDIA-.pdf

120. Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: The dawn of a new era. *Journal of Money Laundering Control*, 26(7), 155–166. https://doi.org/10.1108/JMLC-03-2023-0050

121. Peterson, P., & Konstantopoulos, T. (2021). Insurtech and the disruption of the insurance industry. *Journal of Insurance Issues*, 43(2), 64–96.

122. Pinheiro, P. P., & Battaglini, H. B. (2022). Artificial intelligence and data protection: A comparative analysis of AI regulation through the lens of data

protection in the EU and Brazil. *GRUR International*, 71(10), 924–932. https://doi.org/10.1093/grurint/ikac049

123. Polak, P., Nelischer, C., Guo, H., et al. (2020). "Intelligent" finance and treasury management: What we can expect. *AI & Society*, 35, 715–726. https://doi.org/10.1007/s00146-019-00919-6

124. Poudel, S. (2016). Internet of Things underlying technologies, interoperability, and threats to privacy. *Berkeley Technology Law Journal*, 31(2), 997–1022. https://doi.org/10.15779/Z38PK26

125. Prem, E. (2023). From ethical AI frameworks to tools: A review of approaches. *AI Ethics*, 3(4), 699–716. https://doi.org/10.1007/s43681-023-00258-9

126. Raaijmakers, S. (2019). Artificial intelligence for law enforcement: Challenges and opportunities. *IEEE Security & Privacy*, 17(5), 74–77. https://doi.org/10.1109/MSEC.2019.2925649

127. Rahul, S. (2023). The role of artificial intelligence in financial decision making: Opportunities, challenges, and ethical considerations. *International Journal of Creative Research Thoughts*, 11 (5), j5–j9. https://www.ijcrt.org/papers/IJCRT23A5097.pdf

128. Reed, C. (2018). How should we regulate artificial intelligence? *Philosophical Transactions of the Royal Society A*, 376(2128), 20170360. https://doi.org/10.1098/rsta.2017.0360

129. Reher, M., & Sokolinski, S. (in press). Robo-advisors and access to wealth management. *Journal of Financial Economics*. Advance online version. http://dx.doi.org/10.2139/ssrn.3515707

130. Ridzuan, N. N., Masri, M., Anshari, M., Fitriyani, N. L., & Syafrudin, M. (2024). AI in the financial sector: The line between innovation, regulation and ethical responsibility. *Information*, 15(8), 432. https://doi.org/10.3390/info15080432

131. Ringe, W.-G., & Ruof, C. (2020). Regulating fintech in the EU: The case for a guided sandbox. *European Journal of Risk Regulation*, 11(3), 604–629. https://doi.org/10.1017/err.2020.8

132. Ruseva, M., Angelov, D., & Klisarova-Belcheva, S. (2023). Customer attitude toward digital wallet services. *Systems*, 11(4), 185. https://doi.org/10.3390/systems11040185

133. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply-chain management. *International Journal of Production Research*, 57(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

134. Sari, Yovita & Indrabudiman, Amir. (2024). The Role of Artificial Intelligence (AI) in Financial Risk Management. *Formosa Journal of Sustainable Research*. 3. 2073-2082. 10.55927/fjsr.v3i9.11436.

135. Saule T Omarova, Technology v Technocracy: Fintech as a Regulatory Challenge, *Journal of Financial Regulation*, Volume 6, Issue 1, 20 March 2020, Pages 75–124, https://doi.org/10.1093/jfr/fjaa004.

136. Schueffel, P. (2016). Taming the beast: A scientific definition of fintech. *Journal of Innovation Management*, 4(4), 32–54. https://doi.org/10.24840/2183-0606_004.004_0004

137. Shaikh, A. A., & Karjaluoto, H. (2015). Mobile-banking adoption: A literature review. *Telematics and Informatics*, 32(1), 129–142. https://doi.org/10.1016/j.tele.2014.05.003

138. Shim, Y., & Shin, D.-H. (2016). Analysing China's fintech industry from the perspective of actor–network theory. *Telecommunications Policy*, 40(2), 168–181. https://doi.org/10.1016/j.telpol.2015.11.005

139. Shoetan, P., & Familoni, B. (2024). Transforming fintech fraud detection with advanced artificial-intelligence algorithms. *Finance & Accounting Research Journal,* 6(4), 602–625. https://doi.org/10.51594/farj.v6i4.1036

140. Siciliani, P. (2019). The disruption of the prudential regulatory framework. *Journal of Financial Regulation*, 5(2), 220–238. https://doi.org/10.1093/jfr/fjz009

141. Sinha, S., & Lee, Y.-M. (2024). Challenges with developing and deploying AI models and applications in industrial systems. *Discover Artificial Intelligence*, 4, 55. https://doi.org/10.1007/s44163-024-00151-2

142. Sokolinski, S., Reher, M., & Baur, D. G. (2022). Fintech and financial inclusion. *Southern California Law Review*, 95, 1–54. https://southerncalifornialawreview.com/wp-content/uploads/2023/04/Sokol_Final.pdf

143. Suhadolnik, N., & Ueyama, J. (2023). Machine learning for enhanced credit-risk assessment: An empirical approach. *Journal of Risk and Financial Management,* 16(12), 496. https://doi.org/10.3390/jrfm16120496

144. Svetlova, E. (2022). AI ethics and systemic risks in finance. *AI Ethics*, 2, 713–725. https://doi.org/10.1007/s43681-021-00129-1

145. Taherdoost, H. (2022). Blockchain technology and artificial intelligence: A critical review on applications. *Applied Sciences,* 12(24), 12948. https://doi.org/10.3390/app122412948

146. Tallberg, J., Erman, E., Furendal, M., Geith, J., Klamberg, M., & Lundgren, M. (2023). The global governance of artificial intelligence: Next steps for empirical

and normative research. *International Studies Review*, 25(3), viad040. https://doi.org/10.1093/isr/viad040

147. Trotta, A., Ziosi, M., & Lomonaco, V. (2023). The future of ethics in AI: Challenges and opportunities. *AI & Society*, 38, 245–258. https://doi.org/10.1007/s00146-022-01513-3

148. Uzougbo, C., Adeyemi, D., & Singh, R. (2024). Legal accountability and ethical considerations of AI in financial services. *GSC Advanced Research and Reviews,* 21(1), Article 0954. https://doi.org/10.30574/gscarr.2024.19.2.0171

149. van Bekkum, M., & Zuiderveen Borgesius, F. (2023). Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? *Computer Law & Security Review,* 48, 105770. https://doi.org/10.1016/j.clsr.2022.105770

150. Vassiliades, A., Bassiliades, N., & Patkos, T. (2021). Argumentation and explainable artificial intelligence: A survey. *The Knowledge Engineering Review*, 36, e04. https://doi.org/10.1017/S0269888921000011

151. Vesala, J. (2023). Developing artificial-intelligence-based content creation: Are EU copyright and antitrust law fit for purpose? IIC – *International Review of Intellectual Property and Competition Law*, 54(3), 351–380. https://doi.org/10.1007/s40319-023-01301-2

152. von Eschenbach, W. J. (2021). Transparency and the black-box problem: Why we do not trust AI. *Philosophy & Technology*, 34, 1607–1622. https://doi.org/10.1007/s13347-021-00477-0

153. Walker, G. (2017). Financial technology law – A new beginning and a new future. In *Fifty Years of the National University of Singapore Law Review* (Vol. 50, pp. 137–216). https://doi.org/10.2307/26415633

154. Weerawarna, R., Miah, S., & Shao, X. (2023). Emerging advances of blockchain technology in finance: A content analysis. *Personal and Ubiquitous Computing, 27*, 1–14. https://doi.org/10.1007/s00779-023-01712-5

155. Witt, C., & De Bruyne, J. (2023). The interplay between machine learning and data minimisation under the GDPR: The case of Google's Topics API. *International Data Privacy Law*, 13(4), 284–298. https://doi.org/10.1093/idpl/ipad020

156. Yap, J. Q., & Lim, E. (2022). A legal framework for artificial-intelligence fairness reporting. *Cambridge Law Journal*, 81(3), 610–644. https://doi.org/10.1017/S0008197322000460

157. Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial-intelligence capabilities to improve cybersecurity. *IEEE Access*, 8, 23817–23837. https://doi.org/10.1109/ACCESS.2020.2968045

158. Zhang, B. Z., Ashta, A., & Barton, M. E. (2021). Do FinTech and financial incumbents have different experiences and perspectives on the adoption of artificial intelligence? *Strategic Change*, 30(3), 223–234. https://doi.org/10.1002/jsc.2405
159. Züger, T., & Asghari, H. (2023). AI for the public: How public-interest theory shifts the discourse on AI. *AI & Society*, 38(2), 815–828. https://doi.org/10.1007/s00146-022-01480-5
160. Zuiderveen Borgesius, F. J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *International Journal of Human Rights,* 24(10), 1572–1593. https://doi.org/10.1080/13642987.2020.1743976

CONFERENCE PAPER/PROCEEDINGS

1. Al-Ameer, A., & Al-Sunni, F. (2021). A methodology for securities and cryptocurrency trading using exploratory data analysis and artificial intelligence. In *Proceedings of the 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA 2021)* (pp. 54–61). IEEE. https://doi.org/10.1109/CAIDA51941.2021.9425223
2. Amity University, & Institute of Electrical and Electronics Engineers (Eds.). (2020). *ICRITO 2020: Proceedings of the IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization* (Trends and Future Directions), 4–5 June 2020, Amity University, Noida, India. IEEE.
3. Amity University, Institute of Electrical and Electronics Engineers United Kingdom & Republic of Ireland Section, & Institute of Electrical and Electronics Engineers (Eds.). (2019). *Proceedings of the International Conference on Automation, Computational and Technology Management (ICACTM 2019),* 24–25 April 2019, Amity University, Noida, India. IEEE.
4. Bajracharya, A., Khakurel, U., Harvey, B., & Rawat, D. B. (2023). Recent advances in algorithmic biases and fairness in financial services: A survey. In K. Arai (Ed.), *Proceedings of the Future Technologies Conference (FTC 2022), Volume 1* (Lecture Notes in Networks and Systems, Vol. 559, pp. 597–612). Springer. https://doi.org/10.1007/978-3-031-18461-1_53
5. Brandes, U., Reddy, C., & Tagarelli, A. (Eds.). (2018). Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2018), 28–31 August 2018, Barcelona, Spain. *ACM.*
6. Erdélyi, O. J., & Goldsmith, J. (2018). Regulating artificial intelligence: Proposal for a global solution. In Proceedings of the 2018 AAAI/ACM Conference on AI,

Ethics, and Society (AIES 2018) (pp. 95–101). *ACM*. https://doi.org/10.1145/3278721.3278731

7. Everitt, T. (2018). AGI safety and control challenges. *Journal of Artificial Intelligence Research*, https://www.ijcai.org/proceedings/2018/0768.pdf
8. García Bringas, P., Pastor-López, I., & Psaila, G. (2019, September 12–13). Current trends for blockchain and smart-contracts in financial services. *In Proceedings of ENTRENOVA 2019 – Conference on Interdisciplinary Management Research* (pp. 223–231). Split, Croatia. https://doi.org/10.2139/ssrn.3491754
9. Hsu, H.-H., Huang, N.-F., & Han, C.-H. (2020, May). Collision analysis to motor dashcam videos with YOLO and Mask R-CNN for auto insurance. In *Proceedings of the 2020 International Conference on Intelligent Engineering and Management* (ICIEM) (pp. 311–315). IEEE. https://doi.org/10.1109/ICIEM48762.2020.9160263
10. Zavolokina, L., Dolata, M., & Schwabe, G. (2016, December). FinTech – What's in a name? *In Proceedings of the 37th International Conference on Information Systems (ICIS 2016)* (pp. 1–19). AIS e-Library. https://www.zora.uzh.ch/id/eprint/126806/1/FinTech_Research_Paper_revised.pdf

WORKING PAPERS / PREPRINTS

1. AI in finance: Challenges, techniques, and opportunities. (2021). *arXiv.* https://doi.org/10.48550/arXiv.2107.09051
2. Bao, Y., Hilary, G., & Ke, B. (in press). Artificial intelligence and fraud detection. In V. Babich, J. Birge, & G. Hilary (Eds.), Innovative technology at the interface of finance and operations (Springer Series in Supply Chain Management). *Springer Nature.* Advance online version. https://doi.org/10.2139/ssrn.3738618
3. Buterin, V. (2013). A next-generation smart-contract & decentralized-application platform (White paper). *Ethereum Foundation*. https://ethereum.org/en/whitepaper
4. Cao, L. (2021). AI in Finance: Challenges, Techniques, and Opportunities. https://doi.org/10.48550/arXiv.2107.09051
5. Capponi, A., Olafsson, S., & Zariphopoulou, T. (2019). Personalized robo-advising: Enhancing investment through client interaction *(arXiv:1911.01391). arXiv*. https://arxiv.org/abs/1911.01391
6. Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2017). Artificial intelligence and the "good society" – The US, EU, and UK approach *(SSRN Working Paper No. 2906249). SSRN.* https://doi.org/10.2139/ssrn.2906249
7. Di Maggio, M., Ratnadiwakara, D., & Carmichael, D. (2022). Invisible primes: Fintech lending with alternative data (NBER Working Paper No. 29840). *National Bureau of Economic Research.* https://doi.org/10.3386/w29840

8. Goldblum, M., Schwarzschild, A., Patel, A. B., & Goldstein, T. (2020). Adversarial attacks on machine-learning systems for high-frequency trading *(arXiv:2002.09565). arXiv.* https://arxiv.org/abs/2002.09565
9. Frame, W. S., Srinivasan, A., & Woosley, L. (2001). The effect of credit scoring on small-business lending. *Journal of Money, Credit and Banking*, 33(3), 813–825. https://www.econstor.eu/bitstream/10419/100916/1/wp2001-06.pdf
10. Han, S., Kim, J., Lee, S.-J., & Yun, I. (2024). Automated attack synthesis for constant-product market makers *(arXiv:2404.05297). arXiv.* https://arxiv.org/abs/2404.05297
11. Maple, C., et al. (2023). The AI revolution: Opportunities and challenges for the finance sector *(arXiv:2308.16538). arXiv*. https://doi.org/10.48550/arXiv.2308.16538
12. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf
13. Rathi, S. (2022). Approaches to artificial general intelligence: An analysis *(arXiv:2202.03153). arXiv.* https://doi.org/10.48550/arXiv.2202.03153
14. Tasca, P., & de Roure, C. (2014). Bitcoin and the PPP puzzle *(SSRN Working Paper No. 2461588).* https://doi.org/10.2139/ssrn.2461588
15. Ungureanu, C. T., & Amironesei, A. E. (2023, October 31). Legal issues concerning generative AI technologies *(SSRN Working Paper No. 4689630). SSRN*. https://ssrn.com/abstract=4689630

TECHNICAL & POLICY / REPORTS & SPEECHES

1. Ahluwalia, S. M., Malhotra, H., & Kharmih, L. K. (2024, March 21). *Fintech 2024: Trends and developments in India.* Chambers and Partners. https://practiceguides.chambers.com/practice-guides/fintech-2024/india/trends-and-developments/O16329
2. Bagai, R., Uppal, A., & Baidwan, N. (2024). *Fintech laws and regulations 2024: India.* Global Legal Insights. https://globallegalinsights.com/practice-areas/fintech-laws-and-regulations/india/
3. Bank for International Settlements, Committee on Payments and Market Infrastructures. (2020). *Enhancing cross-border payments: Stage 3 roadmap.* https://www.bis.org/cpmi/publ/d198.pdf
4. Bank for International Settlements. (2021). *Fintech and payments: Regulating digital-payment services and e-money* (BIS Papers No. 124). https://www.bis.org

5. Bank for International Settlements. (2021). *Fintech and the digital transformation of financial services* (BIS Papers No. 117). https://www.bis.org
6. Boston Consulting Group & China Development Research Foundation. (2018). *The impact of AI on the financial job market.* https://en.cdf.org.cn/cdf2018en/qybg/5261.htm?share=true#content
7. Boukherouaa, E. S. B. (2023, August 18). *Generative artificial intelligence in finance: Risk considerations* (IMF Fintech Note No. 2023/004). International Monetary Fund. https://www.imf.org/en/Publications/fintech-notes/Issues/2023/08/18/Generative-Artificial-Intelligence-in-Finance-Risk-Considerations-537570
8. Boukherouaa, E., AlAjmi, K., Deodoro, J., Farias, A., & Ravikumar, R. (2021). *Powering the digital economy: Opportunities and risks of artificial intelligence in finance*. International Monetary Fund. https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2021/10/21/Powering-the-Digital-Economy-Opportunities-and-Risks-of-Artificial-Intelligence-in-Finance-494717
9. Carstens, A. (2024, October 31). *The future of finance* [Speech]. Bank for International Settlements. https://www.bis.org/speeches/sp241031.htm
10. Choudhary, A. K. (2024, July 18). *Fintech sector—Catalyst to growth: Special keynote address at ASSOCHAM's 2nd India International Fintech Festival* [Speech transcript]. National Payments Corporation of India. https://www.npci.org.in/PDF/npci/chairman-speeches/2024/Special-Keynote-Address-delivered-by-Shri-Ajay-Kumar-Choudhary-Non-Executive-Chairman-and-Independent-Director.pdf
11. Comunale, M., & Manera, A. (2024). *The economic impacts and the regulation of AI: A review of the academic literature and policy actions* (IMF Staff Discussion Note). International Monetary Fund. https://www.imf.org/en/Publications/WP/Issues/2024/03/22/The-Economic-Impacts-and-the-Regulation-of-AI-A-Review-of-the-Academic-Literature-and-546645
12. Cross-Border Data Forum. (2021). *Cross-border data transfers in financial services: The EU's new regulatory approach.* https://www.crossborderdataforum.org/cross-border-data-transfers-in-financial-services-the-eus-new-regulatory-approach/
13. Dechert LLP. (2023). *Artificial intelligence: Legal and regulatory issues for financial services*. Dechert LLP.

https://www.dechert.com/knowledge/onpoint/2023/4/artificial-intelligence--legal-and-regulatory-issues-for-financi.html

14. Deloitte Insights. (2024). *AI in financial services*. Deloitte LLP. https://www2.deloitte.com/us/en/insights/research-centers/center-for-financial-services/ai-in-financial-services.html
15. Deloitte. (2020). *Cross-border payments on blockchain: Enabling business-to-business and person-to-person payments across borders on vendor blockchain-based payment rails.* Deloitte Touche Tohmatsu Limited. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/grid/cross-border-payments.pdf
16. Deloitte. (2023). *The Digital Personal Data Protection Act, 2023: Key provisions and impact.* Deloitte Touche Tohmatsu India LLP. https://www2.deloitte.com/in/en/pages/risk/articles/the-digital-personal-data-protection-act-2023.html
17. Deloitte. (2024, February 21). *Cross-jurisdictional data protection and AI overview – Second edition*. https://www.deloitte.com/global/en/services/legal/analysis/cross-jurisdictional-data-protection-ai-overview.html
18. Dhapte, A. (2025, May). *Europe digital-payment market research report: Forecast till 2032.* Market Research Future. https://www.marketresearchfuture.com/reports/europe-digital-payment-market-21609
19. Enterslice. (2024). *RBI's 2024 regulatory sandbox framework*. https://www.enterslice.com
20. European Banking Authority. (n.d.). *Financial innovation and fintech.* https://www.eba.europa.eu/financial-innovation-and-fintech
21. European Central Bank. (2025, May 15). *Harnessing the digital future of payments: Europe's path to sovereignty and innovation* [Speech]. https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp250515~fd8adac5a4.pt.html
22. European Commission. (2024, August 1). *AI Act enters into force.* https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en
23. European Insurance and Occupational Pensions Authority. (2024). *The AI Act and its impacts on the European financial sector.* https://www.eiopa.europa.eu/publications/ai-act-and-its-impacts-european-financial-sector_en
24. EY India. (2023). *Digital Personal Data Protection Act (2023): How fintech companies are dealing with new data-security challenges.* EY India.

https://www.ey.com/en_in/media/podcasts/gateway-to-data-privacy-and-protection/2023/09/episode-4-digital-personal-data-protection-act-how-fintech-companies-are-dealing-with-new-data-security-challenges

25. EY India. (2024). *AI in India: A policy agenda.* EY India. https://www.ey.com/en_in/services/ai/generative-ai-india-report/policy-agenda-india
26. EY. (2023). *The artificial intelligence (AI) global regulatory landscape: Policy trends and considerations.* EY Global. https://assets.ey.com/content/dam/ey-sites/ey-com/en_ch/noindex/ey-the-artificial-intelligence-ai-global-regulatory-landscape.pdf
27. Financial Stability Board. (2023, December 12). *Fintech.* https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/fintech
28. Financial Stability Board. (2024, June 4). *Remarks on artificial intelligence in finance* [Speech transcript]. https://www.fsb.org/2024/06/remarks-by-nellie-liang-on-artificial-intelligence-in-finance/
29. FS-ISAC. (2024). *Deepfakes in the financial sector: Understanding the threats and managing the risks*. https://www.fsisac.com/hubfs/Knowledge/AI/DeepfakesInTheFinancialSector-UnderstandingTheThreatsManagingTheRisks.pdf
30. Gambacorta, L., Huang, Y., Qiu, H., & Wang, J. (2019). *How do machine learning and non-traditional data affect credit scoring?* (BIS Working Paper No. 834). Bank for International Settlements. https://www.bis.org
31. Global Legal Insights. (2024). *Blockchain and cryptocurrency laws and regulations 2024.* https://www.globallegalinsights.com
32. GreyB. (2025). *AI-driven analysis for smart contract security*. https://xray.greyb.com/artificial-intelligence/smart-contract-analysis-ai
33. Herian, R. (2019, January 14). *Legal recognition of blockchain registries and smart contracts.* European Commission. Retrieved from https://blockchain-observatory.ec.europa.eu/publications/legal-recognition-blockchain-registries-and-smart-contracts_en
34. International Monetary Fund. (2023). *Fintech payments in public financial management: Benefits and risks* (IMF Working Paper 23/26). https://www.imf.org/en/Publications/WP/Issues/2023/02/03/Fintech-Payments-in-Public-Financial-Management-Benefits-and-Risks-529100
35. International Monetary Fund. (2024, September 6). *Artificial intelligence and its impact on financial markets and financial stability*.

https://www.imf.org/en/News/Articles/2024/09/06/sp090624-artificial-intelligence-and-its-impact-on-financial-markets-and-financial-stability

36. Internet Crime Complaint Center (IC3). (2024, December 3). *Public service announcement: Cyber-fraud trends for 2024*. https://www.ic3.gov/PSA/2024/PSA241203
37. Jain, M. K. (2023, March 15). *The FinTech revolution in India: Innovation, inclusion and regulation*. Bank for International Settlements. https://www.bis.org/review/r230315d.htm
38. Jain, M., Khurana, A., & Kumar, A. (2024, July 11). *Fintech laws and regulations: India 2024–2025.* ICLG. https://iclg.com/practice-areas/fintech-laws-and-regulations/india
39. Khurana, A., Jain, M., & Kumar, A. (2023, July 10). *Fintech laws and regulations 2023: India.* ICLG. https://iclg.com/practice-areas/fintech-laws-and-regulations/india
40. KPMG International. (2025, March). *Pulse of Fintech H2 2024: Global analysis of funding in fintech.* https://assets.kpmg.com/content/dam/kpmg/de/pdf/Themen/2025/03/kpmg-pulse-of-fintech-h2-24-en.pdf
41. KPMG. (2019). *Insurtech: Infrastructure for new insurance*. https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2019/07/insurance-technology.pdf
42. KPMG. (2022). *Developing regulation to support safe and responsible AI adoption.* https://kpmg.com/xx/en/our-insights/regulatory-insights/developing-regulation-to-support-safe-and-responsible-ai-adoption.html
43. KPMG. (2023, May 12). *Top fintech trends for H2 '23.* https://kpmg.com/xx/en/home/insights/2023/07/top-fintech-trends-in-h1-2023.html
44. KPMG. (2025, February). *Pulse of Fintech H2 '24 – Press release.* https://kpmg.com/cy/en/home/media/press-releases/2025/02/kpmg-pulse-of-fintech-h2-24.html
45. Lalchand, S., Srinivas, V., Maggiore, B., & Henderson, J. (2024, May 29). *Generative AI is expected to magnify the risk of deepfakes and other fraud in banking.* Deloitte Insights. https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html
46. Latham & Watkins. (2023, December). *India's Digital Personal Data Protection Act 2023 vs. the GDPR: A comparison.*

https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf

47. Leitner, G., Singh, J., van der Kraaij, A., & Zsámboki, B. (2024, May). *The rise of artificial intelligence: Benefits and risks for financial stability* (Special article, *Financial Stability Review*). European Central Bank. https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html
48. Leslie, D., et al. (2023). *AI ethics and governance in practice.* The Alan Turing Institute. https://www.turing.ac.uk/sites/default/files/2023-12/aieg-ati-ai-ethics-an-intro_1.pdf
49. Marous, J. (2024, July). *State of AI in banking* (Digital Banking Report). Digital Banking Report / OpenText. https://www.opentext.com/en/media/report/state-of-ai-in-banking-digital-banking-report-en.pdf
50. McKinsey & Company. (2023, April 27). *Tackling bias in artificial intelligence (and in humans).* https://www.mckinsey.com
51. Ministry of Electronics and Information Technology (MeitY). (2024, February 15). *AI & Emerging Technologies Group*. https://meity.gov.in
52. Ministry of Electronics and Information Technology. (2024). *National strategy on blockchain.* https://www.meity.gov.in
53. Mohanty, A., & Sahu, S. (2024, February 22). *India's AI strategy: Balancing risk and opportunity.* Carnegie Endowment for International Peace. https://carnegieendowment.org/posts/2024/02/indias-ai-strategy-balancing-risk-and-opportunity
54. Mordor Intelligence. (2024). *India fintech market – Size, share, COVID-19 impact & forecasts (2025-2030).* https://www.mordorintelligence.com/industry-reports/india-fintech-market
55. Mordor Intelligence. (2024). *AI in fintech market insights*. https://www.mordorintelligence.com/industry-reports/ai-in-fintech-market
56. Mueller, J. (2020). *RegTech: Opportunities for more efficient and effective regulatory supervision and compliance.* Milken Institute. https://milkeninstitute.org/content-hub/research-and-reports/reports/regtech-opportunities-more-efficient-and-effective-regulatory-supervision-and-compliance
57. NITI Aayog. (2018). *National strategy for artificial intelligence*. Government of India. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

58. NITI Aayog. (2021). *Responsible AI for all: Part 2*. Government of India. https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf
59. Ostmann, F., & Dorobantu, C. (2021). *AI in financial services.* The Alan Turing Institute & Oxford Internet Institute. https://www.turing.ac.uk/sites/default/files/2021-06/ati_ai_in_financial_services_lores.pdf
60. Pandev, A. (2024). *Fintech laws and regulations 2024 – USA.* Global Legal Insights. https://www.globallegalinsights.com/practice-areas/fintech-laws-and-regulations/usa/
61. Press Information Bureau. (2024, December 1). *UPI: Revolutionizing digital payments in India.* Government of India. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2079544
62. Prime Minister of India. (2024, March 18). *IndiaAI Mission.* https://www.pmindia.gov.in/en/news_updates/indiaai-mission/
63. PwC. (2022). *Exploring the impact of fintech: Asset & wealth-management insights.* PricewaterhouseCoopers. https://www.pwc.com
64. PwC. (2023). *Digital Personal Data Protection Act 2023: Insights for fintech companies.* PricewaterhouseCoopers India. https://www.pwc.in/consulting/risk-consulting/the-digital-personal-data-protection-act-2023.html
65. PwC. (2024, July). *FinTech – Powering India's USD 5 trillion economy by fostering innovations, enabling inclusion, and building a sustainable future.* https://www.pwc.in/assets/pdfs/industries/powering-indias-usd-5-trillion-economy-by-fostering-innovations.pdf
66. PwC. (2024). *The FinTech route to greater financial inclusion in India*. https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/point-of-view/the-fintech-route-to-greater-financial-inclusion-in-india.pdf
67. Research and Markets. (2023, September 14). *AI in FinTech Global Market Report 2023: North America leads AI in FinTech market, driven by fraud-detection needs and innovation.* GlobeNewswire. https://www.globenewswire.com/en/news-release/2023/09/14/2743101/28124/en/
68. Research and Markets. (2025, April 1). *Digital payments in Europe 2025: Regional trends, adoption and forecasts to 2028 (press release).* GlobeNewswire. https://www.globenewswire.com/news-release/2025/04/01/3053609/
69. Reserve Bank of India. (2024). *Fintech and artificial-intelligence publications compendium 2024*. https://www.rbi.org.in

70. Reserve Bank of India. (2024). *National strategy for financial inclusion (2024 – 2029).* https://www.rbi.org.in/commonman/Upload/English/Content/PDFs/English_16042021.pdf
71. Rusu, J. (2024, October 17). *Ten years of FCA innovation: Impact and opportunity* [Speech]. Financial Conduct Authority. https://www.fca.org.uk/news/speeches/ten-years-fca-innovation-impact-and-opportunity
72. Scott, A. P. (2020, April 28). *Fintech: Overview of financial regulators and recent policy approaches* (CRS Report R46333). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R46333
73. Shabsigh, G., & Boukherouaa, E. B. (2023, August 22). *Generative artificial intelligence in finance: Risk considerations. International Monetary Fund (IMF).* Retrieved from https://www.imf.org/en/Publications/fintech-notes/Issues/2023/08/18/Generative-Artificial-Intelligence-in-Finance-Risk-Considerations-537570
74. Stanford Institute for Human-Centered Artificial Intelligence. (2020). *Artificial intelligence definitions.* https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf
75. Stellar Market Research. (2024, January). *US digital payment market: Industry analysis and forecast (2024–2030).* https://www.stellarmr.com/report/US-Digital-Payment-Market/1575
76. The Alan Turing Institute. (2023). *AI in financial services: 2023 update*. https://www.turing.ac.uk
77. The Clearing House. (2025, January 8). *Skyrocketing RTP® network growth sets stage for 2025* [Press release]. https://www.theclearinghouse.org/payment-systems/Articles/2025/01/RTP_2024_Year_Records_01-08-2025
78. The Payments Association. (2024). *Fintech: The history and future of financial technology.* https://www.thepaymentsassociation.org
79. The White House Office of Science and Technology Policy. (2022, October 4). *Blueprint for an AI Bill of Rights: A vision for protecting our civil rights in the algorithmic age.* https://bidenwhitehouse.archives.gov/ostp/news-updates/2022/10/04/blueprint-for-an-ai-bill-of-rightsa-vision-for-protecting-our-civil-rights-in-the-algorithmic-age/
80. Toms, S., Simon, D. A., & Kamyar, J. A. (2023, December 12). *How regulators worldwide are addressing the adoption of AI in financial services.* Skadden, Arps, Slate, Meagher & Flom LLP.

https://www.skadden.com/insights/publications/2023/12/how-regulators-worldwide-are-addressing-the-adoption-of-ai-in-financial-services

81. World Bank. (2021). *Fintech and the future of finance.* World Bank Group. https://documents1.worldbank.org/curated/en/099450005162250110/pdf/P17300600228b70070914b0b5edf26e2f9f.pdf
82. World Economic Forum. (2024, January 18). *The future of global fintech: Towards resilient and inclusive growth.* https://www.weforum.org/publications/the-future-of-global-fintech-towards-resilient-and-inclusive-growth/

LEGISLATION & REGULATORY INSTRUMENTS

1. Consumer Financial Protection Bureau. (2022, May 26). *Consumer Financial Protection Circular 2022-03: Adverse-action notification requirements in connection with credit decisions based on complex algorithms.* https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/
2. European Data Protection Board. (2022). *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* – Version 2.1. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version-21_en
3. European Union. (2024). Regulation (EU) 2024/1689 on harmonised rules for artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union.* (OJ L, forthcoming pagination) https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
4. European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). *Official Journal of the European Union,* L 119, 1-88. https://gdpr-info.eu/
5. HM Treasury. (2023, December 18). *The Financial Services and Markets Act 2023* (Digital Securities Sandbox) Regulations 2023: Explanatory Memorandum. https://www.legislation.gov.uk/uksi/2023/1398/pdfs/uksiem_20231398_en_001.pdf
6. India Code. (2000). *The Information Technology Act, 2000* (Act No. 21 of 2000). https://www.indiacode.nic.in
7. Office of Management and Budget. (2024, March 28). M-24-10: Advancing governance, innovation, and risk management for agency use of artificial intelligence. *Executive Office of the President*. https://www.whitehouse.gov/wp-

content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf

8. White House Office of Science and Technology Policy. (2022). *Blueprint for an AI Bill of Rights*. https://www.whitehouse.gov/ostp/ai-bill-of-rights
9. Reserve Bank of India. (2024, May). *Key guidelines for fintech and AI in India* (RBI Bulletin). https://www.rbi.org.in
10. Reserve Bank of India. (2023, August 30). *Regulatory sandbox framework*. https://www.rbi.org.in
11. Reserve Bank of India. (2023). *Payment and settlement systems in India – 2023*. https://www.rbi.org.in
12. Reserve Bank of India. (2024, June). *Regulatory sandbox framework: 2024 update*. https://www.rbi.org.in
13. Reserve Bank of India. (n.d.). Latest notifications: Fintech & AI. https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=1888
14. United Nations Commission on International Trade Law. (2022). UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services. https://uncitral.un.org/en/mlit
15. California Legislature. (2018). *California Consumer Privacy Act of 2018* (Cal. Civ. Code 1798.100–1798.199, West 2024). https://leginfo.legislature.ca.gov
16. Government of India. (2019). *Personal Data Protection Bill, 2019* (Parliamentary Bill No. 373 of 2019). Lok Sabha Secretariat. https://prsindia.org/billtrack/the-personal-data-protection-bill-2019
17. United States Congress. (1974). *Equal Credit Opportunity Act* (15 U.S.C. 1691–1691f). https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter41/subchapter4
18. United States Congress. (1970). *Fair Credit Reporting Act* (15 U.S.C. 1681 et seq.). https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter41/subchapter3
19. United Kingdom Parliament. (2010). *Equality Act 2010* (2010 c. 15). UK National Archives. https://www.legislation.gov.uk/ukpga/2010/15
20. United States Congress. (2022). *Algorithmic Accountability Act of 2022* (S. 3572/H.R. 6580, 117th Cong.). https://www.congress.gov/bill/117th-congress/senate-bill/3572
21. Organisation for Economic Co-operation and Development. (2019). *OECD Recommendation on Artificial Intelligence* (OECD/LEGAL/0449). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

22. European Commission High-Level Expert Group on Artificial Intelligence. (2019). Ethics Guidelines for Trustworthy AI. *Publications Office of the EU.* https://ec.europa.eu/futurium/en/ai-alliance-consultation
23. Financial Action Task Force. (2021). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation *(The FATF Recommendations)* (updated March 2022). https://www.fatf-gafi.org/recommendations.html
24. Monetary Authority of Singapore. (2018). Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of AI and Data Analytics in the Financial Sector. https://www.mas.gov.sg
25. European Parliament & Council. (2015). *Directive (EU) 2015/2366 on Payment Services in the Internal Market (PSD2)* (OJ L 337, 35-127). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366
26. Government of India. (2023). *The Digital Personal Data Protection Act, 2023* (Act No. 22 of 2023). https://egazette.nic.in
27. Government of India. (2007). *The Payment and Settlement Systems Act, 2007* (Act No. 51 of 2007). https://legislative.gov.in
28. Government of India. (2019). *The Consumer Protection Act, 2019* (Act No. 35 of 2019). https://consumeraffairs.nic.in
29. Government of India. (1872). *The Indian Contract Act, 1872* (Act No. 9 of 1872). https://indiacode.nic.in
30. Ministry of Electronics & IT. (2011). *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*. https://www.meity.gov.in
31. Ministry of Electronics & IT. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. https://www.meity.gov.in
32. Parliament of India. (1934). *The Reserve Bank of India Act, 1934* (as amended 2024). https://rbi.org.in
33. Parliament of India. (1999). *The Foreign Exchange Management Act, 1999* (Act No. 42 of 1999). https://dea.gov.in
34. European Parliament & Council. (2015). *Directive (EU) 2015/2366 on payment services in the internal market* (PSD2). OJ L 337, 23-12-2015.
35. European Parliament & Council. (2023). *Regulation (EU) 2023/1114 on markets in crypto-assets* (MiCA). OJ L 150, 09-06-2023.
36. European Parliament & Council. (2022). *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector* (DORA). OJ L 333, 27-12-2022.

37. U. S. Congress. (1970). *Bank Secrecy Act* (31 U.S.C. § 5311 et seq.). https://uscode.house.gov
38. U. S. Congress. (1999). *Gramm–Leach–Bliley Act* (Public Law 106-102). https://www.congress.gov
39. U. S. Congress. (1970). *Fair Credit Reporting Act* (15 U.S.C. § 1681 et seq.). https://uscode.house.gov
40. U. S. Congress. (1974). *Equal Credit Opportunity Act* (15 U.S.C. § 1691 et seq.). https://uscode.house.gov
41. U. S. Congress. (1968). *Truth in Lending Act* (15 U.S.C. § 1601 et seq.). https://uscode.house.gov
42. U. S. Congress. (1978). *Electronic Fund Transfer Act* (15 U.S.C. § 1693 et seq.). https://uscode.house.gov
43. California Legislature. (2018). *California Consumer Privacy Act* (CCPA, Cal. Civ. Code § 1798.100 et seq.).
44. California Legislature. (2020). *California Privacy Rights Act* (CPRA).
45. New York State Department of Financial Services. (2015). 23 NYCRR Part 200—Virtual Currency Businesses ("BitLicense").
46. Connecticut General Assembly. (2022). *Connecticut Data Privacy Act* (P.A. 22-15).
47. Utah Legislature. (2022). *Utah Consumer Privacy Act* (Utah Code §§ 13-61-101 ff.).

WEB-ONLY SOURCES

1. A&O Shearman. (2024, May 10).*AI under financial regulations in the U.S., EU, and U.K.* https://www.aoshearman.com
2. Abrams, Z. (2024, April).*Addressing equity and ethics in artificial intelligence. APA Monitor on Psychology.* American Psychological Association. https://www.apa.org/monitor/2024/04/addressing-equity-ethics-artificial-intelligence
3. Aguilar, T. (2023, September 19). *Artificial intelligence and patent law: Navigating the landscape in 2023.* Chambers and Partners. https://chambers.com/articles/artificial-intelligence-and-patent-law-navigating-the-landscape-in-2023
4. Ahuja, I., & Kapadia, S. (2023, August 22). *Digital Personal Data Protection Act, 2023: A brief analysis.* Bar & Bench. https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis
5. American Bankers Association. (2024, January 9). *The impact of AI-generated synthetic fraud on finance.* American Bankers Association – Banking Journal.

https://bankingjournal.aba.com/2024/01/the-impact-of-ai-generated-synthetic-fraud-on-finance/

6. American Bankers Association. (2024, March 18). *AI compliance and regulation: What financial institutions need to know.* American Bankers Association – Banking Journal. https://bankingjournal.aba.com/2024/03/ai-compliance-and-regulation-what-financial-institutions-need-to-know/
7. Balal, A. (2021, June 22). *What is decentralization in blockchain?* Blockchain Council. https://www.blockchain-council.org/blockchain/what-is-decentralization-in-blockchain/
8. Barat, D. (2024, January 9). *India's initiatives on regulating artificial intelligence: Balancing promotion with protection.* Mondaq. https://www.mondaq.com/india/new-technology/1410758/indias-initiatives-on-regulating-artificial-intelligence-balancing-promotion-with-protection
9. Beganski, A. D. (2023, July 17). *Over 200 Ethscriptions nabbed in smart-contract exploit.* Decrypt. https://decrypt.co/148824/ethscriptions-exploit-smart-contract-over-200-stolen
10. Bhardwaj, C. (2022, June 21). *What are smart contracts and are they legal in India?* India Briefing. https://www.india-briefing.com/news/what-are-smart-contracts-and-are-they-legal-in-india-25343.html
11. Bhavsar, M. (2023, March 23). *Fintech with AI: The future of the financial industry in 2023.* Metizsoft Solutions Blog. https://www.metizsoft.com/blog/ai-fintech-industry-in-2023
12. Brighterion AI. (n.d.). *Explainable AI: From black box to transparency.* Mastercard News & Insights. https://b2b.mastercard.com/news-and-insights/blog/explainable-ai-from-black-box-to-transparency/
13. Brookings Institution. (2022, August 16). *Patents and AI inventions: Recent court rulings and broader policy questions*. https://www.brookings.edu/articles/patents-and-ai-inventions-recent-court-rulings-and-broader-policy-questions/
14. Burman, A. (2023, October 3). *Understanding India's new data-protection law.* Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law
15. Caltech Science Exchange. (2024). *What is artificial intelligence?* California Institute of Technology. https://scienceexchange.caltech.edu/topics/artificial-intelligence-research/artificial-intelligence-definition
16. Carnegie Endowment for International Peace. (2023). *Understanding India's New Data Protection Law.* Retrieved from

https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en

17. Chaudhary, P. (2024, August 27). *Fintech as a catalyst for growth: Lessons from India.* ACCA Global. https://www.accaglobal.com/gb/en/professional-insights/technology/fintech-india.html
18. Chu, L. D. (2023, September 8). *The impact of AI on regulatory compliance in fintech.* SmartDev Blog. https://smartdev.com/regulatory-compliance-in-fintech/
19. Clifford Chance. (2023, October 26). *Global fintech update 26-10-23.* Talking Tech Blog. https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2023/10/global-fintch-update-26-10-23.html
20. Cooley LLP. (2023, April 27). *CFPB, federal agencies warn of obligations to avoid algorithmic discrimination.* https://www.cooley.com/news/insight/2023/2023-04-27-cfpb-federal-agencies-warn-of-obligations-to-avoid-algorithmic-discrimination
21. Corrida Legal. (2023, October 9). *Fintech laws in India: Understanding the regulatory regime.* Mondaq. https://www.mondaq.com/india/fin-tech/1369804/fintech-laws-in-india-understanding-the-regulatory-regime
22. Danielsson, J., & Uthemann, A. (2024, January 22). *How AI can undermine financial stability.* VoxEU (Centre for Economic Policy Research). https://cepr.org/voxeu/columns/how-ai-can-undermine-financial-stability
23. Dar, A., Suri, S., Viswanath, N., Aditya, G., & Singh, K. (2022, November 4). *India: An introduction to fintech legal.* Chambers and Partners. https://chambers.com/content/item/4784
24. Dharmaraj, S. (2024, May 11). *AI advancing the fintech ecosystem in India.* OpenGov Asia. https://opengovasia.com/2024/05/11/ai-advancing-the-fintech-ecosystem-in-india/
25. Engler, A. (2023, April 25). *The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment*. Brookings Institution. https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/#anchor8
26. Ferreira, V. (2019, May 7). *Artificial intelligence can now pick stocks and build portfolios.* Financial Post. https://financialpost.com
27. FF News. (2025, February 28). *Global fintech investment falls to seven-year low of $95.6 billion in 2024, but uptick in Q4'24 is a sign of cautious optimism, says KPMG's Pulse of Fintech H2'24*. https://ffnews.com/newsarticle/fintech/global-fintech-investment-falls-to-seven-year-low-of-95-6-billion-in-2024-but-uptick-in-q424-is-a-sign-of-cautious-optimism-says-kpmgs-pulse-of-fintech-h224/

28. Financial Crime Academy. (2024). *Advancing digital finance*. https://financialcrimeacademy.org/advancing-digital-finance/
29. Financial Crime Academy. (n.d.). *Cracking down on financial crime: The role of AI technologies in AML*. https://financialcrimeacademy.org
30. FinTech Futures. (2025, January 15). *India fintech market report 2024–2029, with focus on major startups …* https://www.fintechfutures.com/press-releases/india-fintech-market-report-2024-2029-with-focus-on-major-startups-in-the-fintech-market-including-stable-money-indmoney-bharatpe-and-velocity
31. Foley & Lardner LLP. (2023, September 18). *The most critical factors for AI legal compliance: Transparency and explainability*. https://www.foley.com/insights/publications/2023/09/critical-factors-ai-legal-compliance-transparency/
32. Generis Global. (2024, March 7). *Cross-border data flows and AI: Navigating international laws.* https://generisonline.com/cross-border-data-flows-and-ai-navigating-international-laws/
33. Heidt, A. (2024, September 4). *Intellectual property and data privacy: The hidden risks of AI.* Nature News. https://doi.org/10.1038/d41586-024-02838-z
34. Henderson, A., Scott, G., Moille, C., Dixon-Ward, M., & Popescu, A. (2024, August 9). *EU AI Act: Key points for financial-services businesses*. Goodwin Law. https://www.goodwinlaw.com/en/insights/publications/2024/08/alerts-practices-pif-key-points-for-financial-services-businesses
35. High, M. (2020, June 1). *Data-driven fintech and the IoT evolution*. FinTech Magazine. Retrieved from https://fintechmagazine.com/venture-capital/data-driven-fintech-and-iot-evolution
36. Huspen, M. (2025, April 28). *AI investments, Binance deal spur fintech funding in Q1*. American Banker. https://www.americanbanker.com/news/ai-investments-binance-deal-spur-fintech-funding-in-q1
37. Ikigai Law. (2023, August 16). *Summary of India's Digital Personal Data Protection Act, 2023.* https://www.ikigailaw.com/article/9/summary-of-indias-digital-personal-data-protection-act-2023
38. Inscribe. (2022). *Synthetic fraud detection — An in-depth guide.* https://www.inscribe.ai/fraud-detection/what-is-synthetic-fraud-detection
39. Insider Intelligence. (2024). *The security and privacy issues that come with the Internet of Things.* https://www.insiderintelligence.com/insights/iot-security-privacy/

40. JDSupra. (2024). *AI-driven phishing: An emerging threat*. https://www.jdsupra.com/legalnews/ai-driven-phishing-an-emerging-threat-7801832/
41. Kakoti, A. R., & Singh, G. (2024, May 29). *The EU AI Act: Implications and lessons for India.* Hindustan Times. https://www.hindustantimes.com/ht-insight/international-affairs/the-eu-ai-act-implications-and-lessons-for-india-101716968919076.html
42. Kalra, L. (2023, August 23). *Decoding the Digital Personal Data Protection Act, 2023.* EY Insights. https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023
43. Kenton, W. (2023, June 12). *What is a black-box model? Definition, uses, and examples.* Investopedia. https://www.investopedia.com/terms/b/blackbox.asp
44. Klein, A., & Lee, S. (2024, July 5). *AI and financial stability: Mitigating risks, harnessing benefits.* Brookings Institution. https://www.brookings.edu/articles/ai-and-financial-stability-mitigating-risks-harnessing-benefits/
45. Krishna, H. (2023, December 15). *Regulation and risk mitigation in the age of AI | India. Chambers.* Retrieved from https://chambers.com/legal-trends/ai-regulations-in-india
46. Krishnamurthy, K., & Khandelwal, N. (2024, August 27). *AI regulation in India vs the EU: Balancing innovation and risk.* Mondaq. https://www.mondaq.com/india/new-technology/1509322/
47. Kumar, N. (2025, May 19). *FinTech statistics (2025) – Market share & growth*. DemandSage. https://www.demandsage.com/fintech-statistics/
48. Kunhambu, A. (2021, June 7). *Artificial intelligence and the shift in liability*. iPleaders Blog. https://blog.ipleaders.in/artificial-intelligence-shift-liability/
49. Lehmann, J. (2023, August 14). *Research shows extensive use of AI contains data breaches faster and saves significant costs.* IBM Blog. https://www.ibm.com/blog/research-shows-extensive-use-of-ai-contains-data-breaches-faster-and-saves-significant-costs/
50. Levi, S. D., & Lipton, A. B. (2018, May 26). *An introduction to smart contracts and their potential and inherent limitations.* Harvard Law School Forum on Corporate Governance. https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/
51. Levitt, K. (2024, January 11). *AI takes center stage: Survey reveals financial industry's top trends for 2024.* NVIDIA Blog. https://blogs.nvidia.com/blog/ai-in-financial-services-survey-2024/

52. Lucinity. (2024, March 21). *How AI and ML transform KYC compliance.* https://lucinity.com/blog/how-ai-and-ml-transform-kyc-compliance
53. Mahawar, S. (2022, July 5). *Smart contracts and their enforceability in India.* iPleaders Blog. https://blog.ipleaders.in/smart-contracts-and-their-enforceability-in-india/
54. Mallett, E. (2023, June 9). *Financial services and AI: Recent regulatory developments.* Loeb & Loeb LLP. https://www.loeb.com/en/insights/publications/2023/06/financial-services-and-ai-regulatory-developments
55. Mehra, S. (2021, August 21). *Here's how SEBI uses AI for market regulation.* IndiaAI. https://indiaai.gov.in/article/here-s-how-sebi-uses-ai-for-market-regulation
56. Meola, A. (2023, March 8). *A look at examples of IoT devices and their business applications in 2023.* Insider Intelligence. https://www.insiderintelligence.com/insights/internet-of-things-devices-examples/
57. Mishra, P. K. (2024, February 27). *AI and the legal landscape: Embracing innovation, addressing challenges.* LiveLaw. https://www.livelaw.in/lawschool/articles/law-and-ai-ai-powered-tools-general-data-protection-regulation-250673
58. Mondaq. (2023, November 9). *The Digital Personal Data Protection Act, 2023: A deep dive.* https://www.mondaq.com
59. Moss, J. (2022, June 7). *A new approach to regulating credit-scoring AI.* The Regulatory Review. https://www.theregreview.org/2022/06/07/moss-new-approach-to-regulating-credit-scoring-ai/
60. Nair, D., Agarwal, D., Manoharan, G., Mukherjee, M., Roy Chowdhury, P., et al. (2024, September 23). *RBI amends regulatory sandbox scheme and integrates the new data-privacy law.* Mondaq. https://www.mondaq.com/india/fin-tech/1520480/
61. Natarajan, S. (2024, January 4). *Innovations in banking: RBI's vision on artificial intelligence & generative AI.* TaxGuru. https://taxguru.in/rbi/innovations-banking-rbis-vision-artificial-intelligence-ai-generative-ai.html
62. Neely, M. C. (2021, March 31). *The fintech revolution in banking*. Federal Reserve Bank of St. Louis. https://www.stlouisfed.org/~/media/project/frbstl/stlouisfed/financial-technology/2021/fintech-revolution-in-banking.pdf
63. Notani, S., Jha, P., Ghei, N., & Kushe, S. (2024, March 21). *Navigating AI regulation in India: Unpacking the MeitY advisory in a global context.* Mondaq. https://www.mondaq.com/india/new-technology/1442894/

64. Oliver Wyman. (2023). *AI in Finance Global Challenge 2023*. https://www.oliverwyman.com/our-expertise/events/2023/jun/ai-in-finance-global-challenge-2023.html
65. Ray, A. (2022, October 18). *The Reserve Bank of India and the regulation of fintech*. Mondaq. https://www.mondaq.com/india/fin-tech/1241220/the-reserve-bank-of-india-and-the-regulation-of-fintech
66. Saraswat, D. (2023, January 18). *Laws governing AI in India: Everything you should know.* Legal Service India. https://www.legalserviceindia.com/legal/article-13111-laws-governing-ai-in-india-everything-you-should-know.html
67. Scanlon, L. (2020, May 11). *Liability for AI in financial services*. Pinsent Masons Out-Law. https://www.pinsentmasons.com/out-law/analysis/liability-for-ai-in-financial-services
68. Shahid, T. (2023, June 4). *Smart contracts and the Indian Contract Act: Compatibility and implications.* The Amikus Qriae. https://theamikusqriae.com/smart-contracts-and-the-indian-contract-act-compatibility-and-implications/
69. Shaikh, A. (2024, June 10). *Challenges of IoT in fintech.* Talk FinTech. https://talkfintech.com/featured/challenges-of-iot-in-fintech/
70. Sharma, N. (2024, November 7). *IoT in fintech: How it's transforming the BFSI sector.* Appinventiv Blog. https://appinventiv.com/blog/iot-in-fintech/
71. Shea, S. (2024, April 8). *Generative AI is making phishing attacks more dangerous.* TechTarget – SearchSecurity. https://www.techtarget.com/searchsecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous
72. Sidley Austin LLP. (2024, December 4). *Artificial intelligence in financial markets: Systemic-risk and market-abuse concerns.* https://www.sidley.com/en/insights/newsupdates/2024/12/artificial-intelligence-in-financial-markets-systemic-risk-and-market-abuse-concerns
73. Singh, B. P. (2024, January 29). Budget 2024: *Navigating the future of India's fintech sector.* Forbes India. https://www.forbesindia.com/blog/economy-policy/budget-2024-navigating-the-future-of-indias-fintech-sector-329979.html
74. Smith, J., Bowden, M., & Stoeckler, R. (2024, March 15). *How AI may be used in fintech fraud — and fraud detection.* Law360. https://www.law360.com/articles/1813323
75. Song, N. (2021, April 15). *Why fintech companies should have a Bank Secrecy Act compliance program.* Moss Adams Insights.

https://www.mossadams.com/articles/2021/04/fintech-companies-and-the-bank-secrecy-act

76. Spichiger, R. (2024, December 18). *Highlights from the 2024 EY European Financial Services AI survey.* EY. https://www.ey.com/en_ch/insights/ai/ey-european-financial-services-ai-survey
77. Srivastava, H. (2024, April 22). *Regulatory frameworks for fintech innovation in India: Challenges & opportunities.* TaxGuru. https://taxguru.in/corporate-law/regulatory-frameworks-fintech-innovation-india-challenges-opportunities.html
78. Stackhouse, J. L. (2019, April 28). Fintech: *Understanding AI use in financial services.* Federal Reserve Bank of St. Louis, On the Economy blog. https://www.stlouisfed.org/on-the-economy/2019/april/fintech-understanding-ai-financial-services
79. The Indian Express. (2021, April 1). *RBI orders MobiKwik to probe alleged data leak.* https://indianexpress.com/article/technology/tech-news-technology/rbi-orders-mobikwik-to-probe-alleged-data-leak-7254607/
80. Treacy, S., & Qemali, E. (2024, January 31). *AI in financial services and financial-stability concerns.* Linklaters Tech Insights. https://techinsights.linklaters.com/post/102iyk4/ai-in-financial-services-and-financial-stability-concerns
81. Turner Lee, N., & Malamud, J. (2022, December 19). *Opportunities and blind spots in the White House's blueprint for an AI Bill of Rights*. Brookings Institution. https://www.brookings.edu/articles/opportunities-and-blind-spots-in-the-white-houses-blueprint-for-an-ai-bill-of-rights/
82. Venkatraman, K. R. (2024, February 20). *From black box to open playbook: Bringing transparency to AI in banking.* International Banker. https://internationalbanker.com/technology/from-black-box-to-open-playbook-bringing-transparency-to-ai-in-banking/
83. Verma, R. (2024, February 22). *Global perspectives on AI accountability: A comparative analysis and India's regulatory landscape*. Grant Thornton India. https://www.grantthornton.in/insights/blogs/global-perspectives-on-ai-accountability-a-comparative-analysis-and-indias-regulatory-landscape/
84. Viswanath, N., Muthanna, R., & Jain, P. (2023, May). *Comparative analysis of the key data regulations of India, EU, and the US.* IndusLaw. https://induslaw.com/publications/pdf/alerts-2023/Infolex-Article-Comparative-analysis-of-the-key-data-regulations.pdf

85. Walden, S. (2020, August 4). *What is fintech?* Forbes Advisor. https://www.forbes.com/advisor/banking/what-is-fintech/
86. Walia, S. (2023, August 25). *The Payment and Settlement Systems Act, 2007 and RBI's regulatory powers.* Ahlawat & Associates. https://www.ahlawatassociates.com/blog/the-payment-and-settlement-systems-act-2007-and-rbis-regulatory-powers
87. Wheeler, T. (2023, August 21). The three challenges of AI regulation. *Brookings Institution.* https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/
88. World Finance Council. (2019). *Exploring fintech applications: Examples and impact on financial services.* https://worldfinancecouncil.org/articles/exploring-fintech-applications-examples-and-impact-on-financial-services/
89. Yashi. (2023, May 9). Artificial intelligence and laws in India. *Legal Service India*. https://www.legalserviceindia.com/legal/article-8171-artificial-intelligence-and-laws-in-india.html
90. Yurcan, B. (2022, June 28). How banks can shed light on the "black box" of AI decision-making. *The Financial Brand.* https://thefinancialbrand.com/news/artificial-intelligence-banking/how-banks-can-shed-light-on-the-black-box-of-ai-decision-making-147960/

THESIS

1. Naik, V. (2016). The evolution of digital payments: The past, present and future of digital payments (Master's thesis, Massachusetts Institute of Technology). *DSpace@MIT*. https://dspace.mit.edu/handle/1721.1/115037

LIST OF PUBLICATIONS

Name: Bharanitharan K

ORCiD: 0009-0005-8030-4294

1. Bharanitharan K, Gagandeep Kaur. (2024). The Double-Edged Sword: Legal Implications of AI Errors and Blockchain in Finance. *European Economic Letters (EEL)*, *14*(2), 2838–2846. https://doi.org/10.52783/eel.v14i2.1637

2. Bharanitharan, K., & Kaur, G. (2024, August 22). *Navigating the legal landscape: Addressing AI-driven innovations and challenges in Indian FinTech*. Journal of Informatics Education and Research, 4(3), Article 1361. https://doi.org/10.52783/jier.v4i3.1361

Bharanitharan K

Analyzing Legal Frameworks for Artificial Intelligence in Fintech: A Comparative Study Across India, European Union a...

Quick Submit

Quick Submit

UPES: University of Tomorrow

Document Details

Submission ID
trn:oid:::1:3349996627

Submission Date
Sep 24, 2025, 4:14 PM GMT+5:30

Download Date
Sep 24, 2025, 4:35 PM GMT+5:30

File Name
Full_Thesis_13-51-31-770_for_plag_run.pdf

File Size
2.6 MB

355 Pages

122,791 Words

727,312 Characters

1% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Small Matches (less than 14 words)

Match Groups

60 Not Cited or Quoted 1%
Matches with neither in-text citation nor quotation marks

9 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

1% Internet sources
1% Publications
1% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.