LEGAL CHALLENGES OF THE DIGITALIZATION OF BANKING: REGULATORY GAPS, LIABILITY, AND THE RECONFIGURATION OF FINANCIAL LAW

Abdirasulov Abdilaziz
Master of Laws (LLM) Tashkent State University of Law, Lecturer of the Department of Private International Law
Phone: +998 99 093 50 00
E-mail: abdirasulovabdulaziz@tsul.uz
ORCID iD: 0009-0004-8402-8699

Abstract: *This article examines the principal legal challenges arising from the digitalization of banking from a comparative and doctrinal perspective. It analyses how four jurisdictions — the United States, the European Union, Singapore, and Uzbekistan — address the regulatory perimeter problem, the allocation of liability for cyber incidents and algorithmic decisions, the supervisory treatment of cloud and other critical third-party providers, and the protection of consumers in instant and cross-border digital transactions. The findings demonstrate that, although substantive obligations on cybersecurity, customer authentication, and information disclosure converge across the surveyed regimes, the institutional and doctrinal architecture for addressing emerging risks diverges significantly. Uzbekistan, having reinforced its framework through Law No. ZRU-578 of 2019, Presidential Decree No. PP-381 of November 2023, and Central Bank Regulation No. 3513 of May 2024, has achieved meaningful substantive alignment with international standards. However, the regime lacks codified rules on the oversight of critical third-party providers comparable to the EU's Digital Operational Resilience Act, a framework for the legal accountability of automated decision-making analogous to the EU Artificial Intelligence Act, and a specialised dispute-resolution mechanism for digital-banking disputes. The article argues that the next reform cycle should consolidate the legal infrastructure for operational resilience, algorithmic accountability, and consumer redress.*

Keywords: *banking law; bank digitalization; financial regulation; cybersecurity; operational resilience; algorithmic accountability; third-party providers; comparative law; Uzbekistan*

1. Introduction

1.1. Relevance of the Topic

The digitalization of banking has produced a structural mismatch between the technological reality of contemporary financial services and the legal frameworks designed for an analog, branch-based, and territorially bounded industry[1]. Cloud infrastructure, application programming interfaces, machine-learning models, and instant-payment rails have reshaped how value is produced, distributed, and protected, while regulatory regimes structured around licensed entities and clerical processes have struggled to keep pace. The international regulatory response has accelerated. The European Union has adopted the Digital Operational Resilience Act (DORA), applicable since January 2025[2], and the Artificial Intelligence Act, classifying credit-scoring systems as high-risk applications[3]. The United Kingdom enacted a critical-third-parties regime in 2024[4], and the United States Federal Reserve Board issued supervisory observations on banking-as-a-service arrangements in 2024[5].

In Uzbekistan, mobile banking users grew by 28% in 2023 alone, with non-cash payments now constituting 45% of all transactions[6]. The legal framework anchored in Law No. ZRU-578 of 2019[7] has been reinforced through Presidential Decree No. PP-381 of November 2023[8] and Central Bank Regulation No. 3513 of May 2024[9]. As Uzbekistan moves toward WTO accession in 2026 and projects 75% cashless payments by 2030[10], the adequacy of its legal regime to address the emerging challenges of bank digitalization — operational resilience, algorithmic accountability, third-party concentration, and digital fraud — carries significant consequences for investment, financial stability, and consumer trust.

1.2. Research Objectives

This article presents a doctrinal analysis of the legal challenges raised by bank digitalization in major comparative legal systems and a critical comparative analysis of the Uzbek system. The principal argument is that, while Uzbekistan has achieved substantive alignment with international standards on cybersecurity and authentication, the legal framework for addressing the second-generation challenges of digitalization — direct supervisory oversight of critical third-party providers, accountability for algorithmic decisions, and the legal treatment of cross-border digital services — remains underdeveloped.

2. Methods

This article employs doctrinal legal research combined with functional comparative analysis. The comparative aspect analyses four key issues: (i) the regulatory perimeter and the entity-versus-activity debate; (ii) the legal regime governing operational resilience and critical third-party providers; (iii) the legal accountability of algorithmic and automated decision-making; and (iv) the framework for liability allocation in cyber and digital-fraud incidents. Primary sources include Law No. ZRU-578[11], Presidential Decree No. PP-381[12], Central Bank Regulation No. 3513[13], the EU Digital Operational Resilience Act[14], the EU Artificial Intelligence Act[15], the EU Markets in Crypto-Assets Regulation[16], the UK Critical Third Parties regime[17], U.S. interagency guidance on third-party risk management[18], and the Uzbek Civil Code[19].

3. Results

3.1. The European Union Framework

The European Union has constructed the most comprehensive legal architecture for the digitalization of banking. DORA[20] establishes harmonized requirements for ICT risk management, incident reporting, digital operational-resilience testing, and the oversight of critical third-party providers, with direct supervisory powers conferred on European supervisory authorities. The Artificial Intelligence Act[21] classifies credit-scoring systems used in financial services as high-risk applications, imposing requirements on data governance, transparency, human oversight, and post-market monitoring. The Markets in Crypto-Assets Regulation[22] creates a parallel sector-specific regime for crypto-asset issuers and service providers, while the PSD3/PSR package agreed in 2025[23] extends liability to certain authorised push-payment frauds and codifies fraud-pattern anomaly detection. Together these instruments illustrate the EU's combined entity-based, activities-based, and provider-oriented approach to bank digitalization.

3.2. The United States Framework

The U.S. legal framework on bank digitalization is decentralized across federal banking agencies, the Consumer Financial Protection Bureau (CFPB), and state regulators. The 2023 Interagency Guidance on Third-Party Relationships, issued jointly by the Federal Reserve, FDIC, and OCC[24], consolidates expectations for the management of technology and outsourcing arrangements. Federal Reserve Board supervisory observations published in 2024 addressed banking-as-a-service arrangements

specifically[25]. The Office of the Comptroller of the Currency has issued guidance on the risk management of artificial-intelligence systems in national banks[26], while the CFPB has begun rulemaking on automated decision-making in consumer financial services. The U.S. approach is characterized by strong supervisory expectations rather than a single consolidated digital-resilience statute.

3.3. The Singapore Framework

Singapore has adopted a single-regulator approach under the Monetary Authority of Singapore (MAS), supplemented by the Cyber Security Agency and the Infocomm Media Development Authority. The MAS Technology Risk Management Guidelines[27] set out detailed expectations on cyber resilience, third-party risk management, and incident management. The MAS-IMDA Shared Responsibility Framework for Phishing Scams, effective 16 December 2024[28], allocates anti-scam duties among financial institutions and telecommunication operators on a waterfall basis. MAS has issued FEAT principles on the responsible use of artificial intelligence and data analytics in financial services[29], emphasising fairness, ethics, accountability, and transparency. Singapore's approach combines clear supervisory expectations with codified consumer-protection mechanisms.

3.4. The Uzbekistan Framework

The legal regulation of bank digitalization in Uzbekistan is structured around Law No. ZRU-578 of 1 November 2019[30], supplemented by Presidential Decree No. PP-381[31], Central Bank Regulation No. 3513 of May 2024[32], and the Law on Personal Data[33]. Regulation No. 3513, in force from August 2024[34], imposes detailed cybersecurity obligations including identification mechanisms, real-time fraud monitoring, and incident-reporting duties. Civil remedies are anchored in Article 11 of the Civil Code[35]. Supervisory authority is concentrated in the Central Bank, with the Antimonopoly Committee's Consumer Rights Protection Agency providing a parallel general forum.

Three structural features distinguish the Uzbek framework from the comparator regimes. First, no statutory regime designates critical third-party providers or subjects them to direct supervisory oversight; technology providers are addressed indirectly through outsourcing requirements imposed on banks. Second, no specific legal framework governs algorithmic decision-making in financial services; the general civil-law principles of Article 11 of the Civil Code apply. Third, no specialised dispute-resolution

body exists for digital-banking disputes; out-of-court resolution depends on internal bank-mediation procedures, the Central Bank, the Antimonopoly Committee, or general civil litigation. Presidential Decree No. PP-126 of December 2025 establishes a cashless-payment mandate effective April 2026[36], supporting the target of 75% cashless payments by 2030.

3.5. Comparative Summary

Table 1 synthesises the key comparative dimensions across the surveyed jurisdictions.

Table 1

Comparative Summary of Legal Frameworks Addressing Bank Digitalization

Criterion	USA	EU (DORA / AI Act / MiCA)	Singapore (MAS TRM / SRF)	Uzbekistan (ZRU-578 / Reg. 3513)
Operational resilience statute	Interagency guidance only	DORA (in force 2025)	MAS TRM Guidelines	Reg. 3513 (cybersecurity)
Critical third-party oversight	Indirect; via outsourcing rules	Direct designation under DORA	Indirect; via TRM expectations	Not codified
AI / algorithmic accountability	OCC and CFPB guidance	AI Act high-risk classification	MAS FEAT principles	Not codified
Crypto-asset regime	Federal–state patchwork	MiCA harmonised regime	PSA digital-token framework	Limited; CBU pilot regimes
Specialised digital-disputes body	CFPB + courts	National FOS bodies	FIDReC	No specialised body
Supervisory authority	Federal Reserve, OCC, FDIC, CFPB	National authorities + EBA / ESMA	MAS (single regulator)	Central Bank + Antimonopoly

4. Discussion

4.1. The Regulatory Perimeter and Critical Third-Party Providers

Bank digitalization has revealed the limits of the entity-based regulatory model. Cloud providers, software vendors, and FinTech distributors now perform functions critical to the safe operation of regulated banks, yet they have historically remained outside the prudential perimeter[37]. Three legislative responses can be identified. The EU's DORA establishes a designation regime for critical ICT third-party providers, subjecting them to direct oversight by lead overseers from European supervisory authorities[38]. The UK Critical Third Parties regime adopts a comparable approach[39]. The U.S. relies on supervisory expectations imposed on banks regarding their third-party relationships, supplemented by selective direct oversight of bank service providers under the Bank Service Company Act[40].

Uzbekistan's framework imposes outsourcing requirements on banks under Regulation No. 3513[41], but does not establish a designation regime for critical providers, nor does it confer direct supervisory powers over technology vendors. As cloud adoption accelerates and reliance on a small number of global providers deepens, this institutional gap exposes the financial system to concentration risks that cannot be effectively mitigated through bank-level requirements alone.

4.2. Algorithmic Accountability and the Legal Status of Automated Decisions

The deployment of machine-learning models in credit underwriting, transaction monitoring, and fraud detection raises three legal questions: the right to obtain a meaningful explanation of an automated decision and to contest it, the prohibition of unlawful discrimination through models that produce disparate effects, and the allocation of liability for harms produced by erroneous or biased automated decisions[42]. The EU AI Act addresses these issues by classifying credit-scoring systems as high-risk and imposing requirements on data governance, transparency, and human oversight[43]. The U.S. approach, although less consolidated, includes OCC guidance on model risk management and CFPB enforcement of fair-lending obligations against algorithmic disparate impact. Singapore's FEAT principles provide non-binding guidance on the responsible use of AI in financial services[44].

Uzbekistan does not yet have a sector-specific framework on automated decision-making in financial services. The Law on Personal Data[45] addresses certain aspects of automated processing, but its

application to algorithmic credit decisions remains undeveloped. As Uzbek banks adopt machine-learning models for credit and fraud purposes, the legal vacuum on contestability, explainability, and liability for algorithmic harms is likely to become more consequential.

4.3. Liability Allocation in Cyber and Digital-Fraud Incidents

The legal allocation of losses arising from cyber incidents and digital fraud has emerged as one of the most contested areas of bank digitalization. Three principles compete: the bank-mandate principle, under which a payment authorised by the customer is at the customer's risk; the strict-refund principle adopted under PSD2 Article 73, requiring providers to refund unauthorised amounts immediately[46]; and the shared-responsibility principle introduced by Singapore's SRF and partially adopted under PSD3/PSR for impersonation fraud[47]. Uzbekistan's framework imposes substantive authentication and fraud-monitoring obligations under Regulation No. 3513[48] but does not codify a specific rule on loss allocation. Disputes fall back on Article 11 of the Civil Code and general non-contractual liability rules, placing significant evidentiary burdens on the consumer.

5. Conclusion

This article has analysed the legal challenges of bank digitalization in four legal systems. A clear pattern of substantive convergence has emerged on cybersecurity, authentication, and incident reporting. However, the legal architecture for addressing the second-generation challenges of digitalization — direct oversight of critical third-party providers, accountability for algorithmic decisions, and the harmonized treatment of cross-border digital services — diverges significantly. Uzbekistan has achieved substantive alignment with international standards through Law No. ZRU-578[49], Presidential Decree No. PP-381[50], and Central Bank Regulation No. 3513[51]; the substantive obligations broadly track those imposed under DORA, the MAS TRM Guidelines, and U.S. interagency guidance.

Three structural gaps warrant attention in the next reform cycle: the absence of a designation regime for critical third-party providers analogous to DORA; the absence of a sector-specific framework on algorithmic accountability comparable to the EU AI Act; and the absence of a specialised dispute-resolution mechanism for digital-banking disputes. The principal remaining task is the construction of a legal infrastructure for operational resilience, algorithmic accountability, and consumer redress

that matches the ambition of the substantive cybersecurity framework already in place.

References:

1. Buckley R. P., Arner D. W., Zetzsche D. A., Selga E. "The Dark Side of Digital Financial Transformation: The New Risks of FinTech and the Rise of TechRisk" (2020) UNSW Law Research Paper.

2. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA), [2022] OJ L 333/1.

3. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), [2024] OJ L 1689.

4. Bank of England and Financial Conduct Authority, "Operational Resilience: Critical Third Parties to the UK Financial Sector" (Policy Statement, 2024).

5. Federal Reserve Board, "Supervisory Observations on Banking-as-a-Service Arrangements" (2024).

6. Legal500, "Digital Payments in Uzbekistan: Legal Reforms and Global Implications" (2024). https://www.legal500.com/developments/thought-leadership/digital-payments-in-uzbekistan-legal-reforms-and-global-implications/

7. Law of the Republic of Uzbekistan No. ZRU-578 "On Payments and Payment Systems" (1 November 2019). https://lex.uz/ru/docs/4575788

8. Presidential Decree of the Republic of Uzbekistan No. PP-381 of 30 November 2023.

9. Central Bank of the Republic of Uzbekistan, Regulation No. 3513 of 21 May 2024.

10. Interfax, "Uzbekistan Intends to Increase Share of Cashless Payments to 75% by 2030" (December 2025).

11. Law No. ZRU-578 (1 November 2019).

12. Presidential Decree No. PP-381 of 30 November 2023.

13. Central Bank Regulation No. 3513 of 21 May 2024.

14. Regulation (EU) 2022/2554 (DORA).

15. Regulation (EU) 2024/1689 (AI Act).

16. Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA), [2023] OJ L 150/40.

17. Bank of England and FCA, "Critical Third Parties Policy Statement" (2024).

18. Federal Reserve, FDIC, OCC, "Interagency Guidance on Third-Party Relationships: Risk Management" (2023).

19. Civil Code of the Republic of Uzbekistan, Part One (21 December 1995).

20. Regulation (EU) 2022/2554 (DORA), Articles 28–44.

21. Regulation (EU) 2024/1689 (AI Act), Annex III.

22. Regulation (EU) 2023/1114 (MiCA).

23. Norton Rose Fulbright, "PSD3 and PSR: From Provisional Agreement to 2026 Readiness" (2026).

24. Federal Reserve, FDIC, OCC, "Interagency Guidance on Third-Party Relationships" (2023).

25. Federal Reserve Board, "Supervisory Observations on Banking-as-a-Service Arrangements" (2024).

26. OCC, "Risk Management of Artificial Intelligence in National Banks" (Bulletin, 2024).

27. Monetary Authority of Singapore, Technology Risk Management Guidelines (revised 2021).

28. MAS-IMDA, Guidelines on Shared Responsibility Framework for Phishing Scams (effective 16 December 2024).

29. MAS, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector (2018).

30. Law No. ZRU-578 (1 November 2019).

31. Presidential Decree No. PP-381 of 30 November 2023.

32. Central Bank Regulation No. 3513 of 21 May 2024.

33. Law of the Republic of Uzbekistan "On Personal Data" No. ZRU-547 (2 July 2019).

34. Central Bank Regulation No. 3513 of 21 May 2024.

35. Civil Code of the Republic of Uzbekistan, Part One (1995).

36. Interfax, "Uzbekistan Intends to Increase Share of Cashless Payments to 75% by 2030" (December 2025).

37. Zetzsche D. A., Buckley R. P., Arner D. W. "FinTech, BigTech and the Future of Banks" (2020) Review of Banking & Financial Law 40, 215–270.

38. Regulation (EU) 2022/2554 (DORA), Articles 28–44.

39. Bank of England and FCA, "Critical Third Parties Policy Statement" (2024).

40. Bank Service Company Act, 12 U.S.C. §§ 1861–1867b.

41. Central Bank Regulation No. 3513 of 21 May 2024.

42. Hacker P. "The European AI Act and the Regulation of High-Risk Credit-Scoring Systems" (2023) Common Market Law Review 60(5), 1351–1394.

43. Regulation (EU) 2024/1689 (AI Act).

44. MAS, FEAT Principles (2018).

45. Law of the Republic of Uzbekistan "On Personal Data" No. ZRU-547 (2 July 2019).

46. Directive (EU) 2015/2366 (PSD2), Article 73.

47. MAS-IMDA Guidelines on Shared Responsibility Framework (16 December 2024); Norton Rose Fulbright, "PSD3 and PSR" (2026).

48. Central Bank Regulation No. 3513 of 21 May 2024.

49. Law No. ZRU-578 (1 November 2019).

50. Presidential Decree No. PP-381 of 30 November 2023.

51. Central Bank Regulation No. 3513 of 21 May 2024.