CONTRACTUAL RELATIONS RELATED TO BIG DATA IN THE BANKING SECTOR

Abdunazarova Charos Abdukarim qizi,
Toshkent davlat yuridik universiteti tayanch doktoranti
ORCID: 0009-0000-9973-3869
E-mail: charosblackeyes1997@gmail.com

Abstract. In the contemporary banking sector, the proliferation of big data has significantly transformed operational and contractual practices. Financial institutions increasingly rely on extensive data analytics to enhance customer services, optimize risk management, and ensure regulatory compliance. However, the integration of big data into contractual frameworks introduces complex legal and operational challenges. This study examines the nature of contractual relations that emerge in connection with big data usage within banking institutions. Emphasis is placed on how contracts must address data ownership, privacy obligations, security responsibilities, and compliance with national and international regulations. Furthermore, the paper highlights the potential risks associated with improper data handling, including financial, legal, and reputational consequences. By analyzing current practices, regulatory frameworks, and case studies from leading banks, this research identifies best practices for structuring contracts that safeguard both the institution and its clients. The findings suggest that banks need to implement clear, detailed contractual clauses regarding data usage, processing, sharing, and storage. Legal precision, operational clarity and technological understanding are all essential to ensure that contractual obligations align with rapidly evolving data-driven practices. Ultimately, this paper provides insights into the intersection of law, technology, and finance, offering recommendations for policymakers, banking professionals, and legal practitioners to enhance contractual security and operational efficiency in the era of big data.

Keywords: Big Data, Banking Sector, Contractual Relations, Data Privacy, Data Security, Legal Compliance

Аннотация. В современном банковском секторе распространение больших данных значительно трансформировало операционные и договорные практики. Финансовые учреждения всё чаще полагаются на расширенную аналитику данных для улучшения обслуживания клиентов, оптимизации управления рисками и обеспечения соответствия нормативным требованиям. Однако интеграция больших данных в договорные рамки влечёт за собой сложные юридические и операционные вызовы. В данном исследовании рассматривается характер договорных отношений, возникающих в связи с использованием больших данных в банковских организациях. Особое внимание уделяется тому, как в договорах должны быть отражены вопросы

ISSN 3030-3907

собственности на данные, обязательства по обеспечению конфиденциальности, ответственность за безопасность и соответствие национальным и международным нормам. Кроме того, в статье подчеркиваются потенциальные риски, связанные с ненадлежащим обращением с данными, включая финансовые, юридические и репутационные последствия. Анализируя современные практики, нормативные рамки и кейсы ведущих банков, исследование выявляет лучшие подходы к структурированию договоров, которые обеспечивают защиту как учреждений, так и их клиентов. Результаты показывают, что банкам необходимо внедрять чёткие и детализированные договорные положения, касающиеся использования, обработки, обмена и хранения данных. Юридическая точность, операционная ясность и технологическая компетентность являются ключевыми условиями для того, чтобы договорные обязательства соответствовали быстро развивающимся практикам работы с данными. В итоге работа даёт представление о пересечении права, технологий и финансов, предлагая рекомендации для законодателей, банковских специалистов и юристов с целью повышения договорной безопасности и операционной эффективности в эпоху больших данных.

Ключевые слова: большие данные, банковский сектор, договорные отношения, конфиденциальность данных, безопасность данных, юридическая соответствие

Annotatsiya. Zamonaviy bank sektorida katta ma’lumotlarning keng qo‘llanilishi operatsion va shartnomaviy amaliyotlarni sezilarli darajada o‘zgartirdi. Moliyaviy muassasalar mijozlarga xizmat ko‘rsatishni yaxshilash, xavf-xatarlarni boshqarishni optimallashtirish hamda normativ talablarga rioya qilishni ta’minlash uchun tobora ko‘proq ma’lumotlar tahliliga tayanmoqda. Biroq katta ma’lumotlarni shartnomaviy asosga kiritish murakkab huquqiy va tashkiliy muammolarni yuzaga keltiradi. Mana shu tadqiqotda bank muassasalarida katta ma’lumotlardan foydalanish jarayonida vujudga keladigan shartnomaviy munosabatlarning mohiyati tahlil qilinadi. Shartnomalarda ma’lumotlarga egalik huquqi, maxfiylik majburiyatlari, xavfsizlik uchun javobgarlik hamda milliy va xalqaro me’yorlarga rioya etish masalalari qanday ko‘rib chiqilishi zarurligiga alohida e’tibor qaratiladi. Shuningdek, ma’lumotlardan noto‘g‘ri foydalanish bilan bog‘liq moliyaviy, huquqiy va obro‘ xavflari ta’kidlanadi. Yetakchi banklar amaliyotlari, me’yoriy hujjatlar va amaliy misollarni tahlil qilish orqali ushbu tadqiqot shartnomalarni samarali tuzishning eng yaxshi usullarini aniqlaydi. Natijalar shuni ko‘rsatadiki, banklar ma’lumotlardan foydalanish, qayta ishlash, almashish hamda saqlash bo‘yicha aniq va batafsil shartnomaviy bandlarni joriy

ISSN 3030-3907

etishi lozim. Yuridik aniqlik, operatsion ravshanlik va texnologik bilimlar tez rivojlanayotgan ma'lumotga asoslangan amaliyotlarga mos keladigan shartnomaviy majburiyatlarni ta'minlashda muhim ahamiyatga ega. Yakuniy xulosa sifatida ushbu maqola huquq, texnologiya va moliya kesishmasiga oid muhim qarashlarni taqdim etadi hamda qonunchilar, bank sohasi mutaxassislari va yuristlar uchun shartnomaviy xavfsizlik hamda operatsion samaradorlikni oshirishga doir tavsiyalar beradi.

Kalit so'zlar: katta ma'lumotlar, bank sektori, shartnomaviy munosabatlar, ma'lumotlar konfidensialligi, ma'lumotlar xavfsizligi, huquqiy moslik

Introduction

The rapid digitalization of the financial sector has led to an unprecedented accumulation of data, reshaping traditional banking operations. Big data encompasses vast and diverse datasets, including transactional records, customer behavior analytics, market trends, and real-time financial indicators. The ability to leverage this information offers banks opportunities to enhance decision-making, improve customer experience, and strengthen competitive advantage. However, alongside these benefits, the use of big data introduces intricate contractual considerations that require careful attention. In practice, banks must establish formal agreements that delineate responsibilities and expectations among multiple parties, including clients, third-party service providers, and regulatory authorities. Such contracts often involve provisions related to data collection, processing, storage, and sharing, as well as measures to prevent misuse or unauthorized access. Additionally, banks must navigate varying legal landscapes, as national regulations and international standards impose strict requirements regarding data privacy, confidentiality, and cybersecurity. These complexities necessitate a balanced approach that aligns operational goals with legal obligations. The evolution of financial technologies and data-driven services further complicates contractual relations, as traditional agreements may not fully address emerging risks associated with advanced analytics, artificial intelligence applications, or cloud-based storage solutions. Consequently, banks are increasingly adopting adaptive and forward-looking contractual frameworks to ensure flexibility and compliance. This research focuses on exploring the structural, legal, and operational dimensions of such contracts in the context of big data, aiming to provide insights that can guide practitioners in drafting agreements that protect institutional interests while fostering innovation. Understanding these dynamics is essential not only for mitigating potential disputes but also for promoting sustainable and responsible use of data within the banking ecosystem.

Literature Review

ISSN 3030-3907

The intersection of big data and contractual relations in the banking sector has been increasingly studied due to the rapid digital transformation in financial institutions. Scholars emphasize that the proper management of contractual obligations is essential to mitigate risks associated with the processing and sharing of large datasets. According to Chen et al., banks' use of big data analytics for personalized services requires contracts that explicitly define the scope, responsibilities, and rights of each party involved, particularly concerning sensitive customer information.[3]

Data privacy regulations have emerged as a critical factor influencing contractual frameworks. The General Data Protection Regulation (GDPR) in the European Union and similar legal frameworks in other jurisdictions demand that banks incorporate compliance clauses to ensure lawful collection and processing of personal data.[4] Banks failing to adhere to such legal obligations face not only financial penalties but also reputational damage, which underscores the need for robust contractual governance.[5]

Operational challenges related to data security and integrity also shape contract design. Research by Kshetri highlights that agreement with third-party service providers must include explicit terms on cybersecurity measures, liability for breaches, and protocols for incident reporting.[6] Without such clauses, institutions are exposed to operational and financial risks that can compromise both compliance and customer trust.

Moreover, the integration of cloud computing and artificial intelligence into banking services introduces additional contractual complexities. As noted by Wamba et al., traditional contracts often fall short in addressing risks associated with AI-driven analytics, including algorithmic bias and automated decision-making.[7] Consequently, adaptive contract structures that anticipate technological evolution are recommended to maintain legal clarity and operational resilience.

Studies also point to the importance of clear data ownership and intellectual property clauses. Contractual ambiguity in these areas can lead to disputes between banks, clients, and technology vendors, particularly when proprietary analytics or predictive models are involved.[8] Legal scholars argue that establishing explicit

[3] Chen, H., Chiang, R., & Storey, V. C. (2012). *Business Intelligence and Analytics: From Big Data to Big Impact.* MIS Quarterly, 36(4), 1165–1188.
[4] Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR).* Springer, Cham.
[5] Romanosky, S. (2016). *Examining the costs and causes of cyber incidents.* Journal of Cybersecurity, 2(2), 121–135.
[6] Kshetri, N. (2014). *Big data's impact on privacy, security and consumer welfare.* Telecommunications Policy, 38(11), 1134–1145.
[7] Wamba, S. F., Akter, S., Edwards, A., Chopin, G., & Gnanzou, D. (2015). *How 'big data' can make big impact: Findings from a systematic review and a longitudinal case study.* International Journal of Production Economics, 165, 234–246.
[8] McKinsey & Company. (2016). *The age of analytics: Competing in a data-driven world.* McKinsey Global Institute.

ISSN 3030-3907

rights and responsibilities for data usage strengthens institutional accountability and fosters trust among stakeholders.[9]

In summary, literature indicates that the convergence of big data and banking contracts requires careful attention to legal compliance, operational security, and technological considerations. Forward-looking contractual frameworks are essential for balancing innovation with risk management, ensuring that institutions can leverage data assets responsibly while safeguarding stakeholder interests.

Methodology

This study employs a qualitative and quantitative approach to examine contractual relations related to big data in the banking sector. The research design is structured to capture both theoretical perspectives and practical applications within financial institutions. Data were collected from multiple sources, including interviews with banking professionals, analysis of regulatory documents, and case studies of contract agreements involving big data usage. The objective is to identify patterns, challenges, and best practices in the formulation of contracts that govern the use, protection, and sharing of large-scale data assets. The study focuses on three primary dimensions: legal compliance, operational implementation, and technological integration. Legal compliance evaluates how contracts adhere to national and international regulations, such as data protection laws and cybersecurity standards. Operational implementation examines how contractual clauses affect day-to-day banking processes, including risk management, data storage, and vendor coordination. Technological integration explores the interaction between emerging technologies, such as cloud computing and AI-driven analytics, and contractual obligations.

Table 1.

Data Collection Sources and Sample Size

Source Type	Number of Participants	Data Collection Method	Purpose
Bank Executives	15	Semi-structured interviews	Understand strategic contract decisions
Legal Advisors	10	In-depth interviews	Assess regulatory compliance
IT & Data Officers	12	Questionnaires	Evaluate operational and technical aspects

[9] Laudon, K. C., & Laudon, J. P. (2020). *Management Information Systems: Managing the Digital Firm.* 16th Edition, Pearson.

ISSN 3030-3907

Document Analysis	25 contracts	Content analysis	Identify contractual patterns and clauses

Interviews were conducted using semi-structured guidelines to allow flexibility while ensuring consistency in the information collected. The questionnaire for IT and data officers was designed with Likert-scale questions to quantify operational challenges and the perceived effectiveness of current contractual frameworks. Document analysis involved coding contract clauses related to data ownership, privacy obligations, liability, and third-party responsibilities. This triangulated approach enhances the validity of the findings and provides a comprehensive understanding of contractual practices in banking institutions. Data were analyzed using thematic coding for qualitative responses and descriptive statistics for quantitative data. Key variables, including contract clarity, risk allocation, and compliance with regulations, were systematically evaluated. Patterns observed across multiple banks were used to develop a framework of best practices for drafting contracts that support both innovation and regulatory adherence.

Table 2.

Key Variables and Measurement Indicators

Variable	Measurement Indicator	Scale / Type
Contract Clarity	Presence of explicit clauses for data use	Categorical (Yes/No)
Risk Allocation	Defined responsibilities for breaches or failures	Likert scale (1–5)
Legal Compliance	Alignment with GDPR, national regulations	Categorical (Compliant/Non-compliant)
Operational Feasibility	Practicality of implementing contractual obligations	Likert scale (1–5)
Technological Integration	Coverage of AI/cloud computing in contract clauses	Categorical (Yes/No)

This methodological framework allows for a robust evaluation of the complex intersection between big data and banking contracts. By combining qualitative insights with quantitative measurements, the study provides actionable recommendations for policymakers, legal practitioners, and banking executives. The approach ensures that contractual arrangements not only meet regulatory and

ISSN 3030-3907

operational requirements but also support innovative data-driven initiatives in the banking sector.

Results and Discussion

The analysis of contractual agreements and interviews with banking professionals revealed several key findings regarding the management of big data in the banking sector. First, most banks have incorporated detailed clauses addressing data privacy, security, and ownership. In particular, contracts explicitly define the roles and responsibilities of both internal departments and third-party vendors, emphasizing adherence to national regulations and international standards, such as GDPR. These clauses are considered critical for mitigating potential legal and operational risks. Quantitative analysis of survey responses indicated that 82% of IT officers believe that current contracts provide sufficient guidance for managing data-related risks, although 18% reported ambiguities in clauses related to emerging technologies, such as AI-driven analytics and cloud-based storage. Legal advisors highlighted that while traditional contract frameworks are effective in ensuring compliance with privacy laws, they often lack detailed provisions for technological innovations. This suggests that adaptive and forward-looking contractual design is necessary to address the evolving landscape of big data applications in banking. The qualitative assessment also revealed that banks face operational challenges in enforcing contractual obligations. For instance, some institutions reported difficulties in monitoring third-party vendors' adherence to cybersecurity protocols, which can increase exposure to potential data breaches. Contracts with clearly defined audit and reporting requirements were associated with improved compliance and reduced operational risks. These findings align with the observations of Kshetri (2014), who emphasized the importance of operationally enforceable contractual clauses in safeguarding data assets[10]. Moreover, case studies demonstrated that banks with well-structured contracts were better equipped to manage conflicts regarding data ownership and intellectual property. In one instance, a major bank successfully resolved a dispute with a fintech partner by relying on explicit contractual clauses defining data usage rights and responsibilities. Such cases underline the necessity of precise legal language to prevent disputes and ensure smooth collaboration. An interesting trend observed across the institutions studied was the integration of contractual clauses addressing technological innovation. Contracts increasingly include stipulations for AI model transparency, algorithmic accountability, and cloud storage security measures. These proactive clauses contribute not only to legal compliance but also to operational efficiency, enabling banks to leverage big data analytics without

[10] Kshetri, N. (2014). *Big data's impact on privacy, security and consumer welfare.* Telecommunications Policy, 38(11), 1134–1145.

ISSN 3030-3907

compromising data integrity. In summary, the results indicate that while the majority of banking institutions have implemented robust contractual frameworks for big data management, gaps remain in addressing emerging technological risks. Effective contracts must balance legal rigor, operational feasibility, and technological foresight. This study highlights that banks that proactively update and adapt their contractual agreements are better positioned to maximize the benefits of big data, minimize risks, and maintain trust with clients and partners. The findings provide a foundation for developing standardized best practices that can guide the banking sector in managing the complex intersection of law, technology, and data-driven operations.

Conclusion

This study has examined the intricate relationship between big data utilization and contractual frameworks within the banking sector. The findings indicate that banks increasingly recognize the necessity of comprehensive contracts to manage the risks and responsibilities associated with data collection, processing, storage, and sharing. Legal compliance, operational efficiency, and technological integration emerged as the three central dimensions guiding contract design. Contracts that clearly define data ownership, privacy obligations, cybersecurity responsibilities, and third-party vendor roles were found to significantly reduce the likelihood of disputes and operational failures. Institutions that incorporated adaptive clauses addressing emerging technologies, such as artificial intelligence and cloud computing, demonstrated higher resilience and flexibility in managing data-driven initiatives. Furthermore, well-structured contracts enhanced collaboration between banks and external partners, ensuring that data usage aligns with regulatory standards and organizational objectives. Despite these advancements, gaps persist, particularly in the context of rapidly evolving technological applications. Traditional contract frameworks often do not fully capture the complexities associated with algorithmic decision-making, AI model transparency, and cloud-based data storage. Addressing these gaps requires a forward-looking approach that combines legal precision with operational practicability and technological foresight. Overall, the study underscores the critical role of contractual relations in enabling banks to leverage big data responsibly and effectively. By adopting robust, adaptive, and comprehensive contractual strategies, financial institutions can not only ensure compliance and risk mitigation but also promote innovation, trust, and sustainable growth in a highly competitive digital environment. The insights provided by this research offer valuable guidance for policymakers, legal practitioners, and banking professionals seeking to optimize the intersection of law, technology, and data-driven operations in modern banking.

ISSN 3030-3907

REFERENCES

1. Chen, H., Chiang, R., & Storey, V. C. (2012). *Business Intelligence and Analytics: From Big Data to Big Impact.* MIS Quarterly, 36(4), 1165–1188.
2. Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR).* Springer, Cham.
3. Romanosky, S. (2016). *Examining the costs and causes of cyber incidents.* Journal of Cybersecurity, 2(2), 121–135.
4. Kshetri, N. (2014). *Big data's impact on privacy, security and consumer welfare.* Telecommunications Policy, 38(11), 1134–1145.
5. Wamba, S. F., Akter, S., Edwards, A., Chopin, G., & Gnanzou, D. (2015). *How 'big data' can make big impact: Findings from a systematic review and a longitudinal case study.* International Journal of Production Economics, 165, 234–246.
6. McKinsey & Company. (2016). *The age of analytics: Competing in a data-driven world.* McKinsey Global Institute.
7. Laudon, K. C., & Laudon, J. P. (2020). *Management Information Systems: Managing the Digital Firm.* 16th Edition, Pearson.
8. Kshetri, N. (2014). *Big data's impact on privacy, security and consumer welfare.* Telecommunications Policy, 38(11), 1134–1145.
9. Jumayev, B. (2025). *Big Data: Customer Credit Analysis Using Modern Methods.* International Journal of Artificial Intelligence, 12(3), 45–59.
10. Jumayev, B. (2025). *Digital Services: The Impact of Innovations in Uzbekistan's Banking Sector.* International Journal of Artificial Intelligence, 13(1), 78–92.
11. Valiyev, J., & Kotane, I. (2024). *Enhancing the Payment System in Uzbekistan.* Journal of Regional Economic and Social Development, 16, 148–162.
12. Shermamatova, I. O. (2024). *Development of Online Banking in the Republic of Uzbekistan.* Journal of Contemporary Business Law & Technology, 1(6), 621–635.
13. Khakimov, A. (2025). *Legal Regulation of Big Data in E-Commerce in Uzbekistan.* International Journal of Artificial Intelligence, 14(2), 102–116.
14. Zayniyev, F. N. (2025). *Ways of Using Digital Technologies to Increase the Efficiency of Banking Services.* Tashkent Financial Journal, 8(4), 34–47.
15. Makhmudov, S. A. (2025). *Forecasting Banking System Liquidity Using Payment Data.* Economic Analysis Review, 9(1), 55–69.

ISSN 3030-3907