AGORA International Journal of Economical Sciences, http://univagora.ro/jour/index.php/aijes
ISSN 2067-3310, E-ISSN 2067-7669
Vol. 19, No. 2 (2025), pp. 240-247

REGULATION OF DIGITAL BANKING SERVICES: OBJECTIVES, PRINCIPLES AND FRAMEWORKS

R. MAMMADLI

Ragib Mammadli
Azerbaijan State University of Economics (UNEC), Azerbaijan
https://orcid.org/0009-0009-3721-3548, E-mail: mammadli.raqib.mammadali.2023@unec.edu.az

Abstract: *In recent years, the rapid growth of technological advances has reshaped all sectors of the economy and changed the behaviour of both institutions and customers. By implementing the latest innovations, banks are digitalizing their services and automating most of the internal banking management processes. Digital banking makes services more accessible to customers, increases their transparency and efficiency, and reduces costs for both banks and customers. Today, everyone can conduct banking transactions from home and at any time. But in addition to their benefits, digital banking services also pose serious challenges in terms of privacy, security and customer protection. This article highlights the importance of regulating digital banking services and discusses the objectives and principles of regulation. In addition, it provides a comparative overview of the current state of digital banking regulatory models in selected regions, outlining the main objectives of regulatory authorities.*

Keywords: *digital banking services, regulation, regulatory framework, customer protection*

1. INTRODUCTION

In recent years, the global financial system has undergone a significant evolution under the influence of innovations and digital technologies. Modern innovations contribute to increased productivity, functionality and efficiency in all sectors of the economy. They also affect society and have led to changes in customer behaviour. The application of digital technologies has now become a necessity in order to remain competitive in all sectors.

One of the most important results of technological development is digital banking - a technology-based model of banking services that operates mainly or entirely through digital channels. As a result of the rapid development and constant change of technology, customer expectations regarding banking services are also constantly changing and their new needs arise. Unlike traditional banking, banks now provide simplified, wide-ranging and customer-oriented banking services through mobile applications, web platforms and interfaces powered by artificial intelligence. (Harchekar, 2021)

The application of digital technologies to banking increases the accessibility of banking services, improves efficiency, helps to create new banking products and improve existing ones, and reduces costs for both banks and customers. The application of technology also raises concerns about privacy, cybersecurity and customer protection. Moreover, from a legal point of view, no one can prove that digital technologies in the banking sector are used only for their intended purpose. (Bety, 2023). Regulators should take appropriate measures to minimize these problems.

Regulation of digital banking services should be carried out in a balanced manner. It should support the development of digital technologies, protect the integrity of the financial system, and fully cover the rights of banks and customers in the digital environment. Strict and burdensome regulation can slow down the development of digital technologies and harm the banking sector. On the other hand, weak regulation can lead to the misuse of technologies.

Countries also vary significantly in their approaches to regulating digital banking services. For example, the European Union has many acts and directives related to the operation of digital services, including banking. But in developed countries of Asia, more innovative methods are applied to regulating digital services.

Traditional regulatory frameworks, designed primarily for brick-and-mortar banking models, are insufficient to control the complex nature of technology-based banking services. To this end, regulators in each country should set regulatory standards specifically for the operation of digital banking services.

2. Main Objectives of Regulation of Digital Banking Services

Considering the benefits and risks brought by technological innovation, the main objectives of regulating digital banking services are as follows:

Figure 1. *Objectives of Regulation of Digital Banking Services*

Protecting financial stability. One of the key objectives of regulating digital banking services is to ensure the stability and integrity of the financial system. Financial stability is a core concern of economic regulation, particularly in environments characterized by rapid technological change. Although new financial technologies and innovations in today's digital environment support the growth of diversity and accessibility of banking services, the rapid pace of innovation, the emergence of new business models and non-traditional financial institutions pose a threat to the stability of the financial system. Regulators should assess banks offering digital services on various criteria such as capital buffers, liquidity, stress testing, risk management, etc. and ensure that they operate in accordance with the standards. For example, the Monetary Authority of Singapore regularly conducts stress testing audits of banks and financial institutions offering digital services. (Papathanassiou, 2024). Such measures help identify vulnerabilities in digital technologies and improve the resilience of the entire financial system.

Protecting customer rights. When using digital banking services, customers face new risks such as misuse of personal data, unauthorized transactions and deceptive digital interfaces. These problems can undermine consumer trust and reduce the efficiency of digital financial services. Another key objective of regulating digital banking services is to protect the rights and interests of customers by ensuring transparency between banks and customers. Regulatory methods include clearly disclosing the terms and conditions of using digital services, providing a user-friendly digital interface for using digital services, mechanisms for resolving uncertainties and complaints, etc. Regulators can also give customers full control over their personal data in the digital banking environment to prevent misuse of personal data. (Lee & Thomsett, 2020). Strengthening consumer protection helps increase trust in digital banking services and expand access to financial services.

Cybersecurity. When providing digital banking services, banks collect and process data in real-time using technologies such as application programming interfaces (APIs), cloud services, third-party providers, etc. The widespread use of interconnected digital infrastructures increases operational efficiency, but also expands potential attack surfaces. Despite the numerous benefits of digital banking services, cybercriminals can gain access to banking systems and obtain personal and financial information of customers. (Kern, 2019). Moreover, in recent times, many financial systems are interconnected, a problem in one of them can pose a threat to others. Given the volume and sensitivity of financial data collected in banking systems, regulators should take serious measures to ensure the security and integrity of the digital banking infrastructure from cyber threats. These include data encryption, breach notifications, control of third-party access to the banking system, continuous monitoring of the banking system, etc. Effective cybersecurity regulation is therefore essential to maintaining trust and preventing systemic disruptions.

Customer identification. The accessibility and borderlessness of digital banking services make they a tool for illegal financial activities such as money laundering, terrorism financing and fraud. Weak identification mechanisms can increase the risks of financial crimes in the digital environment. Anonymous transactions through digital banking and financial platforms make it difficult to determine the source and address of money flows. To prevent this, customers using digital banking services must be identified using biometric data. In addition, to prevent the abuse of digital banking, all banking transactions must be monitored, their validity must be confirmed and reports must be required in case of suspicious or unexplained transactions. (Shoshani, 2024). These measures bring digital banking regulation into line with international standards for combating money laundering and terrorist financing.

Fair competition. Effective regulation should encourage banks and financial companies offering digital financial services to work together and create a fair competition environment by preventing monopolies and anti-competitive behaviour in the banking sector. Competitive digital banking markets drive innovation, lower costs, and improved service quality for consumers. It should also reduce barriers to entry for new or smaller banks and financial institutions, provide simplified licenses to support their activities. However, these licenses should reflect all the essential requirements for the proper provision of digital banking services.

Ethical use of technology. Technological innovation is constantly growing and has an impact on all sectors. Regulators should support the introduction of innovations and new digital technologies in order to improve banking services and the banking sector as a whole. However, regulators should require transparency and a detailed explanation of the purpose of the innovations introduced and monitor their use only for the intended purposes. (Lumpkin & Schich, 2020).

3. Key Principles of Regulation of Digital Banking Services

Regulation of digital banking services should be based on principles such as neutrality, proportionality, risk-based approach, adaptive regulation and international cooperation. Below is a detailed explanation of each principle:

Neutrality. When regulating digital banking services, it is necessary to take a neutral approach to all participants in the banking sector, avoiding a biased approach to digitalization, the financial technologies used and the methods of service delivery. This principle ensures that regulation does not distort market competition or favour particular technologies or business models. Regulation should apply equally to banks offering digital services and to traditional banks, fintech companies and other financial institutions, and a fair competitive environment should be ensured between them. Therefore, when regulating digital banking services, attention should be paid not only to the services and business models that use digital financial technologies, but also to their functions and the risks they bear. (Vasant, 2025). Such an approach allows regulators to focus on economic substance rather than form, which is particularly important in rapidly evolving digital financial markets.

Proportionality. According to this principle, when regulating digital banking services, the rules and requirements should not be the same for all market participants, but different approaches should be applied taking into account the size, complexity and range of services offered by the regulated entity. (Omarini, 2024). This principle reflects the need to balance regulatory oversight with the capacity of institutions to comply with regulatory requirements. Differentiated regulatory rules prepared taking into account the specific features of institutions offering digital banking services prevent overloading small market participants, support their development and encourage the application of various digital financial technologies to banking services. As a result, proportional regulation contributes to innovation while maintaining adequate levels of financial stability and consumer protection.

Risk-based approach. When regulating modern banking services that include digital financial technologies, attention should be paid primarily to high-risk services, products or behaviour that pose

a threat to customer rights and financial stability. This approach is particularly relevant in digital banking, where technological complexity can increase operational, cyber and compliance risks. A risk-based approach helps to prioritize areas that most need regulation, allowing for a timely response to risks and improving the effectiveness of regulation. (Dudin, Shkodinskii & Usmanov, 2021).

Adaptive regulation. Given the pace of change and development of digital financial technologies applied to banking services, rigid legal frameworks "written on paper" may prove ineffective for regulation. Digital innovation often outpaces traditional legislative processes, creating regulatory gaps and uncertainties. Regulatory approaches should adapt to the modern technological environment and be based not only on written rules but also on guidelines, consultations and observations. Innovation centres should be created, and new digital financial technologies applied to banking services and management should be tested in an environment under the control of the regulator, their features assessed and then regulated accordingly. (Sharma, 2022). Adaptive regulation allows regulators to respond flexibly to technological change while reducing regulatory uncertainty for market participants.

International cooperation. Unlike traditional banking, banks can offer banking services to customers from all over the world across national borders using digital technology. This cross-border nature of digital banking increases regulatory complexity and requires coordination among national authorities. For example, anyone living in Romania can use international digital banking services offered by a bank operating in any other country without leaving home. However, the different forms of regulation that each country applies to digital banking and financial services can sometimes prevent banks from offering banking services on a global scale. (Frolova & Perm, 2019). To avoid regulatory diversity, regulators in all countries that regulate digital banking and financial services should collaborate with central banks, international financial institutions, and financial cybersecurity agencies in other countries to develop regulatory forms and standards that meet global requirements. Such cooperation supports financial stability, reduces regulatory arbitrage and facilitates the sustainable development of global digital banking markets.

4. Methodology

The article consists of theoretical and analytical parts. While preparing this article, an extensive literature review was conducted based on relevant articles, books, and journals. Using a qualitative research approach, the theoretical part of the article explains the objectives and principles of regulating digital banking services.

The analytical part of the article reviews and compares the methods of digital banking services around the world. To analyse the regulatory framework in different countries, data are collected from official banking laws, regulatory standards, acts, etc. The conclusion part explains the main limitations of regulating digital banking services based on the research results.

The purpose of this study is to clarify the concept of regulation of digital banking services and provide a comprehensive overview of the regulation of digital banking technologies and services worldwide. Although this article does not rely on primary data collection, it contributes to the literature on how to create a secure digital banking environment while supporting technological advancement.

5. Results - Regulation of Digital Banking Services Around the World

Unfortunately, there is currently no regulatory approach anywhere in the world that would fully cover digital banking services and eliminate all their risks. This reflects the complexity and rapid development of digital financial technologies, which often outpace regulatory responses. As a result, regulatory frameworks remain fragmented and are often adapted gradually rather than comprehensively. In many countries, digital banking services are regulated based on traditional banking standards and some specific rules related to digitalization. However, some countries have already started to create special regulatory frameworks related to digital banks, digital banking and

financial services. These emerging approaches demonstrate different regulatory priorities and levels of institutional maturity.

In the European Union, the European Banking Authority (EBA) provides banks with advice on financial innovation, digital security and resilience, and oversees financial stability within the union, ensuring that they comply with regulatory standards and rules. The EBA plays a central coordinating role in the harmonisation of regulatory practices across member states. The main objective of the organization is to create uniform standards covering the rights of customers and banks for all EU countries. Examples of existing regulatory standards related to the operation of digital banking services in the European Union include:

General Data Protection Regulation. The GDPR, which came into force in 2018, sets strict requirements for the protection of customer data and privacy across all sectors, including banking, within the European Union. This regulation has significant implications for digital banking services, which rely heavily on the collection and processing of personal data. According to the regulation, banks must obtain consent from customers before collecting personal data and provide each individual with the right to manage and delete their data in the banking system. (GDPR, 2018).

The Network and Information Security Directive (NIS Directive) is a legal framework consisting of rules and controls covering the protection of technologies, information systems and people from cyber threats and risks in 18 key economic sectors of the European Union, including finance and banking. Cybersecurity is a critical component of digital banking regulation given the interconnectedness of digital financial infrastructures. It requires member states to strengthen their security capabilities in the digital environment, to report on recorded cybercrime incidents and to cooperate with the EU in developing their national strategies for managing information security risks. This directive strengthens cross-border coordination in the fight against cyber threats.

The Payment Services Directive aims to regulate payment systems in the European Union, reduce banks' monopoly on customer data and increase competition between banks and non-bank financial institutions. The directive reflects a shift toward open banking models within the EU. Under the regulation, banks must provide payment service providers with access to customers' bank data to create integrated payment systems. All parties are also required to fully comply with data security and privacy rules.

The Anti-Money Laundering Directive (AMLD) requires banks to verify the identity of customers using digital services, investigate suspicious transactions and determine the final address of these transactions in order to prevent money laundering, terrorist financing and illicit financial transactions in the EU.

The Digital Operational Resilience Act (DORA) aims to improve the digital resilience of all financial institutions, including banks, by requiring them to strengthen the security of their information and communications technology (ICT) against cyber risks. (DORA, 2023). The Financial Conduct Authority (FCA), established in the UK in 2013, supervises all financial services providers, including banks. It licenses banks, provides guidance on the appropriate use of digital technologies, and monitors transparency and fraud in banking services. To ensure the integrity and co-evolution of digitally enabled banking and financial systems, nine major UK banks have been instructed since 2016 to allow other officially licensed financial institutions to access their customer databases. The FCA is also responsible for ensuring that customers are kept safe when sharing personal data.

In the United States, the Federal Reserve System regulates and constantly monitors the activities of banks and financial institutions. It regularly conducts studies on the impact of digital technologies on the development of finance, the economy, and society and publishes articles about its findings on its official website. The Federal Reserve System has also been working on a "digital national currency" project for a long time.

The Consumer Financial Protection Bureau is an organization that protects the rights of customers in the banking and financial sector. It requires banks and financial institutions to explain

their terms of services to customers in detail, not to conduct any transactions without the permission of customers, and to prevent deceptive marketing activities. The Bureau also evaluates customer complaints and takes action against the institution to which the complaint relates.

In addition to the regulation methods of these bodies, states sometimes have their own different regulatory standards for banks, privacy, or digitalization. For example, all institutions and companies in the state of California, including banks, must additionally comply with the California Consumer Protection Act, which came into force in 2020. Among the key provisions of the law, it is noted that California residents (consumers):

- Should know what information companies collect about them and for what purpose;
- Can request a copy of the personal information held about them;
- Can request that their personal information be permanently deleted at any time;
- Can request that their personal information not be shared with third parties under any circumstances;
- Should not be discriminated against based on their privacy preferences, etc. (CCPA).

India has only a few digital security standards for banking and financial services. All other activities are regulated under traditional banking regulatory standards. As a result, digital banking services in India largely operate within existing institutional and supervisory frameworks. However, the government supports the implementation of digital technologies to provide access to banking services to people from all corners of the country and improve their well-being. This policy focus highlights the importance of financial inclusion as a national development goal. India's first formal law on digital privacy was passed in 2023. (DPDP Act). The passage of this law marks an important step towards strengthening data protection and consumer trust in digital financial services.

In the United Arab Emirates, one of the main countries that many banks around the world want to enter as a foreign market, the Financial Services Regulatory Authority (FSRA) oversees the activities of all local and foreign technology-based digital financial services operating in the country. The UAE is positioning itself as a regional financial and fintech hub, attracting international banks and digital service providers. The regulatory framework emphasizes oversight of innovation while ensuring compliance with international financial standards. Through the Financial Services Regulatory Authority (FSRA), the UAE aims to balance market openness with effective risk management in the digital banking sector.

Singapore has one of the world's most advanced digital services regulatory frameworks. In 2019, the Monetary Authority of Singapore (MAS) began issuing digital licenses that cover the operating principles of fully digital banks and financial technology (fintech) companies. The organization has a comprehensive framework on AI ethics, digital data governance, risk control, digital systems, and cryptocurrencies. All new financial technologies, banking and financial services are tested in the country. Only when they are deemed acceptable are they allowed to be offered to the public.

China is one of the countries where digital banking and digital financial technologies are rapidly developing. The scale and pace of digital financial technology adoption in China is unparalleled in many regions. WeBank, which operates in China, is the world leader in the number of digital banking services used, with more than 350 million customers per month. In 2019, a virtual bank license was issued in Hong Kong, a special administrative region of China. In order to improve financial inclusion, the Chinese government supports the operation of digital banking and financial services. However, the country has strict controls on digital services, payment systems, data security and data transfer to other countries.

6. DISCUSSION/CONCLUSION

The results of the research show that the number of digital technologies and software used in banking is constantly increasing. However, no matter how much they are improved, the regulatory methods of countries cannot fully cover digital financial technologies and are constantly lagging

behind. Taking into account the diversity and complexity of digital banking services, the main limitations of their regulation include the following:

Rapid technological development. As technology advances, the technologies used by banks are also constantly changing, the range of digital banking services is increasing, and new digital financial products are emerging. At the same time, the methods of regulation of digital services in the countries are constantly lagging behind and losing effectiveness because they cannot keep up with the pace of technologies. For example, in many countries, regulatory authorities are still unable to determine how to approach banks and non-traditional financial institutions operating in digital form when granting them licenses.

Costs of regulation. New digital technologies are constantly being introduced in the banking sector, new services and products are being created, existing ones are being improved, etc. In order to keep up with these and implement more effective regulation, regulatory authorities must thoroughly understand the essence of each technology applied in the banking and financial sector, involve specialists in digital services and products when developing regulatory methods, and conduct training for existing personnel. Since implementing each of the above requires financial resources from regulatory authorities, it is often not possible to fully implement them, and this negatively affects the quality of regulation. (Alatovic, Gerson & Saade, 2021).

Cross-border incompatibility. Currently, many banks want to serve customers in other countries, beyond the borders of the country in which they operate. However, each country may have its own requirements in terms of banking activities, provision of services, bank and customer rights, security, etc. When entering new markets, banks are often able to adapt to the requirements of those countries and operate in accordance with the local environment. But sometimes countries can demand significant changes in forms or types of digital services. Obstacles such as strict rules and burdensome regulatory methods cause banks to abandon new markets in those countries, which hinders the globalization of modern digital banking services. To minimize such situations, international cooperation between countries, international banks and financial institutions is required. For example, the activities of banks in the European Union countries are regulated through the standard Eurosystem, which is the supervisory mechanism of the European Central Bank. banks in these countries can operate comfortably in each of the European Union countries and offer digital banking services to customers.

Data security and privacy. Protecting the security and privacy of customer data is very important for the trust of both customers and banks. Although regulatory authorities have developed strict frameworks for banks and financial institutions offering digital banking services to ensure the security of customer data, it is often not possible to be completely sure to what extent they comply with these requirements, for what other purposes they use the data, and whether they share it with others without permission. In addition, the vulnerability of all digital platforms to cyberattacks poses a constant threat to the security of customer data stored in any banking system. (Jovan, 2025).

Customer identity verification. As mentioned earlier, the accessibility of digital banking to everyone creates conditions for its use as a tool for illegal financial activities. Therefore, banks, financial institutions and regulatory authorities must be able to verify the identity of customers using digital services. However, in the digital environment, sometimes transactions can be carried out without registration, fake identities can be created, and even transactions can be carried out in someone else's name. Unfortunately, in the current conditions, even with the most modern methods, it is sometimes impossible to identify the real users behind the transactions. (Alatovic, Gerson & Saade, 2021). The future of every sector of the economy is shaped by technological progress. Banks should always use innovations for intended purposes and implement the latest technologies in banking services to meet the growing needs of customers and remain competitive in the financial environment. On the other hand, regulatory authorities should improve their methods of regulating digital services to protect customers and the stability of the financial system.

REFERENCES

1. Alatovic, T. Gerson, H. & Saade J. (2021). Lessons from the rapidly evolving regulation of digital banking, McKinsey & Company Reports.
2. Bety K. (2023). Unveiling the power of artificial intelligence: A comprehensive review of its role in the banking sector. International Journal of Intelligent Computing and Information Sciences, 2023, IJICIS, Vol.24, No.1, p 29-41.
3. Dudin, N., Shkodinskii V. & Usmanov, I. (2021). Key Trends and Regulations of the Development of Digital Business Models of Banking Services in Industry 4.0. Finance: Theory and Practice, Vol. 25, No. 4, 2021. DOI: 10.26794/2587-5671.
4. Frolova, E. & Perm, U. (2019). Legal regulation of digital banking in Russia and foreign countries (European Union, USA, PRC). HeinOnline.
5. Jovan, S. (2025). Legal Aspects of Digital Banking. LAW - Theory and Practice, No.1, 2025.
6. Harchekar, J. (2021). Digitalization in banking sector. International Journal of Scientific Research and Development. Issue 11.
7. Kern, A. (2019). Principles of Banking Regulation. Cambridge University Press.
8. Lumpkin, S. & Schich S. (2020). Banks, Digital Banking Initiatives and the Financial Safety Net: Theory and Analytical Framework. Journal of Economic Science Research, Vol 03, Issue 01, January 2020.
9. Lee, J. & Thomsett, D. (2020). Disruptions and Digital Banking Trends. Journal of Applied Finance & Banking, Vol. 10, No. 6, 2020, 15-56. ISSN: 1792-6580 (print version).
10. Papathanassiou, C. (2024). Digital innovation and banking regulation. ECB Occasional Paper Series No 351.
11. Omarini, A. (2024). The Changing Landscape of Retail Banking and the Future of Digital Banking. Perspectives in Law, Business and Innovation, Springer book series.
12. Sharma, R. (2022). A study on innovation in banking and its impact on customer satisfaction. Integrated Journal for Research in Arts and Humanities. Volume 2, Issue 3, May 2022. pp. 67-72.
13. Shoshani, Y. (2024). Regulatory Compliance in Digital Banking. Ezbab.
14. Vasant, C. (2025). Changing Dimensions of Financial Services and Banking Regulation. Palgrave Macmillan publishing. https://doi.org/10.1007/978-981-96-5443-7.
15. California Consumer Privacy Act (CCPA). Available at: https://oag.ca.gov/privacy/ccpa
16. Digital Operational Resilience Act (DORA). Available at: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
17. General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu
18. Digital Personal Data Protection Act of India, Ministry of Electronics and Information Technology. Available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
19. Federal Reserve System https://www.federalreserve.gov.
20. Monetary Authority of Singapore www.mas.gov.sg.