Srećković Jovan[*]
https://orcid.org/0009-0008-6657-7570

UDK: 336.71:004.738.5
Review article
DOI: 10.5937/ptp2501144S
Received on: November 12, 2024
Approved for publication on:
February 3, 2025
Pages: 144–156

LEGAL ASPECTS OF DIGITAL BANKING

ABSTRACT: The rapid development of digital banking has fundamentally transformed the capabilities of the financial sector, offering a range of new opportunities and challenges. This paper explores the legal aspects of the transformation of the financial sector through digital banking. It analyzes the regulatory framework that impacts the development and implementation of digital banking services, focusing on key laws, regulations, and legal standards that shape this area. The paper also addresses issues of data security, privacy protection, user authentication, and liability in cases of fraud or abuse. The research aims to provide deeper insights into the legal challenges and opportunities arising from the digital transformation of the financial sector, as well as identify potential legal frameworks and strategies for improving the efficiency and transparency of digital banking. The paper further examines the impact of digital banking on traditional banking practices, including customer service, operational efficiency, and revenue-generation models. Special attention is given to exploring the implications of digital banking for financial inclusion, particularly in underserved and remote communities, and its role in fostering economic development.

Keywords: *Internet law, digital banking, commercial law, data protection.*

[*]LLM, PhD student, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: jovansreckovic.js@gmail.com

1. Introductory remarks

The banking sector plays a crucial role in the economic stability and development of every country, including Serbia. Traditional banking, which involves the physical presence of clients in banks, has gradually evolved under the influence of technological innovations. In recent years, digital banking has experienced significant growth, enabling users to conduct financial transactions quickly and efficiently via the internet and mobile applications.

Digital banking offers numerous advantages, such as greater accessibility of services, reduced operational costs, and increased business efficiency. However, along with these benefits come new challenges, particularly in the context of legal regulations and security aspects. Digital financial transactions raise questions of data protection, fraud prevention, and compliance with the existing legal framework.

During the transitional period, the banking sector faced significant challenges, including a high level of non-performing loans, lack of adequate regulation and supervision, as well as a lack of capital and technological infrastructure. These challenges resulted in weak stability of the banking system and limited access to financial services for citizens and businesses, consequently causing numerous legal issues.

However, over the past decade, the banking sector in Serbia has undergone significant changes and progress. Driven by reforms, strengthening of the regulatory framework, and investment in modernization, the banking sector has become more stable, efficient, and competitive.

The significance of digitalization in banking is reflected in several factors. Digitalization opens the banking sector to new players, including financial technology companies (FinTech) and tech giants, who offer new products and services. Digital technologies enable banks to personalize their offerings and provide a better user experience. Through the analysis of user behavior data, banks can offer personalized products and services that meet the specific needs and preferences of each user (Madir, 2024, p. 112).

This paper aims to provide a comprehensive analysis of the legal aspects of banking in Serbia, with a special focus on digital banking. By exploring the current regulatory framework related to digital banking, identifying major legal challenges, and analyzing how these challenges can be overcome, this paper will also review relevant laws and regulations, including the Banking Law, the Law on Payment Services, and other regulations governing this area.

2. Legal Framework of Banking in Serbia

The banking sector in Serbia is regulated by a series of laws and regulations aimed at ensuring the stability, transparency, and efficiency of the financial system. The key laws regulating banking in Serbia include:

- The Law on Banks[1]
- The Law on the National Bank of Serbia (NBS)[2]
- The Law on Payment Services and Electronic Money[3]
- The Law on the Prevention of Money Laundering and Financing of Terrorism.[4]

In Serbia, the competent institutions and regulatory bodies responsible for the regulation and supervision of the banking sector include:

- The National Bank of Serbia (NBS): The main institution responsible for the regulation and supervision of the banking sector, which implements monetary policy, oversees financial stability, and ensures the application of regulations in the banking field.
- The Ministry of Finance of the Republic of Serbia: Has jurisdiction over the financial sector and is responsible for enacting laws, regulations, and policies in the field of banking.
- The Securities Commission: Responsible for regulating the capital market and supervising brokerage firms and investment funds.
- The Deposit Insurance Agency: Oversees the deposit insurance system and provides protection to depositors in case of bank bankruptcy.

The main characteristics of the legal status of a bank are: It is established exclusively in the legal form of a joint-stock company. Headquarters must be

[1] This law defines the basic principles and conditions for the establishment, operation, and termination of banks in Serbia. It regulates the structure, organization, capital, management, supervision, and cessation of banks, ensuring the stability and integrity of the banking sector.

[2] This law regulates the organization, powers, and functions of the National Bank of Serbia as the main regulatory body in the field of banking. The NBS is responsible for implementing monetary policy, supervising financial stability, regulating and overseeing banks, as well as protecting the interests of users of financial services.

[3] This law regulates the provision of payment services, including electronic money, payment cards, money transfers, and other electronic transactions. The aim of the law is to ensure the security, transparency, and efficiency of payment systems in Serbia.

[4] This law aims to prevent the abuse of the financial system for money laundering and terrorist financing purposes. It regulates the obligation of banks to apply appropriate measures for the identification, monitoring, and reporting of suspicious transactions.

located within the domestic territory. It must have a work permit (consent for establishment) from the National Bank of Serbia.

Its activities include performing deposit and credit operations (mandatory activities), and it may also perform other activities in accordance with the law (optional activities).

As I said before, banks are established exclusively in the legal form of a joint-stock company by domestic and foreign legal and natural persons (founders). The process of establishing a bank involves two phases: the first phase is the establishment of the bank in a narrower sense, and the second phase is the registration (i.e., legalization) of the bank (registration in the register of business entities), at which point the bank acquires the status of a legal entity (Carić, Vitez, Dukić Mijatović & Veselinović, 2016, pp. 112–113).

3. Digitization of Banking

The development of the information and communication sector influences dynamic changes in the economy, primarily transforming the banking sector. The effects are manifold, ranging from increased operational efficiency and reduced data processing costs to lowering service costs for customers (Raičević, Matijašević & Ignjatijević, 2012, p. 108).

Digital banking represents the application of digital technologies in providing financial services, enabling users to conduct banking transactions through digital channels such as the internet, mobile applications, and electronic platforms. This encompasses a wide range of activities, including account opening, financial management, payments, money transfers, investments, and obtaining loans, all through electronic devices.

It transforms the way banks communicate with their clients, providing them with greater flexibility, convenience, and speed in conducting financial transactions. Additionally, digital banking opens doors for innovations and new business models, offering users personalized experiences and products tailored to their specific needs.

In many developed countries, digital banking is currently experiencing rapid growth, with a trend towards establishing advanced e-banking transactions (Warf, 20018, p. 67).

The development of this type of banking can be traced through several key phases. Starting from the emergence of the first internet banking systems at the end of the 20th century, digital banking has experienced rapid growth and evolution over the past few decades. The development of mobile technologies and the expansion of internet access via smartphones have contributed to the

expansion of mobile banking, enabling users to conduct banking transactions wherever they are. Additionally, phenomena such as cryptocurrencies and blockchain technology have further expanded the horizons of digital banking, opening up new possibilities for secure and transparent transactions (Vijay & Chandrasekar, 2019, p. 11).

Digital banking involves conducting banking transactions through a direct connection between the client and the bank using specialized software. Thus, special software installed on the client's computer is required to perform transactions and store data on the changes made. (Stamatia & Angelos 2020, p. 145).

Banks utilizing digital banking enjoy numerous advantages, some of which are particularly significant. Establishing the image of an innovative company capable of offering its customers the latest technological solutions is crucial. Additionally, there are greater and better interactive possibilities – for a bank competing for each client in market conditions, communication with them is vital. There is also the potential for rationalizing the bank's potential – by transferring certain services to the internet, the bank reduces operating costs because it does not need to open new business premises, equip them, and hire new employees to increase the number of clients. This is especially interesting for geographic regions where the bank does not have a network of branches or has a small number of clients. Self-service banking is beneficial for both the bank and the client because the client has services available 24 hours a day, 7 days a week, while the bank operates 365 days a year without increasing the number of employees. By appearing on the internet, the bank proves its competitive capabilities and its development as a solid, stable, and technologically advanced company (Vuksanović, 2006, p. 218).

3.1. Legal Aspects of Digital Banking and Protection

Digital banking, as part of the digital transformation of the banking sector, is subject to strict regulation in Serbia to ensure security, transparency, and user protection. The main laws and regulations governing online banking include: Law on Electronic Document, Electronic Signature, and Data Protection in Electronic Business (2017) – This law regulates the rules of electronic business, including online banking, electronic transactions, and data protection.

Law on Personal Data Protection (2018) – This law prescribes rules for the processing and protection of personal data, which is crucial for online banking and user information security.

The National Bank of Serbia issues orders and guidelines related to online banking, including security standards, user identification procedures, risk management, and mandatory data protection protocols. These laws and regulations ensure that online banking in Serbia is under strict supervision and that banks adhere to the highest standards in user and data protection.

The security of digital banking in Serbia is ensured through the implementation of various security mechanisms:

User authentication is a highly successful mechanism. Banks use multi-factor authentication, such as username, password, one-time tokens, biometric data, or SMS confirmations, to ensure that only authorized users access their accounts.

Data encryption provides a higher level of security. All transactions and communications between users and banks are encrypted using strong encryption algorithms to protect data from unauthorized access. The encryption process can be likened to an "online safe."

Protection against cyber attacks is essential to prevent "online robbery." Banks implement security systems that detect and prevent cyber attacks such as phishing, malware, and DDoS attacks to protect users and their systems. Banks regularly update their software and systems to eliminate vulnerabilities and ensure that users have the latest security features (Komlen-Nikolić, et al., 2010, p. 45).

Banking systems are so complex, that it is essential for a court to fully understand the weaknesses to be able to assess the evidence when faced with dealing with disputed transactions involving ATMs and on-line banking (Mason, 2013, p. 1).

Protection of user data and privacy is a key component of online banking in Serbia, and banks are obliged to implement appropriate measures to protect the sensitive information of their users. Banks establish clear privacy policies that describe in detail how user data is collected, used, and protected, in accordance with legal requirements (Petrović, 2004).

Before collecting and processing user data, banks obtain user consent and clearly inform them of the purpose of data collection. Banks apply strict access controls to ensure that only authorized employees have access to sensitive user data. Bank staff are regularly trained on how to handle user data properly and how to recognize and respond to potential data security threats.

These security mechanisms, together with strict regulation, form the basis for user and data protection within digital banking in Serbia.

Unlike other criminals, cybercriminals use very smart techniques to prepare and commit crimes, making it very difficult to track them down. Detecting this

type of crime and gathering evidence against perpetrators is quite specific. Namely, due to the lack of physical evidence such as a body, blood, jewelry, fingerprints, etc., it is difficult to direct and conduct an investigation. Most cybercrime offenses are discovered accidentally or shortly after they occur, but still, the number of detected offenses is not negligible (Bjelajac, 2013, p. 296).

4. Challenges and Limitations of Digital Banking in Serbia

One of the main challenges of digital banking in Serbia is the lack of infrastructure and low digital literacy among the population. Although internet penetration is increasing, there is still a significant portion of the population that lacks access to the internet or mobile devices. Additionally, many users are not sufficiently trained or familiar with digital technologies, making them unprepared to use digital banking services. This situation creates barriers to the expansion of digital banking in rural areas and among older citizens who struggle to adapt to new technologies. Lack of infrastructure, such as fast and reliable internet connection, can also limit access to digital banking services in less developed regions.

Security risks and fraud pose a serious challenge to digital banking in Serbia. The rapid development of technology opens up new opportunities for cyber attacks, phishing, malware, and other forms of fraud. Users face the risk of identity theft, unauthorized access to their bank accounts, and misuse of personal data. Additionally, there is a risk of technical errors and system failures in online banking systems that can lead to data loss or financial losses. Banks are, therefore, under pressure to constantly improve their security measures and educate users about the latest threats and protection methods (Craig, 2012, p. 82).

Another challenge of digital banking in Serbia is the issue of access and inclusivity. While digital technologies enable greater accessibility to banking services, there are population groups that are marginalized or excluded from digital banking. This includes older people, people with disabilities, minority groups, and socially vulnerable communities who may not have access to or the ability to use digital channels. This lack of inclusivity can further deepen the financial inclusion gap and make it harder for economically vulnerable individuals to access banking services. Banks and regulatory bodies must work on developing strategies to ensure that digital banking is accessible to all citizens, regardless of their social or economic circumstances.

The legal framework for digital banking in Serbia faces challenges in terms of regulations that are not fully aligned with the rapid development

of technology. Existing laws, such as the Law on Payment Services and the Law on Electronic Document, Identification, and Trust Services in Electronic Business, provide a basis for regulating digital banking, but often lag behind technological innovations. This creates legal uncertainty and may slow down the further development of digital services.

The state, through the National Bank of Serbia and other regulatory agencies, plays a key role in setting the legal framework and supervising the banking sector. Central banks are mostly nationalized or under strict state control, directly interfering in the business activities that banks can engage in. This includes regulating interest rates, determining credit priorities, and ensuring financial system stability. In the context of digital banking, this regulation is particularly important for protecting users and preserving trust in digital banking services.

A cybercriminal's ability to use technology and exploit the Internet to directly access, manipulate and communicate electronic data is a basic challenge, in the commission of cybercrime and other illicit or criminal behaviours. Internet related technology can be used to commit crime either entirely within a technical environment, or to facilitate conventional crime by using various elements of networked technology (Hunton, 2012, p. 4).

Overcoming these challenges requires collaboration between banks, government authorities, regulatory bodies, technology companies, and civil society to ensure that digital banking in Serbia is safe, accessible, and inclusive for all citizens. Developing integrated strategies to improve infrastructure, increase digital literacy, and strengthen the legal framework is crucial for the long-term success of digital banking in Serbia (Kojić, 2015, p. 96).

5. Enhancement of Legal Regulation of Digital Banking

One of the key recommendations for improving legal regulation in the field of digital banking in is strengthening user protection. This could be achieved through enhancing transparency; banks should clearly communicate with users about the terms of using digital banking services, tariffs, risks, and user rights (Matijašević & Petrović, 2015).

Regulatory bodies should set strict standards for data and transaction security in digital banking, including mandatory implementation of multi-factor authentication and data encryption. Additionally, developing effective mechanisms for resolving disputes between banks and users of digital banking services to ensure fair and prompt solutions in case of issues is necessary to implement (Ferrari, 2022, p. 5).

The modernization of legislation and regulation itself is crucial for adapting to rapid changes in digital banking. The revision of existing laws, where regulatory bodies regularly review and update laws and regulations governing digital banking to respond to new technological and market trends, is essential. A more adaptable legal framework enables faster implementation of innovations and technological changes, thereby encouraging innovation and the development of new banking products and services. Authorities, in close collaboration with banks, FinTech companies, technology experts, and other stakeholders, develop optimal regulations for digital banking (Buckley, Arner & Zetzsche, 2023, p. 69).

Encouraging innovation and competition is crucial for the development of a dynamic and competitive digital banking market. Open API platforms would enable FinTech companies to develop innovative products and services that utilize banking data and infrastructure. Authorities can provide financial incentives, subsidies, or tax breaks for companies developing innovative solutions in the field of digital banking.

Ensuring fair competition in the digital banking market prevents monopolies and unfair practices, thereby promoting innovation and utilizing market competition to improve services and lower prices. To properly understand the channels through which digital banking can pose a threat to monetary sovereignty, it is important to introduce the two key design features of digital money: the stabilization mechanisms and the collateralization (Martino, 2024, p. 3).

These are some of the ideal conditions for creating a favorable environment for the development of digital banking in Serbia, encompassing all legal aspects, which will benefit both banks and the financial sector, as well as end-users of financial services.

6. Concluding considerations

Digital banking represents a key segment of the modern financial sector, which has a significant impact on how users access and utilize banking services. In Serbia, digital banking is experiencing growing expansion and development, bringing numerous benefits such as greater accessibility, efficiency, and innovation in delivering financial services.

However, despite these advantages, there are challenges and limitations that digital banking in faces. Lack of infrastructure and digital literacy, security risks and fraud, as well as issues of access and inclusivity, are key obstacles

that need to be overcome to ensure sustainable and inclusive digital banking for all citizens.

Therefore, enhancing legal regulation in the field of digital banking plays a crucial role in addressing these challenges and creating a favorable environment for further sector development. Strengthening user protection, modernizing legislation, and promoting innovation and competition are key recommendations that can contribute to improving digital banking.

Harmonizing domestic legislation with European standards, such as the PSD2 directive, can enhance the security and efficiency of digital banking. This includes stricter standards for user authentication and regulation of new services such as open banking.

The implementation and oversight of laws related to data protection, such as GDPR, are of paramount importance. It is necessary to ensure that banks implement the latest data protection standards and that users are adequately informed about their rights and ways to protect their data. The state and banks should invest in citizen education programs to increase digital literacy. This is particularly important for elderly citizens and residents of rural areas to reduce the digital divide and enable broader access to digital banking services. Regulatory bodies should ensure that digital banking is inclusive and accessible to all segments of society, including persons with disabilities, minority groups, and socially disadvantaged communities. This may involve developing accessible digital platforms and providing user support through various channels.

Collaboration between banks, regulatory bodies, government, and technology companies is crucial for addressing security issues and improving digital banking. Joint efforts to develop cybersecurity standards and protocols can reduce the risk of fraud and cyber attacks (Craig, 2012, p. 87).

Overcoming the challenges of digital banking in Serbia requires a holistic approach that includes legal, technological, and social aspects. With proper regulation, infrastructure strengthening, and increased digital literacy, digital banking can become a powerful tool for economic inclusion and enhancement of financial services in Serbia.

Global world can create a robust digital banking ecosystem that benefits all citizens and drives economic growth.

Srećković Jovan
Univerziteta Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

PRAVNI ASPEKTI DIGITALNOG BANKARSTVA

APSTRAKT: Brzi razvoj digitalnog bankarstva temeljno je promenio mogućnosti finansijskog sektora, pružajući niz novih prilika i izazova. Ovaj rad istražuje pravne aspekte transformacije finansijskog sektora putem digitalnog bankarstva. Analizira regulatorni okvir koji utiče na razvoj i implementaciju digitalnih bankarskih usluga, fokusirajući se na ključne zakone, propise i pravne standarde koji oblikuju ovo područje. Rad takođe adresira pitanja bezbednosti podataka, zaštite privatnosti, autentifikacije korisnika i odgovornosti u slučajevima prevare ili zloupotrebe. Istraživanje ima za cilj pružanje dubljih uvida u pravne izazove i prilike koje proizilaze iz digitalne transformacije finansijskog sektora, kao i identifikaciju mogućih pravnih okvira i strategija za unapređenje efikasnosti i transparentnosti digitalnog bankarstva. Rad se bavi i uticajem digitalnog bankarstva na tradicionalne bankarske prakse, uključujući pružanje usluga korisnicima, operativnu efikasnost i modele generisanja prihoda. Posebna pažnja posvećuje se ispitivanju implikacija digitalnog bankarstva za finansijsku inkluziju, posebno u nedovoljno servisiranim i udaljenim zajednicama, i njegovoj ulozi u podsticanju ekonomskog razvoja.

***Ključne reči**: Internet pravo, digitalno bankarstvo, privredno pravo, zaštita podataka.*

References

1. Bjelajac, Ž. (2013). *Organizovani kriminal* [*Organized Crime*]. Novi Sad: Univerzitet Privredna akademija, Pravni fakultet za privredu i pravosuđe
2. Buckley, R. P., Arner, D. W., & Zetzsche, D. A. (2023). *FinTech – Finance, Technology and Regulation*. Cambridge: University Press. DOI: 10.1017/9781108555640

3. Carić, S., Vitez, M., Dukić Mijatović, M., & Veselinović, J. (2016). *Privredno pravo* [*Commercial Law*]. Novi Sad: Fakultet za ekonomiju i inženjerski menadžment, Univerzitet Privredna akademija
4. Craig, B. (2012). *Cyberlaw – The Law of the Internet and Information Technology*. Harlow, UK: Pearson Education. DOI: 10.4324/9780203809570
5. Ferrari, V. (2022). The Platformisation of Digital Payments: The Fabrication of Consumer Interest in the EU FinTech Agenda. *Computer Law & Security Review*, *45*(1), pp. 71–86. DOI: 10.1016/j.clsr.2022.105561
6. Hunton, P. (2012). Data Attack of the Cybercriminal: Investigating the Digital Currency of Cybercrime. *Computer Law & Security Review*, *28*(2), pp. 201–207. DOI: 10.1016/j.clsr.2012.01.007
7. Kojić, M. (2015). Izazovi kompjuterskog kriminala, monografska studija [Challenges of Computer Crime, Monographic Study]. *Kultura polisa*, *12*(27), pp. 461–475
8. Komlen-Nikolić, L., Gvozdenović, R., Radulović, S., Milosavljević, A., Jeković, R., Živković, V., Zivanović, S., Reljanović, S., & Aleksić, I. (2010). *Suzbijanje visokotehnološkog kriminala* [*Suppression of High-Tech Crime*]. Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije
9. Madir, J. (2023). *FinTech Law and Regulation.* Cheltenham, UK: Edward Elgar Publishing. DOI: 10.4337/9781802209844
10. Martino, E. D. (2024). Monetary Sovereignty in the Digital Era: The Law & Macroeconomics of Digital Private Money. *Computer Law & Security Review*, *52*(1), pp. 119–36. DOI: 10.1016/j.clsr.2023.105632
11. Mason, S. (2013). Electronic Banking and How Courts Approach the Evidence. *Computer Law & Security Review*, *29*(2), pp. 144–151
12. Matijašević, J., & Petković, M. (2011). Krivična dela protiv bezbednosti računarskih podataka – analiza pozitivnih zakonskih rešenja i njihov značaj u kontekstu suzbijanja visokotehnološkog kriminala [Criminal Acts Against the Security of Computer Data – Analysis of Positive Legal Solutions and Their Importance in the Context of Suppressing High-Tech Crime]. In*:* Matijević, M. (ur.), *Zbornik radova sa međunarodne naučno-stručne konferencije "Kriminalističko-forenzička istraživanja"* [*Proceedings of the International Scientific and Professional Conference "Criminalistic-Forensic Research*"], (pp. 598–609). Banja Luka: Internacionalna asocijacija kriminalista
13. Raičević, V., Matijašević, J., & Ignjatijević, S. (2012). Ekonomski efekti i pravni aspekti elektronskog novca i elektronskog plaćanja [Economic

Effects and Legal Aspects of Electronic Money and Electronic Payment]. *EMC Review-Economy and Market Communication Review*, *3*(1), pp. 89–100. https://doi.org/10.7251/EMC1201089R

14. Stamatia, K., & Angelos, T. (2020). Digital Banking and Its Impact on Customer Experience. *International Journal of Bank Marketing*. *24*(3-4), 59–68
15. Vijay, K., & Chandrasekar, R. (2019). Digital Banking: A New Paradigm for Financial Services. *Journal of Financial Services Marketing*, *24*(3-4), pp. 59–68
16. Vuksanović, E. (2006). *Elektronsko bankarstvo* [*Electronic Banking*]. Beograd: Fakultet za bankarstvo, osiguranje i finansije, Beogradska bankarska akademija
17. Warf, B. (2018). *The SAGE Encyclopedia of the Internet*. Los Angeles: CA: SAGE Publications. DOI: 10.4135/9781473960367
18. Zakon o bankama [Law on Banks]. *Službeni glasnik RS*, br. 107/05 i 91/10
19. Zakon o deviznom poslovanju [Law on Foreign Currency Transactions]. *Službeni glasnik RS*, br. 62/06, 31/11, 119/12, 139/14 i 30/18
20. Zakon o Narodnoj banci Srbije [Law on the National Bank of Serbia]. *Službeni glasnik RS*, br. 72/03, 55/04, 85/05 – drugi zakon, 44/10, 76/12, 106/12, 14/15, 40/15 – odluka Ustavnog suda i 44/18
21. Zakon o ratifikaciji Konvencije o visokotehnološkom kriminalu [Law on Ratification of the Convention on High-Tech Crime]. *Službeni glasnik RS*, br. 19/09
22. Zakon o sprečavanju pranja novca i finansiranju terorizma [Law on the Prevention of Money Laundering and the Financing of Terrorism]. *Službeni glasnik RS*, br. 113/17, 91/19 i 153/20
23. Zakon o zaštiti podataka o ličnosti [Law on Personal Data Protection]. *Službeni glasnik RS*, br. 87/18