ITJ | The International Tax Journal

Digital banks in the Algerian banking system according to Law 23/09

ABDESSEMED Rima [1]

[1] Faculty of Law and Political Science, University of Batna 1, Algeria. Email: Rima.abdessemed@univ-batna.dz

Abstract---Algeria has, in recent years, adopted a strategy aimed at embracing banking digitization through the implementation of electronic payment systems and digital banks. However, the adoption of artificial intelligence in the banking sector raises a legal issue regarding the effectiveness of the legislative and regulatory framework in accommodating these developments. The use of AI-based programs in the banking sector, such as fraud detection, risk analysis, and liquidity management, is essential for achieving the transition toward digital banks. Nevertheless, this transformation requires effective protection of the intellectual property rights related to these intelligent systems, particularly with regard to data protection and trade secrets. This represents a legal challenge in ensuring adequate protection for the smart systems used in digital banks in Algeria.

Keywords---digital banks, banking digitization, legal challenges, cybercrimes.

Introduction

Technological development has impacted all fields, including economic, financial, and legal sectors worldwide. The banking sector is one of the most significantly affected areas by these changes. In this field, artificial intelligence is not merely a supportive technical tool but a means to develop financing instruments and banking digitalization. Consequently, banks are accelerating the development of their services to align with the requirements of the digital economy by relying on artificial intelligence technologies, whether in data analysis, combating money laundering and terrorist financing, among others. However, this digital transformation was preceded by amendments in legislative frameworks to keep pace with these applications, protect the involved parties on one hand, and encourage technological investment on the other.

How to Cite:
ABDESSEMED, R. (2025). Digital banks in the Algerian banking system according to Law 23/09. *The International Tax Journal*, *52*(6), 4539–4547. Retrieved from https://internationaltaxjournal.online/index.php/itj/article/view/434

The International tax journal ISSN: 0097-7314 E-ISSN: 3066-2370
Submitted: 14 March 2025 | Revised: 19 September 2025 | Accepted: 17 October 2025

Despite the importance of digital transformation in the banking sector, there remains a limited level of protection for financial transactions and the rights of parties involved worldwide. Therefore, the European Union countries have resorted to issuing an European Artificial Intelligence Regulation aimed at striking a balance between encouraging innovation and ensuring effective legal rules for protection.

Algeria, for its part, is seeking to modernize its banking system by incorporating digital banks and promoting the development of electronic payment. This is evident through the Monetary and Credit Law, in addition to regulatory texts related to the digitalization of financial services.

Despite the importance of adopting technology in the Algerian banking sector and the banking reforms introduced by the Algerian legislature, balancing the encouragement of banking innovation with the protection of all parties requires legal frameworks to keep pace with digital transformations and align with international standards.

Study problem

This raises the central issue: Does the Algerian legal framework keep up with technological transformations in the banking sector?

Study methodology

To address this issue, the study relied on the descriptive method by defining the purpose of digital banks and the mechanisms for adopting artificial intelligence within digital banks, as well as describing the legal challenges facing digital banks in Algeria. Additionally, the analytical method was employed through the analysis of various legal texts related to banks in Algeria.

To address this issue, a dual-structured approach was adopted. The first part focuses on artificial intelligence and banking operations in Algeria, addressing the applications of AI in the financial and banking sectors, as well as the implications of relying on AI in banking. The second part is dedicated to the legal challenges of keeping pace with technological transformations in the banking sector and their impact on banking operations.

1. Artificial Intelligence and Banking Operations in Algeria

The banking sector is a cornerstone of national economies and a key driver of economic development. Like other sectors, it has been significantly impacted in recent years by technological transformations. The integration of artificial intelligence (AI) technologies in banking operations has become an urgent step, driven by client demands, financial security requirements, and the competitive pressures on this sector. Consequently, the Algerian banking system is gradually moving towards adopting modern technologies in electronic payment, financial data management, and digital banking, influenced by the banking systems of developed countries. However, the application of modern technologies in the banking sector necessitates a legal framework capable of accommodating these transformations, in order to avoid potential negative repercussions that could directly impact national economies.

1.1 Applications of Artificial Intelligence in the Financial and Banking Sector:

Digital banks refer to credit institutions that rely on digital methods to provide banking and financial services. They are assigned the same tasks as traditional banks, such as opening accounts, accepting deposits, granting loans, and offering payment and transfer services. However, all these activities are conducted through electronic platforms (Maha Lakshmi,2019).

Often, the requirements for establishing digital banks involve obtaining a banking license from the central bank, along with the necessity of complying with standards related to data protection and privacy to safeguard customers. Additionally, they require protecting the digital consumer's access to

services through clear and accurate disclosure of service terms and fees, and establishing mechanisms for submitting complaints and resolving disputes via electronic means.

Digitization is the first stage of digital transformation, during which paper documents and customer signature forms are converted into digital format, allowing computers to recognize and process them. This is followed by the second stage, known as the visual representation stage, which involves creating online communication channels that enable customers to interact with the bank. The third stage of the digital transformation journey is where the bank's functions are transformed thanks to new models that rely on physical equipment, software, the internet, and other electronic networks, in addition to new digital technologies such as artificial intelligence, cloud computing, and blockchain.

However, the success of digital transformation in banks is linked to digital resources, which consist of digital capabilities encompassing information and communication infrastructure, along with information storage tools aimed at enhancing banks' analytical capabilities and maximizing the benefits of modern technologies. These technologies are designed to combat money laundering, as well as include chatbots intended for customer communication.

1.1.1. **The Role of Digital Resources in Combating Money Laundering:**

The threat of money laundering to global markets has increased with the emergence of technology, leading many countries to rely on modern technologies such as artificial intelligence to combat money laundering at the international level. According to the European Committee's 1990 guide, money laundering is defined as "the process of converting money or assisting a person who has committed a crime to avoid legal responsibility and retain the proceeds of that crime."(Abd al-Nabi Muhammad Ahmad, 2010) Therefore, money laundering involves resorting to illegal and unethical sources to make it appear as if the earnings were obtained through legal and legitimate means (Hiba Sahnoon, Kheireddine Bouzrib, 2020).

The methods of money laundering operations in banks vary according to technological development. Traditional methods relied on depositing and transferring money to a bank located abroad, or re-borrowing through depositing illicit funds in a foreign country characterized by stability, the absence of income taxes, and a lack of stringent banking supervision. Subsequently, the individual establishes shell companies and then requests loans from local banks in other countries.

Additionally, among the traditional methods of money laundering is relying on forged invoices in the field of import and export by purchasing goods and selling them while inflating the value of the goods and services listed on the invoice. The difference represents the laundered money (Fatimah Miftah, Ahmed Ali Al-Kadeeki, Hanan Musa Al-Abidi, 2024).

Regarding modern methods of money laundering in the banking sector, they involve the use of electronic money, electronic checks, as well as the use of gambling clubs or electronic cards (Fatimah Miftah, Ahmed Ali Al-Kadeeki, Hanan Musa Al-Abidi, 2024).

Therefore, banks rely on modern standards in addition to traditional ones to confront this phenomenon. Banks are committed to adopting internal standards aimed at knowing customers and rigorously monitoring accounts and transactions that are suspicious. This is achieved by verifying customer identities, tracking movements and transactions, in addition to continuously monitoring accounts that involve risks to identify unusual operations and transactions and their economic justification. In the event of any suspicions, the bank or financial institution is obligated to close the account and notify the Financial Intelligence Processing Unit and the Banking Commission, while continuously updating all available data (Fadhila Boutoura, 2022). The purpose of collecting customer information is to assess loan risks, detect money laundering, and combat fraudulent activities.

Artificial intelligence technologies are used in combating money laundering through data analysis. This is done by analyzing financial, economic, and banking data to detect unusual and suspicious activities in financial operations, particularly concerning domestic and international transfers, in addition to identifying suspicious economic and financial patterns with the aim of alerting these financial institutions and detecting transactions. This enables financial and banking institutions to verify transactions, take necessary measures, and identify beneficiary customers. Indeed, artificial intelligence allows for the analysis of financial records and the identification of customers involved in money laundering operations (Muhammad Al-Sadiq Abdullah Muhammad, Suleiman Muhammad Al-Hamed, Saad Mamoun Abdulrahman Abu Alwan, 2024).

Combating money laundering stops the generation of income through illegal activities. Therefore, most countries around the world are turning to adopting artificial intelligence instead of rule-based systems to combat money laundering. The results achieved in fighting fraud and deception using artificial intelligence are accurate and effective. An example is the FICO FALCON Fraud Scoring System, which relies on a neural network to deploy advanced artificial intelligence systems based on deep learning (Hiba Sahnoon, Kheireddine Bouzrib, 2020).

1.1.2 Chatbots:

These chatbots aim to respond to customer inquiries sent through electronic platforms, providing immediate answers to their questions. Among the most prominent inquiries sent to chatbots are questions about bank branch working hours, foreign exchange rates, and account balance inquiries

The Consumer Financial Protection Bureau (CFPB) in the United States of America has revealed that the use of chatbots is beneficial in responding to basic customer inquiries. However, the effectiveness of this role diminishes if the legal system is unable to keep pace with this development, as chatbots may pose risks to security and privacy, which affects customer trust(CFPB, 2023).

They are specialized programs designed to interact with humans, providing information and answering questions. Two prominent successful examples of chatbots are: Ceba: This is a chatbot affiliated with Comm Bank (CBA). It offers various services to customers through branches in the United States of America, Australia, Asia, and parts of Europe. The bank relies on this chatbot to respond to customer inquiries and provide assistance via mobile phones. The customer receives a message from the chatbot notifying them that it is ready to answer any banking-related questions, while keeping the conversation confidential. The user is required to provide the chatbot with some personal data, such as a phone number and identification (Ionuţ-Alexandru CÎMPEANU, Denis-Alexandru DRAGOMIR, Răzvan Daniel ZOTA, 2023).

The second example of the most successful chatbots today is Citi Bot SG, a conversational program affiliated with an American bank that has offices in the United States of America, India, Mexico, and Europe. It relies on text messages to interact with users, providing features such as granting information about the account balance, transactions conducted, upcoming payments, and the user's debts with the bank. Not only that, but it also awards points as gifts for conducting more transactions and banking operations. Additionally, it offers innovative digital loans to customers, assisting them in their economic activities while providing accurate information about the economic sector the user requires (Ionuţ-Alexandru CÎMPEANU, Denis-Alexandru DRAGOMIR, Răzvan Daniel ZOTA, 2023).

One of the advantages of chatbots is continuous communication with customers and obtaining easy and quick answers without the need to visit the bank. It contributes to saving time and effort for both the bank and the customers. It also reduces service expenses, redirecting funds towards other investments and profits. Furthermore, it provides the feature of communication even outside working hours, provided there is an internet connection. Additionally, the chatbot helps complete transactions in a short time, which helps eliminate waiting queues.

1.2 Legal Texts Regulating Banking Digitalization in Algerian Legislation

In recent years, Algeria has adopted a strategy aimed at embracing banking digitization through the adoption of electronic payment systems, the introduction of digital banks, and the development of innovative financial tools. However, the adoption of artificial intelligence in the banking sector raises legal concerns regarding the effectiveness of the legislative and regulatory framework in accommodating these changes.

1.2.1 Digitization of Banking Services under Law 23-09, the Law on Money and Banking

The Algerian legislator has pursued the digitization of banking services by updating the monetary and banking law and issuing regulations concerning digital banks and electronic payments. However, this framework lacks precise provisions for data protection or the assessment of ethical risks. In contrast, the approach in France has involved the Prudential Supervision and Resolution Authority (ACPR) and the Bank of France issuing guidance documents that establish controls for the use of artificial intelligence, with a focus on monitoring model performance after deployment. These controls are aligned with the General Data Protection Regulation (GDPR) and digital financial systems legislation, alongside the European AI Act, which classifies the use of AI in loan granting as high-risk, thereby necessitating stringent oversight and a higher level of transparency.

The Algerian legislator has provided for the possibility of establishing financial institutions that offer their services through electronic means under Law No. 23-09, issued on June 21, 2023, concerning Money and Credit. This type of bank is subject to the supervision of the Bank of Algeria and is obligated to comply with cybersecurity standards and customer data protection requirements.

The Algerian legislator aims to enhance the stability of the financial system by introducing new powers for the Bank of Algeria, as well as newly established committees, to prevent any financial crisis. Regarding payment methods, the legislator has established a committee dedicated to studying and examining means and mechanisms that facilitate banking and payment operations. This committee is named the National Payment Committee. It is responsible for developing a suitable national strategy for advancing written payment methods, which contributes to keeping pace with banking and financial developments, particularly by relying on electronic payment methods.

The primary objective of Law 23/09 is to establish procedures that contribute to the stability of the financial system, alongside addressing liquidity issues and combating inflation (Henni Abdel Salam, Seghir Birem Abdel Majid, 2024)

1.2.2 Electronic Payment under Law 18-05

The Algerian legislator has recognized electronic contracts while guaranteeing the confidentiality of consumer financial data. The foundations and procedures for electronic payment were defined by Law 18-05, dated May 10, 2018, on Electronic Commerce. Articles 5, 8, and 14 of this law mandate the disclosure of the electronic operator's identity and ensure the protection of consumer data during network-based payments. Furthermore, Instruction No. 01/2020 established mobile payment, enabling the provision of secure digital payment services through the use of the Carte Gold (Gold Card) and online bank payment platforms.

Law 18-05 established the general rules governing electronic commerce for goods and services. Online banking is considered the most important form of electronic banking. This was achieved through the creation of an institution to assist Algerian banks, called Algeria Islamic Banking Services Company (Algeria Islamic E-Banking Services Company), which aims to modernize banking services and electronic payment systems (Boaza Hidaya, 2020).

What can be observed from this law is that Algeria has adopted and utilized technology in its banking system through the implementation of electronic payment systems in Algerian banks. However, the reliance on electronic payment tools remains limited.

2. **Legal Challenges of Transitioning to Digital Banking in Algeria**

The aim of the transition to digitization in the banking sector is to improve the quality of services in Algeria and reduce reliance on cash transactions. However, despite its importance, this transition faces legal, technical, and economic challenges, in addition to the most prominent challenge: digital user culture. Algerian banks still face obstacles related to updating technological systems to ensure the protection of customer data and encouraging society to adopt digital usage. This would contribute to an effective and globally aligned digital banking transformation. Nevertheless, our current study focuses on the legal challenges facing the transition to digital banking in Algeria.

2.1 **Protection of Intellectual Property for Smart Systems in Algeria**

Relying on artificial intelligence programs in the banking sector for fraud detection, risk analysis, liquidity management, and other purposes is essential for transitioning to digital banks. However, this transition requires effective protection of the intellectual property rights of these smart systems, particularly concerning data protection and trade secrets.

2.1.1 **Limited protection through copyright**

Computer-related software is protected as literary and artistic works. "Software" refers to a set of instructions expressed in words, symbols, diagrams, or any other form, which aids in performing a specific task or achieving a particular result. This information is readable by a machine and translatable through electronic or similar means (Usama bin Yattu, 2015).

Computer programs consist of operating systems, known as system software, as well as application programs, which enable the computer to perform specific functions. Computer programs are intellectual works that enjoy legal protection under copyright law, as they are considered literary and artistic works based on the creative nature of their programming structure. This protection covers the source code, which is written in a programming language understandable by programmers, and the object code, which represents the binary or machine-readable format understood by the computer.

Accordingly, any copying, modification, reproduction, or translation of these codes without the authorization of the rights holder constitutes copyright infringement, leading to civil and criminal liability in accordance with national legislation and international conventions, particularly the Berne Convention for the Protection of Literary and Artistic Works and the TRIPS Agreement. This is affirmed by the Algerian legislator, which recognizes software as being protected under the same provisions granted to literary works, without requiring registration or deposit as a condition for legal protection, pursuant to Law No. 03/05 on Copyright and Related Rights.

Infringement upon the source code or object code of computer programs entails legal liability, depending on the severity of the act and its intended purpose. From a civil perspective, copying, modifying, reverse-engineering, or making a program available to others without the rights holder's authorization constitutes an infringement of literary and artistic property rights. This entitles the author or the holder of economic rights to claim compensation for both material and moral damages resulting from the infringement, in addition to demanding the cessation of unauthorized use and the withdrawal of counterfeit copies from circulation.

From a criminal standpoint, the legislator considers such an act as software counterfeiting or piracy—a crime punishable by fines, imprisonment, or both, as it violates the author's rights and infringes upon the economic exploitation rights of the program. Liability may also extend to parties benefiting from the use of an unauthorized copy, even if they did not commit the act of copying themselves.

The importance of this liability is particularly evident in the professional and banking sectors. Financial institutions rely on sensitive software systems, and any infringement upon their code poses risks to service continuity, data integrity, and information confidentiality. Therefore, legal protection for software is essential to ensuring information security and the technical stability of institutions.

In contrast, the European Court of Justice (ECJ) and the European Union provide broad protection covering both source code and object code. In a ruling dated May 2, 2012, the ECJ held that protection is not limited to source code alone but also extends to object code, along with the program's structure and internal organization, provided that they possess a creative character. The Court concluded that **"the subject matter of protection includes, in any form, a computer program such as source code and object code, which enables the reproduction of the program in different computer languages."** (Court of justice of the European union,2012)

2.1.2 **The Inadequacy of Patent Law for Protection**

Protection under a patent is applicable when a technical invention, adopted by banks nationwide after being developed, offers a new technical solution. In this case, protection is granted under patent law. Although Algerian patent law provides protection for technological innovations, this protection is partial and insufficient for artificial intelligence inventions in the banking sector. This is due to the evolving nature of AI, where the law attributes inventorship to a human, whereas in the case of AI, the inventor may be the system itself. This leads to a gap in protection under the patent regime as stipulated in Ordinance 03/07 on Patents. Additionally, the procedures for examining and protecting an invention through a patent require a timeframe that can extend to a year or more, which is incompatible with the nature of inventions in the banking sector, as the value of a banking innovation may diminish over such a period.

Despite the technical development of digital banking services in Algeria, patent law remains inadequate in providing effective protection for software innovations related to banking transactions, particularly those involving electronic payment systems or cybersecurity applications. The reason for this inadequacy is that Algerian patent law excludes software from patent protection, which weakens the competitiveness of banking institutions and exposes them to piracy and unauthorized exploitation.

2.2 **Inadequate Protection under the Law on Cybercrime**

The banking sector in Algeria is undergoing a rapid transformation toward digitization, relying on electronic banking services and the development of digital payment systems, which has contributed to facilitating financial transactions. However, this technological advancement has been accompanied by an increase in cybersecurity threats, particularly those related to electronic fraud, information system breaches, and payment method forgery. In this context, Law No. 09/04, pertaining to the prevention and combating of information and communication technology-related crimes, is considered the foundational framework for combating various electronic crimes that may target digital banks.

2.2.1 **Preventive Measures for Monitoring Electronic Communications**

This law focuses on preventing and suppressing digital crimes. It supplements the penal code by providing a legal framework specifically designed to address the unique aspects of cybercrimes, defining the procedural safeguards for combating them. However, it is insufficient to protect the banking sector in light of the increasing number of cybercrimes and the evolution of their methods. Therefore, it is essential to establish comprehensive principles and guidelines that precisely define cybercrimes, specify how to investigate them, and outline the procedures for handling them (Boudjelal fatma zohra, 2025)

To prevent the proliferation of cybercrime, the Algerian legislator established the National Judicial Center for Combating Information and Communication Technology-Related Crimes. This is achieved through the surveillance of electronic communications, including their monitoring (Ajaoud Saad,2022) review, and interception. However, according to Article 4 of Law 09/04, such surveillance is permitted

only for the prevention of acts classified as terrorism, sabotage, or crimes against state security; or when there is information indicating a potential threat to an information system that jeopardizes public order, national defense, state institutions, or the national economy; or when required for judicial investigations and inquiries where it is difficult to achieve results relevant to ongoing investigations without resorting to electronic surveillance. Electronic surveillance may also be employed in the execution of requests for international mutual legal assistance.

2.2.2 **Mechanisms for Combating Cybercrime in the Banking Sector**

Article 3 of Law 09/04 refers to the inspection procedure for protecting public order and judicial investigations. Inspections can be conducted within an information system. Remote inspection is carried out in two cases: first, of an information system or part thereof, and second, of the information data stored within it. During the inspection process, any person knowledgeable about the operation of the information system under investigation or the measures taken to protect the information data it contains may be enlisted to assist (Samiha Belkacem, Hamid Bouchoucha, 2023), Seizure may also be resorted to, whether it involves physical computer components or copies of data under investigation, as stipulated in Articles 6 and 7 of Law 09/04.

Conclusion

This study discusses the legal challenges of protecting smart systems used in digital banks in Algeria, by examining the adequacy of frameworks related to copyright, patents, trade secrets, and the law concerning information technology crimes, particularly in light of the specific challenges posed by artificial intelligence. Based on the preceding analysis, we conclude that:

- The success of the digital transformation process in banks requires providing digital resources, primarily consisting of information and communication infrastructure, along with data storage tools. The purpose of these resources is to support banks' analytical capabilities and maximize the benefits of modern technologies. Among the most important digital technologies relied upon during digital transformation in banks is artificial intelligence, manifested in Mobile Banking technology, through which funds are transferred from one bank account to another.
- Although Algeria's patent law provides protection for technological innovations, this protection remains partial and insufficient for artificial intelligence inventions in the banking sector, due to the nature of artificial intelligence.
- Law 23-09 constitutes a fundamental pillar for combating cybercrimes that threaten digital banks in Algeria. However, it does not achieve comprehensive protection on its own, as it focuses on criminalization and punishment without providing a detailed regulatory framework for digital banking services, data security, and the use of artificial intelligence in banking transactions.
- herefore, genuine legal protection for digital banks requires the integration of this law with the Personal Data Protection Law, intellectual property legislation, and the directives of the Bank of Algeria concerning digital transformation and cybersecurity.

Accordingly, we propose a set of recommendations:

- Developing an intellectual property legal framework that keeps pace with artificial intelligence innovations in banking systems.
- Enhancing a culture of digital prevention within banks by training employees and improving monitoring and tracking systems.
- Therefore, it can be said that Law 23-09 represents a fundamental stage in protecting digital banks, but it is insufficient on its own to ensure the security of this vital sector amidst the acceleration of cybercrimes and the evolution of their tools. Hence, a comprehensive legislative approach is required, based on integrating punitive legislation, regulating digital banking services, data protection, and cybersecurity.

References

Abd al-Nabi Muhammad Ahmad, Al-Raqaba al-Masrifiyya (Banking Supervision), Zamzam Publishers and Distributors, Jordan, 2010.

Ajaoud Saad, Majallat Al-Risala lil-Dirasat wal-Buhuth Al-Insaniya, Al-Mujallad 07, Al-'Adad 04, Juwan 2022, pp. 2014-234

Boaza Hidaya, Al-Daf' al-Iliktroni fi al-Qanun al-Jaza'iri Majallat al-Dirasat al-Qanuniyyah al-Muqaranah Al-Mujallad /60, Al-'Adad 60 ,2006,, pp. 195-219.

Boudjelal fatma zohra, Crimes Associated with ICT and Communication Technology: Preventive Measures (In Accordance with Law No. 09-04 on the Prevention and Suppression of Offenses in the Digital Domain), Algerian Journal of Law And political Sciences - Volume 10, Issue 01(2025) - p. 1116/1128

Fatimah Miftah, Ahmed Ali Al-Kadiki, Hanan Musa Al-Abeedi, "Dawr Al-Āliyāt Al-Muḥāsabiyyah li Al-Ḥawkamah fī Al-Ḥadd min 'Amaliyyāt Ghassīl Al-Amwaāl The Role of Accounting Mechanisms of Governance in Limiting Money Laundering Operations, Majallat Al-Dirāsāt Al-Iqtiṣādiyyah, Kulliyat Al-Iqtiṣād, Jāmi'at Surt, 2024, Volume 07, Issue 02, pp. 117-142

Fadhila Boutoura, Ijra'at Muwajahat Jarimat Ghassil al-Amwal fi al-Jihaz al-Masrifi al-Jaza'iri: Taqrir Bahthi Qanuni, Procedures for Confronting Money Laundering Crimes in the Algerian Banking System: A Legal Research Report, Al-Majallah al-'Arabiyyah al-Qanuniyyah li 'Ulum al-Shari'ah wa al-Qanun, 2022, Issue 01, Volume 01, pp. 141-160.

Henni Abdel Salam, Seghir Birem Abdel Majid, Magazine Dafatir Al-Huqooq wa Al-Ulum Al-Siyasiya (Notebooks of Law and Political Sciences) Al-Markaz Al-Jami'i M'ghnia (Maghnia University Center) Volume: 04 / Issue: 02 (2024), pp. 26–45.

Hiba Sahnoon, Khair Eddine Bouzeraâb, Al-Thatakka' al-Isstina'i wa Tatbeeqatuh fi al-Qita' al-Masrifi: Qira'a fi al-Tajriba al-Hindiyya ma' Dirasat Halat Bank HDFC (Artificial Intelligence and Its Applications in the Banking Sector: A Look at the Indian Experience with a Case Study of HDFC Bank), in: Collective Book titled Tatbeeqat al-Thatakka' al-Isstina'i ka Ittijah Hadith li Ta'ziz Tanafusiyyat Munaththamât al-A'mal, February 2020, pp. 149-169.

Ionuţ-Alexandru CÎMPEANU, Denis-Alexandru DRAGOMIR, Răzvan Daniel ZOTA, Banking Chatbots: How Artificial Intelligence Helps the Banks, published by Sciendo, 2023, p-p, 1716-1727

Maha Lakshmi, M. Kavitha, ADALYA JOURNAL, Volume 8, Issue 10, October 2019, 435-439, researchgate.net/publication/376602146_A_Study_On_Digital_Banking_and_its_Impacts

Muhammad al-Sadiq Abdullah Muhammad, Sulayman Muhammad al-Hamid, Saad Ma'moun Abd al-Rahman Abu 'Alwan,Dawr al-Tiqniyah fi al-Tadabir al-Wiqai'iyyah li Mukafahat Jarimat Ghasil al-Amwal,The Role of Technology in Preventive Measures to Combat Money Laundering Crimes, Al-Majallah al-Dawliyyah fi al-'Ulum al-Qanuniyyah wa al-Ma'lumatyyah, Volume 4, Issue 01, 2024, pp. 11-19.

Samiha Belkacem, Hamid Bouchoucha, Cyber Crime: A New Dimension of Crime in Algeria: Its Reality and Mechanisms to Confront it, Majallat Al-Ulum Al-Insaniya li-Jami'at Umm Al-Bawaki, Al-Mujallad 10, Al-'Adad 01, Juwan 2023,pp. 532-566

Usama bin Yattu, Himayat Barmaj al-Hasub al-Ali bayna Nizamay Huquq al-Mu'allif wa Barā'at al-Ikhtirā, Protection of Computer Programs Between Copyright and Patent Systems, A Thesis Submitted to Obtain a Master's Degree, Specialization: Intellectual Property Law, University of Batna, 2015. CFPB warns AI chatbots in banking must comply with law, https://bankingjournal.aba.com/2023/06/cfpb-warns-ai-chatbots-in-banking-must-comply-with-law

Intelligence artificielle pour le secteur financier, https://acpr.banque-france.fr/fr/publications-et-statistiques/publications/intelligence-artificielle-enjeux-pour-le-secteur-financier

Court of justice of the European union, SAS institute Inc, v World programming Ltd, Case C-406/10, Judgment of 2 May 2012, https://curia.europa.eu/juris/liste.jsf?num=C-406/10