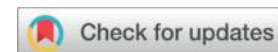




Legal Challenges of the Use of Artificial Intelligence in Financial Services

Dr. Narimane SIHAMDI



University Frères Mentouri Constantine 1, Faculty of Law, Algeria

Email: Sihamdi-narimane@hotmail.com

 <https://orcid.org/0009-0004-6764-6874>

Submission : 05/04/2026

Acceptation : 09/10/2026

Publication :10/10/2026

Abstract:

The use of artificial intelligence in financial services has expanded rapidly due to its ability to enhance efficiency and improve the accuracy of decision-making processes. However, this development also raises significant legal and regulatory challenges that require careful consideration.

Key issues include the protection of personal data, particularly in relation to its collection, processing, and cross-border transfer within increasingly complex and evolving legal frameworks. Transparency and explainability also represent major concerns, as many artificial intelligence systems operate as “black boxes,” limiting their interpretability and raising serious questions regarding legal accountability.

In addition, algorithmic bias, often resulting from unbalanced or historically distorted datasets, may lead to discriminatory outcomes that undermine the principle of equality in financial services. Cybersecurity risks further intensify these challenges, especially given the growing sophistication of attacks targeting AI-based systems. Moreover, determining legal liability remains particularly complex due to the multiplicity of actors involved in the development and deployment of artificial intelligence technologies.

This article concludes that there is a pressing need for flexible and coherent regulatory frameworks capable of balancing technological innovation with the protection of fundamental rights and legal certainty in the financial sector.

Key Words: Artificial Intelligence (AI); Financial Services; Legal Challenges; Financial Innovation; Cybersecurity.

1. Introduction:

The integration of artificial intelligence (AI) into financial services represents a profound structural transformation that is reshaping the operational foundations of the banking and financial industries. This evolution is not merely technological in nature; it also places legal systems in direct engagement with the probabilistic and adaptive characteristics of contemporary AI models.

Artificial intelligence is increasingly redefining the financial sector by improving decision-making processes, enhancing fraud detection mechanisms, automating customer onboarding procedures, and enabling a high degree of personalisation in financial products and services tailored to individual client profiles.

Despite these significant advantages, the deployment of AI technologies gives rise to substantial legal and regulatory challenges. Central among these is the need to ensure compliance with existing legal frameworks governing financial activities and data processing. In this context, issues relating to data protection and the explainability of “black-box” systems have become particularly salient, as such models may fail to provide sufficient legal justification for automated decisions affecting individuals’ rights and interests.

Moreover, the absence of a unified regulatory framework has led to a fragmentation of applicable rules across multiple legal instruments, thereby complicating regulatory compliance for financial institutions. These challenges are further compounded by the emergence of increasingly stringent international standards, notably the European Union Artificial Intelligence Act, which classifies key financial applications—such as creditworthiness assessment—as high-risk systems, subject to enhanced requirements concerning governance, transparency, accountability, and human oversight.

Accordingly, financial institutions are required to comply with complex and evolving regulatory obligations aimed at safeguarding consumers, combating financial crime, preserving systemic trust, and strengthening transparency. However, the rapid pace of AI development continues to outstrip the capacity of both regulators and institutions to ensure adequate legal adaptation.

Against this background, this study seeks to answer the following research question:
What are the principal legal challenges arising from the use of artificial intelligence in financial services?

2. Legal and Regulatory Challenges Relating to Data

Data constitute the fundamental cornerstone for the development of artificial intelligence systems in the financial sector. However, they also give rise to complex legal and regulatory challenges, primarily related to data quality, privacy, and ownership. On the one hand, the development of effective AI models requires access to high-quality data that are accurate, comprehensive, and standardized. Any deficiency in these characteristics may lead to

misleading outcomes or inaccurate decisions, thereby adversely affecting the stability of financial transactions and undermining user confidence in financial services.

On the other hand, increasing concerns have emerged regarding the risks associated with what is commonly referred to as *data poisoning*. This occurs when datasets are deliberately manipulated during the training phase, compromising the integrity, reliability, and robustness of AI models. Such practices may significantly impair the performance of financial AI systems and expose institutions to legal, operational, and reputational risks.

Neural networks, Large Language Models (LLMs), and Deep Learning models rely extensively on the quality, integrity, and reliability of training data, as these elements ultimately determine the functionality and performance of the model. Such data may originate from a variety of sources, including the Internet, governmental databases, and third-party data providers. By introducing inaccurate, manipulated, or biased information—commonly referred to as poisoned data—into training datasets, malicious actors may alter a model’s behavior either subtly or significantly.⁽¹⁾

For instance, data poisoning may lead to the misclassification of information, thereby reducing the efficiency, accuracy, and reliability of artificial intelligence and machine-learning systems. Moreover, such attacks may generate serious cybersecurity risks, potentially compromising the security and resilience of financial infrastructures that increasingly depend on AI-driven technologies.

In addition, the protection of personal data raises further legal concerns, particularly in relation to the unauthorized collection, processing, or use of personal information. These concerns are exacerbated by the fragmentation of existing regulatory frameworks and, in certain cases, by their inability to adequately address the activities of non-bank entities operating within the evolving financial ecosystem.

In this context, there is a growing doctrinal and regulatory trend advocating a shift from an “opt-out” system⁽²⁾, which presumes implicit consent, towards an “opt-in” model⁽³⁾ based on explicit consent, thereby strengthening consumer protection and reinforcing individuals’ effective control over their personal data.⁽⁴⁾

In addition, the cross-border transfer of data constitutes a further significant challenge, raising concerns related to national security and compliance with international legal standards. This situation calls for a reconsideration of existing regulatory frameworks in order to ensure a

¹- Tom Krantz, Alexandra Jonker, What is data poisoning?, <https://www.ibm.com/think/topics/data-poisoning>, consulted on: 02/03/2026.

²- In this system, the customer is presumed to give implicit consent to the use of their data, unless they subsequently choose to opt out.

³- In this system, the customer is deemed to have provided implicit consent to the use of their data, unless they subsequently choose to object or withdraw such consent.

⁴-Samuel Goldstein, Opt-in et opt-out : les règles de consentement à respecter, 2021, <https://www.legalplace.fr/guides/opt-in-opt-out/>, consulted on: 02/03/2026.

careful balance between fostering technological innovation and protecting individuals' fundamental rights.

Moreover, a strand of legal scholarship argues that current data protection frameworks may be insufficient to keep pace with the increasing complexity introduced by the deployment of artificial intelligence, particularly with regard to data collection, processing, and subsequent reuse practices.

A review of recent Algerian legislative instruments, in particular Law No. 25-11 ⁽¹⁾ of 24 July 2025, which amends and supplements Law No. 18-07⁽²⁾ on the protection of natural persons in the processing of personal data, indicates that the Algerian legislator has begun to establish a regulatory framework that is increasingly aligned with technologies related to artificial intelligence, even though no fully autonomous and dedicated legal regime has yet been enacted for this purpose.

The alignment of Algerian law with the use of artificial intelligence is reflected in the following academic and legal considerations:

2.1. Legal Framework for Identifying Personal Attributes

Personal attributes are considered sensitive information, as they may reveal an individual's personality, preferences, or capabilities. They constitute a fundamental basis for the functioning of artificial intelligence algorithms. Algerian law defines automated processing, under Article 03 of Law No. 18-07, as **“operations performed wholly or partially by automated means, such as recording data, applying logical and/or arithmetic operations to such data, modifying, deleting, retrieving, or disseminating it”** This encompasses any form of automated processing of personal data used to evaluate certain aspects relating to a natural person, particularly for the analysis or prediction of elements concerning their professional performance, economic situation, health, or location, this definition is substantially consistent with the concept of **“Data Profiling”**⁽³⁾ in artificial intelligence systems.

2.2. Protection Against Fully Automated Decision-Making

Algerian law imposes strict limitations on decision-making processes based solely on artificial intelligence systems, as follows:

¹- Law No. 25-11 amending and supplementing Law No. 18-07 on the protection of natural persons with regard to the processing of personal data, dated 24 July 2025, Official Gazette No. 48, issued on 24 July 2025.

²- Law No. 25-11 amending and supplementing Law No. 18-07 on the protection of natural persons with regard to the processing of personal data, dated 24 July 2025, Official Gazette No. 48, issued on 24 July 2025.

³- **Data profiling**, sometimes referred to as “preliminary data mining” or “data archaeology,” is the process of examining and cleansing data in order to better understand its structure and to maintain data quality standards within a financial institution. The primary objective of this process is to obtain a clear overview of data quality by applying methods of review, summarisation, and assessment. This task is typically carried out by data engineers who rely on a combination of business rules and analytical algorithms.

- Prohibition of fully automated adjudication: Article 45 bis 1 of Law No. 25-11 stipulates that “**judicial decisions requiring an assessment of a person’s conduct may not be based solely on the automated processing of data...**”.
- Legal effects: As provided in Article 45 bis 1(2), no decision producing legal effects concerning an individual may be taken solely on the basis of “automated processing” intended to determine aspects of their personality or to evaluate certain dimensions of their behaviour.
- Exception: Article 45 bis 1(3) introduces an exception allowing automated processing where it is necessary for the conclusion or performance of a contract, provided that the data subject has been given the opportunity to present their observations, as well as in cases where decisions are taken in response to the data subject’s request.

2.3. Mandatory Data Protection Impact Assessment for Emerging Technologies

When new technologies—such as artificial intelligence—are used in data processing operations that are likely to result in a high risk to individuals’ rights and freedoms, Law No. 25-11 requires, under Article 45 bis 6, that the data controller conduct a prior “impact assessment” before initiating the processing activity. This assessment is designed to evaluate potential risks and to identify the necessary security and mitigation measures required to address them. It thereby enables the development of innovative digital financial solutions while simultaneously ensuring the protection of privacy rights.

2.4. Strengthening Oversight and Transparency

Law No. 25-11 introduced, pursuant to Article 04 amending and supplementing Law No. 18-07, a new Chapter One bis establishing the role of the “**Data Protection Officer**” Under Article 41 bis, this officer is appointed on the basis of professional qualifications and expertise, particularly in law and practices relating to personal data protection. Article 41 bis 1 further provides that the Data Protection Officer is responsible for raising awareness among data controllers and employees regarding their obligations under the law, as well as providing advisory support upon request.

This mechanism contributes to ensuring that financial institutions comply with best practices in the protection of users’ personal data and enhances overall transparency and regulatory oversight.

Article 45 bis 7 further requires data controllers to implement appropriate internal technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorised disclosure, or unauthorised access. This requirement is particularly crucial for the development and expansion of AI-driven financial services.

This regulatory framework renders Algerian law broadly aligned with the requirements governing the use of artificial intelligence, insofar as it seeks to strike a balance between technological development and the protection of individuals’ fundamental rights. In its underlying philosophy, it is closely aligned with the principles of the European General Data

Protection Regulation (GDPR). However, the legal framework still requires further refinement in order to enhance the protection of consumers' data and to ensure their effective ability to correct errors generated by artificial intelligence systems.

3. Algorithmic Bias and Lack of Transparency

The application of artificial intelligence in the financial sector raises a set of complex legal challenges, foremost among which are limited transparency and the exacerbation of algorithmic bias. AI models may inadvertently learn and replicate biases embedded in historical datasets, thereby producing discriminatory outcomes in automated financial decision-making.

For instance, credit scoring systems may assign lower credit ratings to certain groups, insurance models may estimate higher risk levels for specific demographic categories, and fraud detection systems may generate false-positive alerts disproportionately targeting individuals from minority groups.

Legislative authorities require financial institutions to ensure fairness and non-discrimination in the deployment of such models, as biased algorithms may generate significant legal risks and negatively affect customer trust. In this regard, the World Economic Forum warns that **“AI in the financial sector could exacerbate existing inequalities if models are not rigorously tested and continuously monitored”**⁽¹⁾ This underscores the necessity of developing robust oversight mechanisms to ensure integrity and transparency in AI-driven decision-making processes.

On the one hand, many advanced models rely on complex algorithms operating as **“black boxes”** which makes it difficult to explain how specific decisions are reached. This opacity undermines legal accountability requirements and limits the ability of financial institutions to provide clear and comprehensible justifications to customers, particularly in sensitive cases such as the rejection of loan applications.

On the other hand, training these models on historically biased datasets may lead to the reproduction—and even amplification—of discrimination in an automated manner, thereby raising serious challenges in relation to the principles of equality and non-discrimination in financial transactions.

The situation becomes more complex with the emergence of the phenomenon of **“hallucination”**⁽²⁾ in generative artificial intelligence models, whereby these systems may

¹- World Economic Forum, Artificial Intelligence in Financial Services, January 2025, p 15.

²-The undesirable phenomenon known as “hallucination,” defined as the generation of inaccurate or logically incoherent text by natural language generation models, shares certain conceptual similarities with psychological hallucinations, which explains the use of the same terminology. Hallucinated outputs often appear fluent and natural, despite being factually incorrect or logically inconsistent. They may also give the impression of being grounded in a given real-world context, whereas in reality such a context is difficult to identify or verify. Just as it is challenging to distinguish between psychological hallucinations and “real” perceptions, hallucinated textual outputs are likewise difficult to detect at first glance.

produce inaccurate yet highly plausible outputs. This poses a significant risk in the context of financial decision-making.⁽¹⁾

On the other hand, another challenge arises from the increasing concentration of the artificial intelligence market in the hands of a limited number of large technology companies providing so-called foundation models. This concentration generates systemic risks, as any disruption to these services may have cascading effects that extend to the stability of the financial system as a whole.

Financial institutions also face the issue of vendor lock-in⁽²⁾, which makes the transition to alternative providers or the return to on-premises systems particularly difficult and highly costly in terms of both time and financial resources. This situation leads to the effective confinement of data and applications within the ecosystem of the existing provider, thereby reducing institutional flexibility in selecting the most suitable technological alternatives for their operational needs.

In such circumstances, switching to another provider becomes increasingly complex due to high technical and financial costs, as well as the limited bargaining power and technical capacity of financial institutions to effectively monitor the quality of the solutions provided.

Limited transparency and the explainability of artificial intelligence decisions constitute among the most significant challenges to its deployment in the financial sector. Many advanced models operate according to a “black-box” logic, producing outcomes such as loan approvals or fraud detection decisions without providing a clear explanation of how these results are reached.

This raises important legal complexities, particularly as financial institutions are under an obligation to justify decisions that affect customers, especially in areas such as credit scoring, insurance pricing, and fraud detection.

The difficulty lies in the fact that complex machine learning models are often technically difficult to interpret, which limits customers’ ability to understand the reasons behind the rejection of their applications. It also places financial institutions under an increased burden of proof to demonstrate that their decisions are fair and free from bias. In this regard, the European Banking Authority (EBA)⁽³⁾ emphasizes the need for artificial intelligence decisions to be “traceable, explainable, and auditable,” thereby strengthening transparency and accountability requirements and ensuring compliance with applicable regulatory frameworks.

In light of these challenges, there is a growing need to develop legal and regulatory frameworks that enhance transparency and mitigate bias, in order to achieve a balance between innovation, the protection of the financial system, and the safeguarding of users’ rights.

4. Compliance with Multiple Legal and Regulatory Frameworks

¹-ZIWEI JI, NAYEON LEE, RITA FRIESKE, TIEZHENG YU, DAN SU, YAN XU, ETSUKO ISHII, YEJIN BANG, DELONG CHEN, WENLIANG DAI, HO SHU CHAN, ANDREA MADOTTO, and PASCALE FUNG, Survey of Hallucination in Natural Language Generation, ACM Computing Surveys, Vol. 1, No. 1, 2022, p 04.

²- Amal Alhosban, Saichand Pesingu, Krishnaveni Kalyanam, CVL: A Cloud Vendor Lock-In Prediction Framework, Mathematics 12, no. 3: 387, 2024, p 07.

³- European Banking Authority, AI Governance in Financial Services, 2023, <https://www.eba.europa.eu/>, consulted on: 02/03/2026.

If the use of artificial intelligence is adopted in financial services within the Algerian banking sector, it would subject such activities to a multiplicity of laws and regulatory instruments, in the absence of a unified and comprehensive legal framework specifically governing AI. These include, in particular, the Monetary and Banking Law, the Electronic Commerce Law, the Law on the Protection of Natural Persons in the Processing of Personal Data, the legislation laying down the general rules relating to electronic signature and certification, and the law on the prevention and combating of money laundering and the financing of terrorism, in addition to various regulatory instruments and directives issued by the Bank of Algeria.

At the international level, legislative authorities continue to update and refine the regulatory framework governing the use of artificial intelligence. This requires financial institutions to comply with a complex and overlapping set of rules, including existing financial regulations, emerging AI-specific legislation, data protection laws, and cybersecurity requirements. Given the continuously evolving nature of these regulatory instruments, institutions often face significant difficulties in identifying the precise standards with which they must comply, thereby increasing legal and regulatory uncertainty in the adoption of artificial intelligence technologies.

In this regard, Deloitte notes that **“the AI regulatory environment is fragmented and rapidly evolving, creating uncertainty for financial institutions”**.⁽¹⁾

5. Cybersecurity Risks Associated with Artificial Intelligence

Artificial intelligence systems are increasingly exposed to attacks or manipulation attempts by cybercriminals, who may seek to deceive AI-based fraud detection systems, poison training datasets, interfere with AI-driven trading systems, or steal personal data used in machine learning models.

Regulatory authorities in the financial sector expect high standards of cybersecurity; however, artificial intelligence technologies introduce new vulnerabilities that may not be adequately addressed by traditional security frameworks. In this regard, IBM notes that “AI-powered cyberattacks are increasingly on the rise, requiring stronger regulatory and supervisory controls”.⁽²⁾

Cybercriminals are also using artificial intelligence to “amplify” cyberattacks, for instance by generating highly convincing phishing messages and deploying more sophisticated malware, which makes detection and response increasingly difficult. In addition, deepfake technologies are being used to bypass banking authentication systems and enable unauthorized access to customer accounts.

¹-Wooller, K. , AI Regulation in Financial Services: Challenges, Global Trends, and the Future of Innovation. FinTech Weekly, 2025, p 20.

²-IBM, Artificial intelligence (AI) cybersecurity solutions, <https://www.ibm.com/solutions/ai-cybersecurity>, consulted on: 02/03/2026.

6. Legal Liability in the Use of Artificial Intelligence

When an artificial intelligence system commits an error, such as approving a high-risk loan or failing to detect a fraudulent transaction, a fundamental question arises regarding the allocation of liability for such failure. Potentially responsible parties may include the bank itself, the AI solution provider, the data provider, or the system developer.

The legal framework remains insufficiently defined in this regard, as many financial authorities worldwide are working to develop clearer rules governing liability in cases where artificial intelligence systems fail.

In this context, the UK Financial Conduct Authority (FCA)⁽¹⁾ states that institutions must adopt “clear accountability frameworks for managing AI-driven decision-making processes, thereby enhancing transparency, legal accountability, and reducing systemic risks.”

7. Conclusion:

Artificial intelligence has the potential to radically transform financial services; however, it simultaneously raises fundamental legal challenges. Issues related to transparency, data privacy, fairness, cybersecurity, and accountability must be addressed with great care to ensure that the use of artificial intelligence remains safe, ethical, and trustworthy.

Financial institutions must work closely with regulatory authorities, adopt robust governance frameworks, and continuously monitor AI systems. Although more coherent global regulatory standards are expected to emerge in the coming years, companies are currently required to adopt a proactive approach to managing AI-related risks.

Responsible use of artificial intelligence is not merely a legal requirement but a fundamental pillar for building long-term trust in financial services. This study has reached the following findings:

- Artificial intelligence undoubtedly enhances the efficiency and accuracy of decision-making and fraud detection; however, it simultaneously introduces complex legal challenges related to privacy, transparency, data poisoning, accountability, and cybersecurity threats.
- Many advanced models operate as opaque algorithms whose decision-making processes are difficult to interpret, thereby undermining legal accountability and complicating the provision of clear explanations to customers in sensitive cases such as loan rejections.

¹-Financial Conduct Authority, Generating and using synthetic data for models in financial services: governance considerations, 2023, <https://www.fca.org.uk/>, consulted on: 02/03/2026.

- Biased or historically unbalanced datasets may lead to the reproduction of discrimination against certain groups, thereby undermining the principle of equality and generating legal risks for financial institutions.
- Malicious actors may manipulate training data through data poisoning, thereby compromising model integrity, in addition to the emergence of new threats such as deepfakes, which are used to bypass banking authentication systems.
- The allocation of liability in cases of system failure between banks, developers, or data providers remains a complex legal obstacle requiring clear accountability frameworks.
- Regarding technological dependency (vendor lock-in), financial institutions face significant difficulties in switching technology providers due to high costs and data entrapment, which may generate legal risks affecting financial system stability.
- Legal uncertainty resulting from fragmented regulations and the absence of a unified and comprehensive AI framework creates uncertainty for financial institutions.
- Algerian law provides a foundational legal framework that may support the use of artificial intelligence in financial services; however, these provisions require updating to reflect the specificities of such technologies, alongside the development of adequate infrastructure to enable their effective deployment.

In this context, the following recommendations can be advanced:

- The development of flexible and comprehensive legal frameworks that strike a precise balance between fostering AI-driven financial innovation and safeguarding individuals' fundamental rights;
- Clarifying the legal responsibilities of financial institutions regarding their use of artificial intelligence in their relationship with customers;
- Strengthening data protection and privacy safeguards, and ensuring transparency in decision-making processes through legislative updates aimed at providing comprehensive protection of banking data against AI-based applications, alongside the establishment of clear cybersecurity standards.

References

- Law No. 25-11 amending and supplementing Law No. 18-07 on the protection of natural persons in the processing of personal data, dated 24 July 2025, Official Gazette No. 48, issued on 24 July 2025.
- Law No. 18-07 on the protection of natural persons in the processing of personal data, dated 10 June 2018, Official Gazette No. 34, issued on 10 June 2018.
- Amal Alhosban, Saichand Pesingu, Krishnaveni Kalyanam, CVL: A Cloud Vendor Lock-In Prediction Framework, *Mathematics* 12, no. 3: 387, 2024.

- European Banking Authority, AI Governance in Financial Services, 2023, <https://www.eba.europa.eu/> , consulted on: 02/03/2026.
- Financial Conduct Authority, Generating and using synthetic data for models in financial services: governance considerations, 2023, <https://www.fca.org.uk/>, consulted on: 02/03/2026.
- IBM, Artificial intelligence (AI) cybersecurity solutions, <https://www.ibm.com/solutions/ai-cybersecurity> , , consulted on: 02/03/2026.
- Samuel Goldstein, Opt-in et opt-out : les règles de consentement à respecter, 2021, <https://www.legalplace.fr/guides/opt-in-opt-out/> , consulted on: 02/03/2026.
- Tom Krantz, Alexandra Jonker, What is data poisoning?, <https://www.ibm.com/think/topics/data-poisoning> , consulted on: 02/03/2026.
- Wooller, K. , AI Regulation in Financial Services: Challenges, Global Trends, and the Future of Innovation. FinTech Weekly, 2025.
- World Economic Forum, Artificial Intelligence in Financial Services, January 2025.
- ZIWEI JI, NAYEON LEE, RITA FRIESKE, TIEZHENG YU, DAN SU, YAN XU, ETSUKO ISHII, YEJIN BANG, DELONG CHEN, WENLIANG DAI, HO SHU CHAN, ANDREA MADOTTO, and PASCALE FUNG, Survey of Hallucination in Natural Language Generation, ACM Computing Surveys, Vol. 1, No. 1, 2022.