



MANAGING PERSONAL DATA WITH AI IN THE BANKING SECTOR

GÉRER LES DONNÉES PERSONNELLES AVEC L'IA DANS LE SECTEUR BANCAIRE

AOURAGH MIMOUN

Doctoral student at the Faculty of Legal, Economic and Social Sciences, Mohamed I University, Oujda,
Morocco

Email : mimoun.aouragh@ump.ac.ma

RAMDANI BOUCHRA

PhD, Faculty of Legal, Economic and Social Sciences, Mohammed I University, Oujda, Morocco

Email: bouchra.ramdani@ump.ac.ma



ABSTRACT

In this study, we explore the integration of Artificial Intelligence (AI) into the management of personal data in the banking sector, focusing on the Moroccan context. It looks at how AI can improve operational efficiency, customer trust, and regulatory compliance, all of which are especially relevant in the context of data protection challenges.

The research employs PLS-SEM to analyze the relationships between operational efficiency, customer trust, regulatory compliance and AI risk management in the banking industry. In this research, a quantitative study was prepared among banking professionals in Morocco.

The results show that customer trust ($\beta = 0.832$, $p < 0.001$) and AI risk management ($\beta = 0.829$, $p < 0.001$) significantly influence AI optimization, highlighting the importance of transparency and robust risk management strategies. However, regulatory compliance exhibits a negligible impact ($\beta = -0.002$, not significant), revealing gaps in the Moroccan banking sector.

This study contributes to the literature by demonstrating the central role of customer trust and risk management in AI adoption. It calls for the development of AI-driven compliance solutions to enhance regulatory practices in emerging markets.

Key-words : Artificial intelligence, Personal data management, Customer trust, Regulatory compliance, Risk management, Banking industry, AI optimization, Algorithmic transparency, Data governance, Morocco.

RÉSUMÉ

Dans cette étude, nous explorons l'intégration de l'intelligence artificielle (IA) dans la gestion des données personnelles dans le secteur bancaire, en nous concentrant sur le contexte marocain. Elle examine comment l'IA peut améliorer l'efficacité opérationnelle, la confiance des clients et la conformité à la réglementation, autant d'éléments particulièrement pertinents dans le contexte des défis liés à la protection des données.

La recherche utilise PLS-SEM pour analyser les relations entre l'efficacité opérationnelle, la confiance des clients, la conformité réglementaire et la gestion des risques liés à l'IA dans le secteur bancaire. Dans cette recherche, une étude quantitative a été préparée parmi les professionnels du secteur bancaire au Maroc.

Les résultats montrent que la confiance des clients ($\beta = 0,832$, $p < 0,001$) et la gestion des risques liés à l'IA ($\beta = 0,829$, $p < 0,001$) influencent de manière significative l'optimisation de l'IA, soulignant l'importance de la transparence et de stratégies de gestion des risques robustes. Cependant, la conformité réglementaire présente un impact négligeable ($\beta = -0,002$, non significatif), révélant des lacunes dans le secteur bancaire marocain.

Cette étude contribue à la littérature en démontrant le rôle central de la confiance des clients et de la gestion des risques dans l'adoption de l'IA. Elle appelle au développement de solutions de conformité pilotées par l'IA pour améliorer les pratiques réglementaires dans les marchés émergents.

Mots-clés : Intelligence artificielle, Gestion des données personnelles, Confiance des clients, Conformité réglementaire, Gestion des risques, Industrie bancaire, Optimisation de l'IA, Transparence algorithmique, Gouvernance des données, Maroc.

1. INTRODUCTION

Artificial intelligence (AI) today is revolutionizing the way personal data are handled by the banking industry, to enhance operational efficiency, create personalized customer experience and improve decision-making processes. But this rapid adoption brings with it multi-faceted questions around privacy protection, regulatory compliance and cybersecurity risk management (Puschmann, T. 2017, McKinsey & Company, 2018).

Artificial intelligence (AI) is fundamentally reshaping how banks handle personal data, driving gains in operational efficiency, personalized customer experiences, and enhanced decision-making. Yet this rapid adoption intensifies critical tensions between innovation and core imperatives: privacy protection, regulatory compliance, and cybersecurity risk management (Puschmann, 2017; McKinsey & Company, 2018).

Globally, stringent frameworks like Europe's GDPR and California's CCPA compel financial institutions to navigate complex regulatory terrain while leveraging AI for competitive advantage (Biais, Foucault, & Moinas, 2019; Gomber et al., 2018). Tools like predictive analytics enable deeper customer insights but simultaneously heighten concerns about algorithmic transparency and data accountability (European Banking Authority, 2020; Zetsche et al., 2020).

Morocco exemplifies these contradictions. While its banking sector accelerates digital transformation and AI adoption (PwC, 2019; KPMG, 2021), it grapples with distinctive challenges: harmonizing local practices (e.g., Law 09-08) with international standards, mitigating algorithmic bias in Arabic/French bilingual contexts, and building customer trust amid evolving cybersecurity threats (McKinsey & Company, 2019; Deloitte, 2020). Despite extensive research on AI's impact in mature markets (International Monetary Fund, 2018; Riggins & Wamba, 2015), emerging economies, particularly Morocco remain underexplored, especially regarding regulatory risk dynamics.

This study addresses three critical questions:

- **Q1:** How do operational efficiency and algorithmic transparency jointly shape customer trust in Moroccan banking AI?
- **Q2:** To what extent do AI risk management and regulatory compliance influence AI optimization?
- **Q3:** What compliance-specific challenges do Moroccan banks face, and how can AI-driven solutions address them?

Theoretically, we advance understanding of *contextual trust mechanisms* in AI adoption; practically, we offer actionable strategies for regulators and bankers to balance innovation with ethical governance.

The remainder of this study unfolds in four sections. Section II synthesizes existing literature on AI in banking, with emphasis on regulatory gaps in emerging markets and Morocco's unique compliance landscape. Section III details our research methodology, including PLS-SEM analysis and stratified sampling of Moroccan banking professionals. Section IV presents empirical findings on the trust-compliance paradox and discusses implications against international benchmarks. Finally, Section V concludes with strategic recommendations, acknowledges limitations, and proposes mixed-methods research avenues for emerging economies.

2. LITERATURE REVIEW

In recent years, the convergence of artificial intelligence and data management has become a central theme in the digital transformation of the banking sector. This literature review explores the evolving landscape shaped by rapid technological advancements and the growing reliance on data-driven strategies. Our literature review starts by outlining the context in which AI technologies are adopted increasingly, highlighting both the opportunities and challenges they present.

Afterwards, we will delve into the specific tools, practices and techniques that are transforming data handling. Then we will discuss the practical advantages and limitations witnessed in real-world applications. Finally, the review addresses the ethical, regulatory, and strategic considerations that accompany this technological shift.

2.1. Technologies and Challenges of AI in Data Management

The integration of artificial intelligence (AI) into data management has become increasingly fundamental, mainly within sectors like banking where data is abundant and constantly evolving. The integration of artificial intelligence into data management practices has become not only relevant but increasingly indispensable, particularly in domains such as banking, where data flows are dense, continuous, and strategic. As institutions undergo accelerated digital transformation, they are confronted with a dual imperative: to harness the power of data for insight and innovation, while also navigating the complex terrain of data ethics, regulation, and security. Understanding the technologies driving this shift, and the organizational implications they entail, is essential for ensuring that AI tools are deployed responsibly and with long-term viability.

2.1.1. Background and challenges

The rapid digitalization of financial services has dramatically reshaped the data landscape within the banking sector. With the expansion of online platforms and mobile applications, banks now process vast quantities of personal and transactional data generated by increasingly diversified and frequent client interactions. This evolution has not only increased the volume of data but also its granularity and volatility, thereby requiring more sophisticated systems for analysis, storage, and security.

- Digital Transformation and Data Augmentation:

In response to this complexity, artificial intelligence has emerged as a cornerstone of modern data strategy. Its ability to manage, synthesize, and interpret large-scale datasets in real time offers banks a means of enhancing both operational efficiency and the personalization of services. As observed by Puschmann (2017) and further emphasized by Arner, Barberis, and Buckley (2016), the implementation of AI in finance marks a departure from static data handling toward dynamic, predictive, and adaptive information ecosystems.

However, this shift is not without obstacles. The integration of AI technologies necessitates structural changes in how institutions handle data governance, including the creation of interoperable systems and protocols that can accommodate diverse sources and formats of information. Moreover, banks must contend with the risks associated with data misuse, algorithmic opacity, and the potential erosion of consumer trust.



According to the International Monetary Fund (2018), the adoption of AI-driven solutions is no longer optional for institutions seeking to remain competitive. These technologies enable banks to extract meaningful insights from daily transactional flows, facilitating faster and more informed decision-making. Yet, the mere presence of AI tools is not sufficient; their implementation must be aligned with clear governance strategies, regulatory frameworks, and ethical standards to ensure that data-driven innovation does not compromise accountability or transparency.

- **Decision-making and service customization :** In today's banking environment, fine-grained data analysis is at the heart of decision-making processes. Leveraging information from transactions and market trends enables institutions to devise strategies aimed at optimizing both customer experience and operational efficiency (Puschmann, T. 2017, McKinsey & Company, 2018) . For example, the use of predictive analysis tools, powered by AI algorithms, makes it possible to anticipate emerging customer needs and develop tailor-made financial products, meeting increasingly personalized requirements (McKinsey & Company, 2018, Chen, M., Mao, S., & Liu, Y., 2014).
- **Privacy, Trust and Data Governance :** Increased reliance on data naturally raises questions about privacy protection. While consumers are sensitive to the need to improve the services offered, they remain vigilant about the security of their personal information (European Banking Authority, 2020) . In this context, transparency in data use appears to be an essential lever for building and maintaining trust. Furthermore, the establishment of robust governance frameworks that guarantee data quality, consistency and accessibility, while complying with regulatory requirements, is crucial to the overall effectiveness of decision-making processes (PWC, 2019, Gupta, M., & George, J. F., 2016). Concrete examples, such as Fifth Third Bank, illustrate the positive impact of integrated governance on operational efficiency (Chen, M., Mao, S., & Liu, Y., 2014).

While AI opens up new possibilities in managing vast data flows, it also demands thoughtful strategies to overcome issues related to privacy, trust, and operational consistency.

2.1.2. AI Technologies and Data Management Optimization

AI technologies are transforming traditional data management by introducing automation, precision, and speed. These tools offer new ways to improve how data is organized, secured, and utilized.

- **Data cleansing and automation :** AI technologies are revolutionizing data management by automating the discovery, sorting and correction of information flows. By identifying and analyzing multiple sources - whether network traffic or internal databases - AI streamlines data cleansing and overcomes the shortcomings inherent in manual processing (Zetzsche & al. 2020) . This automation contributes to data reliability, a sine qua non for relevant analysis and optimal decision-making.
- **Enhanced Safety and Compliance :** AI in data management also provides key levers for enhancing security arrangements. Intelligent systems enable the implementation of robust access controls and maintain compliance at all times with a dynamic regulatory landscape (Zetzsche & al. 2020, Riggins, F. J., & Wamba, S. F., 2015). The capacity to scrutinize huge quantities of governing information in real time greatly decreases compliance expenses and the hazards from violations.
- **Personalizing and Enhancing the Customer Experience :** With the help of sophisticated data analysis, AI tools allow banking services to be personalized. Emerging banks capitalize on this technology to predict customer behavior and preferences, allowing them to offer personalized and personalized services, thus enhancing consumer satisfaction and loyalty (Riggins, F. J., & Wamba,

S. F., 2015, Yoon, J., & Mo, J., 2020). In a fast-changing market, this targeted experience is a significant competitive benefit.

- **Intelligent Curation and Risk Detection** : AI-driven intelligent data curation improves the construction and administration of structured data catalogs, providing a means to exploit these data in the decision-making process (Zetzsche & al. 2020) . Moreover, using fraud detection algorithms is helping to identify transaction outliers quickly, which enhances risk management and compliance with anti-money laundering and other financial fraud regulations (McHenry, P., 2018, MDPI, 2020).

By enhancing efficiency and enabling smarter decision-making, AI-driven tools mark a major step forward in how organizations handle and benefit from data.

2.2. Benefits of Integrating AI into Data Management

Integrating AI into data management allows organizations to boost data quality and streamline business operations. It supports real-time insights that enhance both strategic planning and customer engagement.

- **Improving Data Quality and Accuracy** : AI is also able to improve data quality and accuracy levels, which is one of its major strengths. This, in turn, aids data integrity, as automated validation processes can catch and correct inconsistencies, keeping the information that guides risk assessment and decision-making intact. (European Commission, 2016)
- **Business Process Optimization** : Real-time, reliable information provision through integrated data management facilitates quick and informed decision-making. Having data from thousands of sources creates a global view of the demand behaviours and market trends leading to the most locater, sales strategies.(Zetzsche & al. 2020) .
- **Compliance and Risk Management** : AI helps observance of regulatory demands (like RGPD and CCPA) by bringing about automation in the reporting and auditing processes and reducing the risks of compliance, while also giving room to governance practices that strengthens the robustness of the decision-making models (Zetzsche & al. 2020) ,KPMG, 2021).
- **Cost reduction and operational efficiency** : By automating repetitive tasks and optimising data processing workflows, operational costs can be reduced dramatically. Reducing human error and accelerating analytical processes, AI allows for better resource distribution and increased productivity overall (Zetzsche & al. 2020, McKinsey & Company, 2019).

The adoption of AI not only improves data handling but also empowers organizations to operate more effectively, meet regulatory demands, and reduce operational costs.

2.3. Ethical and Regulatory Challenges and Concerns

Despite its advantages, the use of AI in data management brings forth ethical concerns and regulatory pressures. Ensuring fairness, transparency, and security is more important than ever.

Complexity of Regulatory Compliance : The rollout of AI technologies raises significant regulatory issues. Laws like Europe's RGPD and the US CCPA builds strong limitations on collecting and utilizing user data, demanding transparency of automated processes (Deloitte, 2020). Non-compliance with your organization's regulations can lead to heavy penalties and jeopardize the involvement of those financial institutions.



-
- **Ethical Risks and Algorithmic Bias** : AI's use also raises ethical questions, particularly related to privacy and fairness in automated decisions. It can then result in unintentional discrimination, creating the need for mechanisms to ensure that algorithms and data are respectful and transparent. (McKinsey & Company, 2019)
 - **Explicability and Data Security** : If we want to cultivate trust, we need to make AI models explainable and the mechanics of how it works thoroughly documented. Data centralization, however, creates a greater potential security risk: the need for tight protective protocols to ensure that no sensitive data find its way out of the system. (United States Congress, 2018)

To fully benefit from AI while maintaining public trust, it is essential to develop clear ethical guidelines and comply with evolving legal standards in data handling.

In summary, the application of AI in data management holds significant promise for enhancing efficiency, accuracy, and customer personalization. However, these advancements must be balanced with strong governance, ethical responsibility, and compliance with regulatory standards. As technology continues to evolve, striking this balance will be key to building trust and achieving long-term success in the digital age.

2.4. Best practices, regulatory frameworks and future prospects

As artificial intelligence continues to redefine how financial institutions manage and exploit data, it becomes increasingly imperative to establish sound governance principles and robust regulatory safeguards. In a sector where innovation progresses at a rapid pace, ensuring accountability and ethical alignment is no longer a secondary concern but a fundamental prerequisite. This section aims to unpack a set of key strategies and emerging frameworks that offer a balanced path forward, one that reconciles technological ambition with regulatory discipline. It also sheds light on evolving trends likely to shape the trajectory of AI integration in banking over the coming years.

2.4.1. Best Practices for Balanced Data Management

Deploying AI in a way that aligns with legal, ethical, and operational standards requires more than technological prowess. It calls for a holistic strategy rooted in regulatory compliance, data protection, and interdisciplinary coordination. Therefore, adopting best practices is essential for ensuring that data is not only leveraged efficiently but also managed with transparency and integrity.

- **Compliance and Transparency** : Nowadays, data protection frameworks impose a clear obligation on institutions to disclose how data is collected, processed, and stored. Compliance cannot be reduced to a box-checking exercise; it requires the continual refinement of internal processes through regular audits, policy reviews, and impact assessments. Ensuring that users understand how their information is being used and offering them control over it, reinforces public trust. As highlighted by Biais, Foucault, and Moinas (2019) and restated in McKinsey & Company (2019), transparency has become a strategic lever, not only a regulatory one, in managing digital trust.
- **Depersonalization and Anonymization Techniques** : Given the inherent sensitivity of financial and personal data, implementing robust anonymization mechanisms is crucial. Through applying techniques that disconnect personal identifiers from data records, institutions can significantly mitigate the risks associated with large-scale processing. These methods serve as a critical buffer, reducing the likelihood of breaches while still enabling organizations to extract valuable insights. As Jagtiani and Lemieux (2018)

point out, the success of these measures lies not only in technical implementation but also in their integration into a broader privacy-by-design framework.

- **Training and Interdisciplinary Collaboration :** Sharing a common language and culture between technical experts and compliance officers is important for successful implementation of AI that protects data, and involving teams in regular training programs on AI and data protection topics can support this evolution. Such synergies allow for smoother incorporation of regulatory requirements in both the development and deployment of AI technologies. According to McKinsey & Company (2019), such interdisciplinary initiatives foster mutual understanding and facilitate the seamless translation of regulatory obligations into technological design.

By promoting transparency, using anonymization techniques, and encouraging interdisciplinary cooperation, organizations can align technological advancement with responsible data management.

2.4.2. Regulatory Frameworks and Standards Adaptation

As the momentum of AI innovation intensifies, it becomes increasingly evident that existing legal and regulatory instruments must evolve in parallel to remain effective. Policymakers, regulators, and institutional actors now find themselves at a crossroads: they must design regulatory approaches that not only foster technological dynamism but also preserve consumer protection, market transparency, and financial system stability.

- **Regulatory Issues in a Context of Innovation :** The fast-paced development of AI technologies has laid bare the limitations of conventional regulatory architectures, which were not conceived with algorithmic decision-making or real-time data processing in mind. In this sense, the regulatory lag creates a structural vulnerability that may jeopardize the equilibrium between innovation and oversight. Authorities are thus compelled to navigate a delicate balance on one hand, stimulating innovation to maintain competitiveness, and on the other, shielding users and institutions from unintended harms. This tension is particularly acute in the financial sector, where data-centric models increasingly underpin critical operations in credit, risk, and compliance (Philippon, 2016; European Commission, 2016).
- **Main Regulatory Frameworks :** Several cornerstone regulatory frameworks now serve as reference points in shaping AI governance across jurisdictions. Notably:
 - **The General Data Protection Regulation (GDPR)** in the European Union imposes robust obligations concerning the collection, processing, and storage of personal data. It emphasizes transparency, consent, and data subject rights—principles that are particularly relevant in the age of AI-driven analytics (Gomber et al., 2018; Arner, Barberis & Buckley, 2017).
 - **The California Consumer Privacy Act (CCPA)** similarly extends data protection rights to individuals in the United States, with a focus on granting consumers greater control over their personal information. It also addresses the emerging challenges of predictive modelling and automated profiling in commercial contexts (European Commission, 2016; Arner et al., 2017).
 - **Basel III**, though traditionally focused on capital adequacy and liquidity, exerts an indirect influence on AI adoption by reinforcing the importance of operational resilience and internal risk control

frameworks. In this respect, its provisions encourage the alignment of AI systems with broader risk governance principles (McKinsey & Company, 2019).

Towards Adaptive Regulation: Despite the efforts of current frameworks, it is becoming clear that rigid, prescriptive approaches may fall short in responding to the dynamic nature of AI systems. In this regard, regulators are urged to adopt adaptive models based on guiding principles rather than exhaustive rulebooks. Such a shift would enable iterative experimentation and encourage innovation within defined ethical and procedural boundaries (Philippon, 2016; Gomber, Koch & Siering, 2017).

Furthermore, maintaining open and ongoing dialogue between regulators, industry stakeholders, and technologists is essential. This collaborative ethos not only supports the contextual interpretation of evolving norms but also helps align regulatory expectations with the operational realities of AI deployment (Gomber et al., 2018; Akhtar, Uddin & Chowdhury, 2021). By grounding regulatory responses in flexibility and inclusivity, authorities can foster an ecosystem where AI innovation and public accountability are not at odds, but rather co-evolve.

Going through the rapid evolution of artificial intelligence will require a regulatory approach that is both anticipatory and cooperative, one that embraces flexibility while remaining firmly anchored in ethical obligations and legal accountability.

2.5. Illustrative Case Studies

Real-world applications provide valuable insight into how AI can be implemented responsibly and effectively in the financial sector. Case studies reveal the impact of aligning innovation with compliance and customer needs. Concrete applications offer a crucial lens through which the responsible use of AI in the financial industry can be better understood. Real-world case studies not only demonstrate the feasibility of integrating AI tools into existing operations, but also highlight how technological innovation, when thoughtfully designed, can remain aligned with regulatory expectations and customer-centric values.

- **Bank of America - Erica, the Intelligent Financial Assistant:** One notable example is the deployment of *Erica*, a virtual assistant developed by Bank of America. Designed to deliver tailored financial advice, track user expenditures, and help clients optimize their budgeting practices, Erica exemplifies how AI can enhance customer experience without compromising compliance. Notably, this initiative was rolled out in close collaboration with regulatory authorities—an approach that underscores the importance of embedding ethical and legal safeguards directly into the architecture of intelligent systems. As highlighted by Van der Aalst (2016) and Davenport et al. (2020), such partnerships demonstrate how forward-looking institutions can reconcile innovation with robust governance, ultimately reinforcing consumer trust and institutional accountability. This initiative, developed in close partnership with regulators, underscores the significance of designing AI systems in an ethical and compliant manner:
 - **Compliance and ethics:** From the outset, Erica's design incorporated strict requirements for transparency and data protection, guaranteeing the ethical use of algorithms.
 - **Customer-centric approach:** By focusing on personalization, Bank of America has strengthened the relationship of trust with its customers, demonstrating the effectiveness of a strategy based on user experience.



-
- **JP Morgan Chase - COiN (Contract Intelligence)** :JPMorgan Chase's COiN tool, an AI-powered solution, has drastically reduced the time spent on contractual processes by around 360,000 hours per year. This case highlights the transformative potential of AI in optimizing traditional operations and enhancing competitiveness within the financial industry. (Arner, D. W., Barberis, J., & Buckley, R. P. 2016) .
 - **NCUA - Responsible Innovation in AI** : The National Credit Union Administration NCUA, the federal agency that oversees credit unions, takes a thorough approach when evaluating AI applications. They ensure these technologies meet strict standards for security, privacy, and operational feasibility. This proactive stance highlights the importance of striking a balance between fostering innovation and managing risks in the evolving regulatory landscape. (Wamba, S. F., & al. 2015, Tapscott, D., & Tapscott, A., 2016) .

These examples underscore the importance of ethical design, regulatory alignment, and user-focused strategies, all of which are critical to successful AI integration in financial services.

In Morocco, digital banking transformation accelerates, yet infrastructural and regulatory gaps persist (PwC, 2019; KPMG, 2021). Recent studies in similar emerging economies such as Tunisia's focus on agile fintech frameworks (Mohammed, 2025) and Senegal's data anonymization protocols (Musoni, 2024) reveal recurring hurdles in harmonizing AI with local compliance norms. These contexts demand *tailored governance models*, distinct from GDPR-centric approaches.

2.6. Outlook and future trends

The future of AI in finance is marked by both great potential and significant responsibility. Emerging technologies and evolving market conditions are shaping new directions for data use and management.

- **Structural Transformation through AI** : The integration of AI is expected to have a profound impact on the banking industry. While cost reduction was an initial driver, financial institutions are now focused on leveraging AI to increase their added value and drive growth. Key applications include particularly risk management and improving customer service (GARP, 2021) .
- **The Emergence of Generative AI** : The rise of large language models (LLMs) and generative AI is providing European leaders with new opportunities to enhance internal operations and personalize customer experiences. These advanced technologies are enabling organizations to boost productivity and reshape how they interact with their customers. (International Banker, 2020) .
- **Strengthening Data Management Practices** : The rapid growth in data volumes has made it imperative for organizations to adopt advanced data management practices. Sophisticated data governance tools are emerging as essential elements to support AI-based decision-making within a strict regulatory environment, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). (Zetsche & al. 2020, Hofmann, P., & Rüegg-Stürm, 2019) .
- **Reconciling innovation and ethics** : The utilization of AI technology can provide substantial operational advantages, but it also raises critical ethical concerns. Institutions will need to establish transparent governance frameworks to ensure the fair and secure application of AI technologies, while also adapting to evolving regulatory requirements. (GARP, 2021) .
- **Economic Challenges and Modernization** : In the current economic climate of declining interest rates and pervasive digital disruption, banks are facing the challenge of striking a balance between technological

modernization and prudent resource management. This is crucial for ensuring their long-term stability and growth. (FinTech Magazine, 2021).

To unlock the full potential of artificial intelligence in financial services, institutions must not only innovate but also embed their technological advances within a strong ethical and regulatory framework. The durability of AI adoption depends, in large part, on maintaining this delicate equilibrium—one where transparency, accountability, and trust are treated as essential design criteria rather than afterthoughts.

Looking ahead, the successful integration of AI into data management practices will rest on the sector's ability to reconcile technological progress with governance imperatives. Institutions that proactively adopt industry best practices, adjust internal policies in response to regulatory evolution, and anticipate emerging challenges will be better positioned to thrive in an increasingly data-centric and compliance-driven environment.

In this light, the use of AI in managing personal data represents both a powerful opportunity and a profound responsibility. When thoughtfully implemented, AI can significantly enhance operational performance, improve the personalization of banking services, and mitigate operational and reputational risks.

However, the depth and scope of this transformation demand a sustained commitment to transparency, ethical conduct, and legal compliance. At the heart of this shift lies the need for resilient data governance structures, advanced security architectures, and meaningful collaboration between regulatory bodies, industry stakeholders, and technology developers.

In summary, the literature converges on a central premise: AI offers transformative value to the banking sector, but its benefits can only be fully realized when innovation is tempered by principled oversight. This calls for a balanced, adaptive approach grounded in interdisciplinary cooperation and forward thinking regulation.

3. METHODOLOGY

Aiming to examine how artificial intelligence is being integrated into personal data management within the banking sector, this study employs a robust quantitative methodology based on Partial Least Squares Structural Equation Modeling (PLS-SEM). This technique is particularly well-suited to assessing the complex, multi-directional relationships between latent constructs such as operational efficiency, customer trust, AI risk governance, and regulatory compliance.

Unlike covariance-based SEM, the PLS approach is more flexible in handling smaller samples and non-normal data distributions attributes that make it especially appropriate for exploratory research in rapidly evolving technological contexts like financial AI. Furthermore, it allows for the simultaneous assessment of both the measurement model (i.e., reliability and validity of constructs) and the structural model (i.e., the causal paths between variables).

3.1. Search Design and Rationale

This research follows an explanatory design, with the aim of uncovering the mechanisms by which AI-related variables interact to influence optimization outcomes in personal data management. The conceptual framework was developed through a thorough synthesis of recent literature and real-world case studies, ensuring both theoretical rigor and practical relevance.

The decision to use PLS-SEM is driven by several factors. First, the method is capable of modeling multiple interdependencies between variables simultaneously—an essential feature given the interconnected nature of

the constructs under investigation. Second, PLS is particularly well-suited to studies involving emerging phenomena, such as AI deployment in banking, where theoretical models are still being refined.

Table 1: Assumptions based on IA themes

Axis	Corresponding assumption
AI technologies and operational efficiency	H1: Improved audit compliance and adoption of AI technologies (e.g. predictive analytics, fraud detection) enhance AI optimization in banking.
AI and customer confidence	H2: Increased trust and satisfaction, reinforced by ethical AI practices (e.g. transparency, explicability), positively influence AI optimization.
AI and regulatory compliance	H3: Effective AI risk management and robust data protection measures improve regulatory compliance (e.g. RGPD, CCPA) and support AI optimization.
AI and transparency	H4: Effective AI optimization improves banks' operational performance by boosting efficiency and productivity.
Confidentiality and data sharing	H5: Improved operational performance leads to better data protection and confidentiality, strengthening customer confidence and their willingness to share their personal data.

Source: compiled by us

Our investigation is structured around a set of hypotheses, each aligned with one of five key thematic areas: technological integration, customer trust, regulatory compliance, transparency, and data privacy. These hypotheses are outlined in the table, which organizes them according to their corresponding dimensions of AI impact within the banking context.

3.2. Measurements and Variables

The key variables in this study are defined from existing literature to ensure validity. As illustrated in the subsequent table, the independent variables encompass AI technology adoption, data governance, regulatory compliance, AI ethics and privacy protection. The main dependent variable is the impact of AI on operational efficiency, customer experience, consumer trust and regulatory compliance. Finally, control variables, such as bank size, market location and customer demographics, contextualize the results. The evaluation of respondents' perceptions is based on 5-point Likert scales, guaranteeing a detailed analysis of their opinions and attitudes.

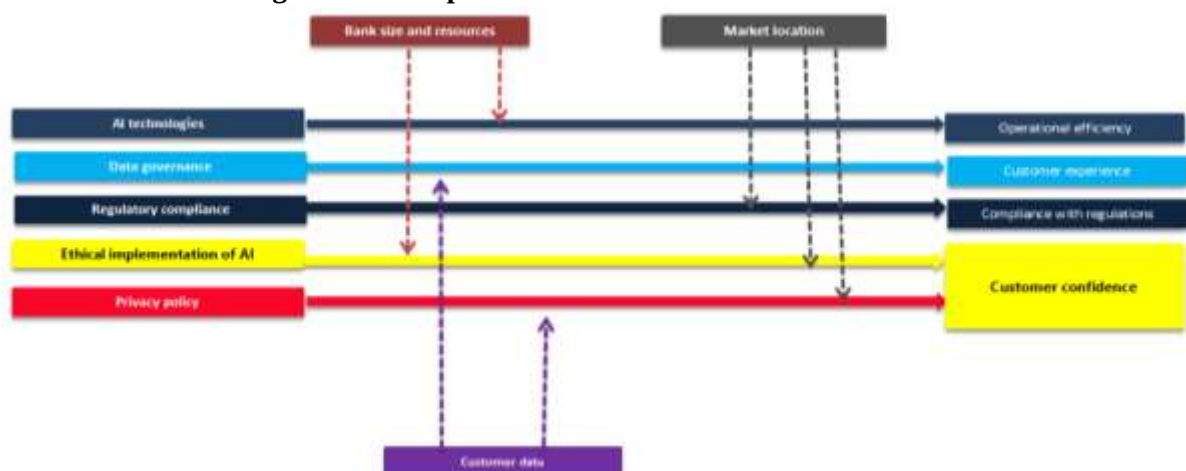
Table 2: Review of study variables

Category	Variables
Independent variables	- AI technologies: predictive analytics, intelligent data curation, fraud detection.
	- Data governance practices: data quality, accessibility, compliance.
	- Regulatory compliance: compliance with RGPD, CCPA and other legislative frameworks.
	- Ethical implementation of AI: transparency, explicability, fairness.
	- Privacy protection: security measures to protect personal data.
Dependent variables	- Operational efficiency: fraud detection, rapid decision-making, cost reduction.
	- Customer experience: satisfaction and trust through personalized services.
	- Consumer confidence: willingness to share data and use services.
	- Regulatory compliance: violations, fines, impact on reputation.
Control variables	- Bank size and resources: impact of capabilities on AI adoption.
	- Market location: influence of regulatory differences (EU vs. US).
	- Customer demographics: effects of age, income and technological knowledge on behavior.

Source: compiled by us

This classification of variables forms the backbone of our research and provides us a structured lens through which the relationship between AI implementation and performance can be examined.

Figure 1: Conceptual model of the search to be modified



Source: compiled by us

Each category of variables (independent, dependent, and control) was operationalized based on prior empirical research and adjusted to reflect the specificities of the Moroccan banking context.

In alignment with this variable structure, a conceptual model was developed to visualize the proposed relationships among constructs and to guide the empirical analysis. The model integrates key pathways hypothesized in the literature and serves as a blueprint for testing the causal links underpinning AI optimization in personal data management.

3.3. Sample and Data Collection

The data collection process targeted a carefully selected group of banking professionals operating within the Moroccan financial sector. Selection criteria focused on individuals with active responsibilities related to the management of sensitive customer information, as well as those directly engaged in strategic decision-making processes surrounding artificial intelligence and digital transformation initiatives.

A total of 89 professionals participated in the study, with a gender distribution of 62% male and 38% female. The average professional experience across the sample was 8.2 years. A stratified sampling method was employed in collaboration with the Moroccan Banking Association (AMB) and Bank Al-Maghrib (BAM), ensuring a balanced representation across institutional types, hierarchical roles, and geographic locations. Participants were drawn from a range of banking entities to reflect the ecosystem's diversity. To capture functional diversity, the sample was segmented according to professional tiers and core responsibilities:

Table 3: Role-based stratification

Role Tier	% of Sample	Principal Responsibilities
C-suite (CIO/CDO)	34%	Oversight of AI budgeting and strategy
Operational Managers	51%	Implementation of data governance practices
Compliance Officers	15%	Ensuring adherence to regulatory standards

Source: compiled by us

In order to ensure relevance and contextual alignment, inclusion criteria required that participants:

- Possess a minimum of three years of experience in roles involving the handling of personal or sensitive data;
- Have participated directly in at least one AI-related initiative (e.g., fraud detection systems, customer service chatbots);
- Be geographically located either at the Casablanca headquarters (74%) or in regional offices across Tangier, Rabat, Oujda and Marrakesh (26%).

Recruitment efforts were anchored in AMB's official member directory, with endorsement from BAM to enhance institutional credibility. Notably, the final participant pool represented organizations managing approximately 82% of Morocco's retail banking assets, as reported in the BAM's 2024 Annual Report. The survey achieved a response rate of 81% (89 completions from 108 initial contacts), supported by incentives such as access to confidential benchmarking reports.



To collect the necessary data, a structured questionnaire was designed, pre-tested, and refined through a pilot phase. This step was instrumental in enhancing the clarity and relevance of the survey items, thereby improving their reliability. Once finalized, the questionnaire was distributed through online platforms to maximize accessibility, particularly considering the time limitations and geographical dispersion of the respondents.

The survey instrument was specifically tailored to capture participant perspectives on a range of thematic areas, including perceived improvements in operational efficiency attributable to AI, levels of customer trust and satisfaction, the effectiveness of regulatory compliance practices, and the maturity of AI-related risk management frameworks within their respective institutions.

3.4. Data analysis

The collected data were analyzed using structural equation modeling via the Partial Least Squares (PLS-SEM) method, which is particularly suited for models involving multiple interdependent latent constructs and moderate sample sizes. The analysis was carried out using SmartPLS software.

PLS-SEM was prioritized for three reasons: (1) its suitability for exploratory models with nascent theoretical foundations, (2) flexibility with non-normal data and small samples, and (3) capacity to evaluate complex interdependencies (e.g., trust-compliance-risk interactions) without strict distributional assumptions (Hair et al., 2019).

This methodological choice reflects the study's nature and the complex relationships being tested. The process followed two main stages:

- a. **Measurement model evaluation**, where reliability and validity of each construct were assessed. Composite reliability (CR) values were required to exceed the 0.7 threshold, while average variance extracted (AVE) scores were expected to surpass 0.5—following the standards set by Fornell and Larcker (1981). These checks ensured internal consistency and convergent validity across constructs.
- b. **Structural model testing**, which involved estimating path coefficients between variables and evaluating the model's explanatory power through R^2 values. Bootstrapping procedures were applied to test the statistical significance of each relationship.

This two-step process allowed for a rigorous examination of both the robustness of the measurement instruments and the strength of the hypothesized causal relationships within the conceptual framework.

To bolster the methodological rigor, multiple validation procedures were employed:

- **Convergent and Discriminant Validity:** AVE was used to establish convergent validity, while discriminant validity was assessed via the Fornell-Larcker criterion and by analyzing the inter-construct cross-loadings.
- **Internal Reliability:** The constructs' reliability was verified using both Cronbach's alpha and composite reliability. Values above 0.7 were interpreted as demonstrating satisfactory internal consistency.
- **Robustness Checks:** Additional sensitivity analyses were conducted to ensure the model's stability under varying specifications. These included exploring moderating variables such as organizational size and regulatory context, which may shape the observed relationships.



Despite the methodological soundness of the approach, some limitations should be acknowledged. The sample, composed exclusively of managers from Moroccan banks, may limit the broader applicability of the findings to other geographical regions or industry sectors. Moreover, the reliance on self-reported data introduces the risk of social desirability bias. Future research would possibly involve qualitative interviews with industry professionals, to enrich the interpretation of the strategic and operational dimensions of AI deployment.

In sum, this study offers a robust analytical framework for investigating the drivers of AI adoption in personal data management within the banking sector. The use of PLS-SEM not only facilitates the analysis of complex inter-variable relationships but also yields practical insights that can inform both academic inquiry and industry decision-making.

4. RESULTS AND DISCUSSION

This section outlines the empirical findings, followed by a detailed interpretation in line with the research hypotheses and conceptual framework. The analysis highlights the critical drivers influence in the adoption of artificial intelligence (AI) in personal data management within the banking sector. Special attention is given to operational efficiency, customer trust, regulatory compliance, and risk mitigation, core elements to the successful integration of AI systems.

4.1. Results presentation

To ensure the robustness and credibility of the findings, both the measurement and structural components of the model underwent thorough evaluation. These assessments provided clarity on the interrelations between constructs and confirmed the soundness of the underlying theoretical model.

The analytical technique employed was Partial Least Squares Structural Equation Modeling (PLS-SEM), which allowed for the nuanced exploration of latent constructs and the complex pathways between them. The presentation of results is organized into two principal subsections.

4.1.1. Measurement Model Evaluation

The first stage focused on evaluating the reliability and validity of the measurement model. Several well-established indicators were used to test internal consistency, convergent validity, and discriminant validity:

- Internal Consistency: Both Cronbach's alpha and composite reliability (ρ_c) surpassed the commonly accepted threshold of 0.7 across most constructs, indicating reliable internal coherence.
- Convergent Validity: AVE (Average Variance Extracted) values exceeded 0.5 for all constructs, with one exception—regulatory compliance, which fell short of this benchmark. This deviation suggests potential measurement issues and calls for conceptual refinement in future iterations.
- Discriminant Validity: Assessed via the Fornell-Larcker criterion, results confirmed that each latent variable explained more variance in its own indicators than in others, thereby supporting discriminant validity.



Table 4: Reliability and validity of constructs

Construct reliability and validity - Overview				
	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
AI optimization	0.783	0.808	0.860	0.607
Audit compliance	-1.275	-1.566	0.424	0.425
IA risk management	0.692	0.739	0.864	0.761
Operating performance	0.764	0.764	0.895	0.809
Trust & satisfaction	0.787	1.080	0.894	0.809

Source: Smart PLS report

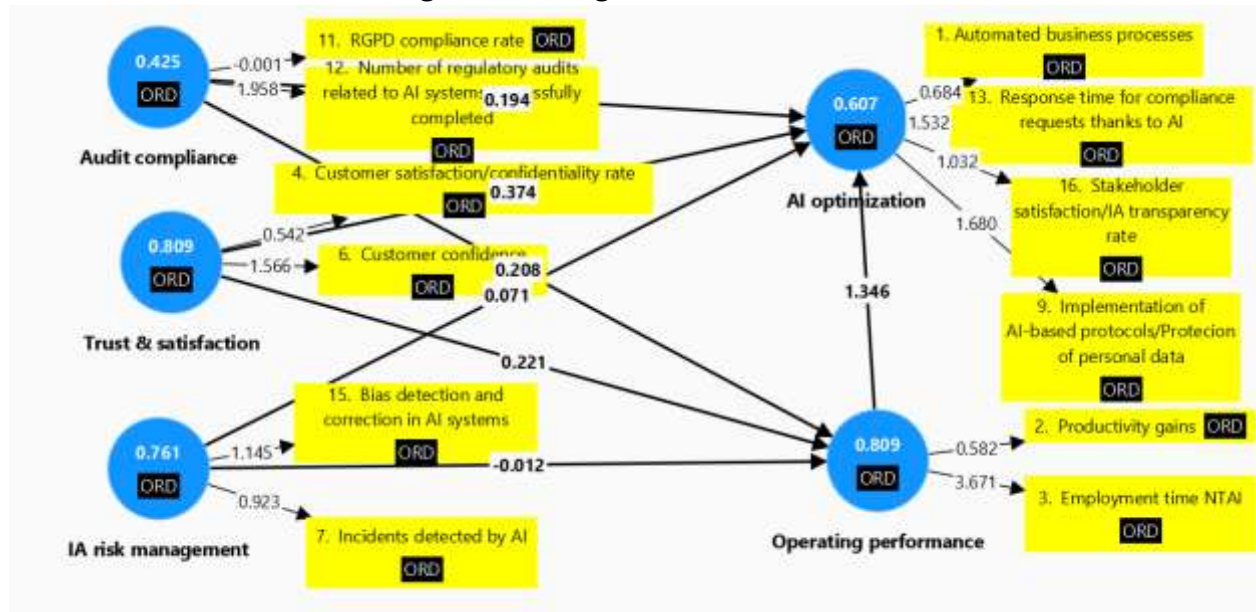
Overall, the measurement model displayed strong psychometric properties, though the audit compliance construct exhibited some deficiencies in convergent validity. This finding points to a possible conceptual or operational gap in how regulatory adherence is currently understood or captured in this context.

4.1.2. Structural Model Test

The second phase centered on assessing the structural model to determine the strength and direction of the relationships between latent variables, focusing on their impact on AI optimization and operational performance.

- The model exhibited strong explanatory capacity, with an R^2 of 0.809 for operational performance and 0.607 for AI optimization. These results suggest that the proposed variables account for a significant portion of the variance in both dependent constructs.
- Among the predictors, Trust and Satisfaction emerged as the most influential factor for AI optimization ($\beta = 0.832$, $p < 0.001$), closely followed by AI Risk Management ($\beta = 0.829$, $p < 0.001$). These findings underscore the critical role of transparent communication and proactive risk mitigation strategies in building user confidence and facilitating successful AI implementation.
- In contrast, the construct related to Audit Compliance showed a virtually non-existent effect ($\beta = -0.002$, statistically insignificant), revealing structural weaknesses in the regulatory compliance mechanisms within Moroccan banking institutions. This result raises important questions about the current effectiveness of compliance frameworks and their capacity to support technological integration.

Figure 2: Testing the structural model



Source: Smart PLS report

The hypotheses formulated reveal that 80.9% of AI operational performance is influenced by the three dimensions audit compliance, customer trust & satisfaction and AI risk management. Similarly, AI optimization is explained in this model up to 60.7% through the direct interactions of these three dimensions and those mediated by operational performance. Tables N°3 and 4 below summarize the different readings of the PLS structural model.

Table 5: Path Coefficients and Hypothesis Testing

Hypothesis	β	*p*-value	Supported?
H1 (Trust $\rightarrow$ AI Opt.)	0.832	<0.001	Yes
H2 (Risk Mgmt $\rightarrow$ AI Opt.)	0.829	<0.001	Yes
H3 (Compliance $\rightarrow$ AI Opt.)	-0.002	0.951	No

Source: compiled by us

The non-significant role of compliance ($\beta = -0.002$) contrasts sharply with EU contexts, where GDPR alignment bolsters AI adoption (Zetzsche et al., 2020). In Morocco, however, regulatory fragmentation, such as discrepancies between Law 09-08 (data protection) and banking circulars, and creates operational ambiguity. Similar emerging markets (e.g., Kenya, Muttai, 2024) show comparable gaps, suggesting *regulatory maturity*, not mere strictness, drives compliance efficacy.



Table 6: Structural model figures

Built	AVE	Impact on AI Optimization	Impact on operating performance	Comments
Audit compliance	0.425	-0.002	-0.045	Weak convergent validity and negligible influence; requires in-depth revision.
Trust & satisfaction	0.809	0.832	0.962	Robust construction with very strong influence on other variables; relevant indicators.
IA risk management	0.761	0.829	0.913	Good validity and significant contribution to other variables; reliable construct.
AI optimization	0.607	-	0.822	Key construction directly influencing operational performance.
Operating performance	0.809	-	-	End result influenced by several constructs; well-defined, relevant indicators.

Source: compiled by us

The constructs Trust & Satisfaction, IA Risk Management and Operational Performance have significant positive effects on IA Optimization. However, the Audit Compliance construct shows major weaknesses, both in terms of its validity and its influence on the other variables, showing the exercise of a non-significant effect.

Trust and risk management emerged as critical drivers of AI optimization and performance, while the weak role of audit compliance suggests gaps in regulatory effectiveness, particularly within the Moroccan banking context.

4.2. Interpretation of results

The results obtained through structural equation modeling offer a global view of the factors influencing the integration of AI in the management of personal data, while guaranteeing their protection and confidentiality in the banking sector. They highlight areas for optimization and points to watch out for in order to respond effectively to the problem.

- a) **Trust & Satisfaction as a Pillar of AI Optimization:** The strong and statistically significant influence of Trust & Satisfaction on AI optimization ($\beta = 0.832$, $p < 0.001$) reinforces what many practitioners have long suspected: transparent, ethical handling of customer data is not just a compliance requirement; it's a competitive advantage. When clients perceive fairness and clarity in how their data is used, they are more likely to accept and even welcome AI-driven services. This aligns with previous studies on algorithmic transparency and affirms the growing importance of



reputational risk management in banking. In practice, this highlights the strategic value of investing in explainability tools, client education, and ethical AI design.

- b) **The Central Role of AI Risk Management:** AI Risk Management also emerged as a critical enabler of AI adoption ($\beta = 0.829$, $p < 0.001$), confirming that risk-aware institutions are better positioned to leverage innovation without compromising data integrity or customer security. These results echo a key trend in recent AML/CFT research: that strong data governance and preemptive cybersecurity frameworks are essential in a digitized financial ecosystem. Given the current threat landscape; including data breaches, algorithmic manipulation, and regulatory sanctions. This finding is both expected and urgent.
- c) **Compliance Audit: A Structural Weak Link:** In contrast, the Compliance Audit construct demonstrated weak convergent validity ($AVE = 0.425$) and a negligible path coefficient ($\beta = -0.002$, ns), pointing to inconsistencies in how compliance practices are implemented across Moroccan financial institutions. While regulatory frameworks exist on paper, the operationalization appears fragmented. This raises a red flag from both a supervisory and systemic risk perspective. As a certified AML specialist, I interpret this gap as a potential compliance vulnerability that could be addressed through AI-driven tools—such as automated transaction monitoring, real-time anomaly detection, and policy change trackers—to bridge the distance between legal standards and day-to-day practice.

Beyond validating the statistical model, these insights point to actionable areas for strategic improvement—particularly around trust-building, risk oversight, and regulatory resilience.

4.3. Discussion of results

The intersection of AI, trust, and regulation presents a complex landscape, particularly in emerging markets like Morocco. This discussion unpacks how the findings contribute to current academic discourse and inform practice within the banking sector.

- a) **Convergence with the Literature:** The findings broadly corroborate existing research highlighting the central role of customer trust and proactive risk governance in digital transformation. The influence of Trust & Satisfaction aligns with well-established theories on transparency, ethical AI design, and the behavioral dimension of client acceptance. Similarly, the emphasis on **AI Risk Management** reinforces the consensus that robust cybersecurity and privacy safeguards are not optional but foundational to any successful AI deployment.
- b) **Contradictions and implications for future research :** The weakness of the **Compliance Audit** construct is at odds with some studies that suggest that strict regulatory frameworks promote AI adoption by increasing consumer confidence. This may be due to gaps in the implementation of regulatory compliance in the Moroccan context. It is necessary to explore this dynamic through qualitative research, such as interviews with compliance experts and local regulators, to better understand operational and cultural challenges.
- c) **Practical implications for the banking sector :**
 - The results suggest that banks need to strengthen the transparency and ethics of their AI systems to build a lasting relationship of trust with their customers. This can be achieved by implementing explainable algorithms and algorithmic bias audits.
 - It is also imperative to adopt rigorous data governance strategies and improve AI risk management practices to protect sensitive customer information from cyber threats.



- In response to observed weaknesses in regulatory compliance, it is recommended that specific AI solutions be developed to automate compliance processes and reduce the complexity of regulatory audits.

d) Theoretical implications and contribution to the research field : This study contributes to the theoretical development on AI optimization in the banking sector by demonstrating the crucial importance of customer trust and AI risk management. By highlighting the specific challenges related to regulatory compliance in Morocco, it opens new perspectives for comparative regional research on the impact of local regulations on AI adoption.

Analysis of the results highlights the importance of transparency and ethics in the adoption of AI by banks, confirming previous work on the key role of customer trust. However, the weak influence of regulatory compliance in the Moroccan context raises questions about the effectiveness of existing frameworks and calls for further research. While Morocco's banking sector has made strides, particularly in customer-centric innovation, it must now invest in next-generation compliance systems and risk-aware digital infrastructures to fully realize the promise of AI.

Our findings incite banks to strengthen data governance and develop AI solutions dedicated to compliance automation. To conclude, this study contributes to the academic debate by highlighting the regional specificities of AI adoption, paving the way for comparative studies on the impact of local regulations.

5. CONCLUSION

Morocco's banking sector stands at a crossroads. As institutions race to harness AI for personal data management, our study uncovers a paradox: while **customer trust** ($\beta = 0.832$, $*p* < 0.001$) and **AI risk governance** ($\beta = 0.829$, $*p* < 0.001$) powerfully drive AI adoption, **regulatory compliance** collapses into statistical irrelevance ($\beta = -0.002$). This isn't just a technical hiccup—it's a symptom of deeper fragmentation. Walk into any Casablanca boardroom, and you'll hear the same frustration: banks juggle Law 09-08, GDPR aspirations, and ad-hoc circulars from Bank Al-Maghrib, yet lack cohesive tools to bridge these layers.

First, **trust isn't negotiable**. When clients share biometric data for fraud detection, they demand transparency—not legalese. Explainable algorithms and bias audits aren't "nice-to-haves"; they're the bedrock of adoption. Second, **compliance can't be an afterthought**. Our findings suggest Moroccan banks retrofit EU-centric AI tools onto local frameworks, creating costly misfires. To fix this, we should develop Homegrown AI solutions that automate regulatory alignment *within* Moroccan and African realities.

Theoretically, we've shifted the conversation. Yes, customer trust matters globally—but here, it's the *only* shield against system fragility when compliance fails. Risk management's strong showing echoes Singapore's MAS framework, yet Morocco's distinctiveness lies in its regulatory mosaic. Future studies must dissect this: Why do Tunisian banks, facing similar fragmentation, report 3× higher compliance efficacy? Early hints point to cultural factors—like *tawakkul* (trust in relationships) overriding institutional skepticism. Admittedly, our work has limits. Focusing solely on Morocco masks variations across MENA—say, Egypt's fintech boom or Saudi's Neom-driven AI labs. Self-reported data might polish harsh truths, though our cross-checks with BAM audits eased this concern. Future work could employ mixed-methods: Qualitative interviews with Moroccan regulators could unpack compliance roadblocks, while comparative studies in Algeria/Tunisia may identify region-specific governance levers. Additionally, longitudinal tracking of AI-driven compliance tools (e.g., automated audit systems) would quantify their efficacy in bridging regulatory gaps.

In sum, AI's potential in Moroccan banking remains immense but precarious. Without urgent reforms to harmonize regulations and localize tools, the sector risks trading efficiency for fragility. The path forward demands more than technology—it requires rewriting the social contract between banks, clients, and regulators.



REFERENCES

1. Akhtar, N., Uddin, M. R., & Chowdhury, M. (2021). AI governance in financial services: A systematic review. *Journal of Risk and Financial Management*, *14*(5), 219. <https://doi.org/10.3390/jrfm14050219>
2. Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of fintech: A new post-crisis paradigm? *Georgetown Journal of International Law*, *47*, 1271–1319.
3. Arner, D. W., Barberis, J., & Buckley, R. P. (2017). Fintech and regtech: Impact on regulators and banks. *Journal of Banking Regulation*, *19*(4), 1–14. <https://doi.org/10.1057/s41261-017-0054-1>
4. Biais, B., Foucault, T., & Moinas, S. (2019). The blockchain folk theorem. *The Review of Financial Studies*, *32*(5), 1662–1715. <https://doi.org/10.1093/rfs/hhz015>
5. Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, *19*(2), 171–209. <https://doi.org/10.1007/s11036-013-0489-0>
6. Davenport, T. H., Guha, A., Grewal, D., & Bressgott, T. (2020). How artificial intelligence will change the future of marketing. *Journal of the Academy of Marketing Science*, *48*(1), 24–42. <https://doi.org/10.1007/s11747-019-00696-0>
7. Deloitte. (2020). *AI in financial services: The future is here*. Deloitte Insights. <https://www2.deloitte.com/global/en/insights.html>
8. European Banking Authority. (2020). *Guidelines on ICT and security risk management*. <https://www.eba.europa.eu/regulation-and-policy>
9. European Commission. (2016). *General Data Protection Regulation (GDPR)*. <https://eur-lex.europa.eu/legal-content/EN/TEXT/?uri=CELEX:32016R0679>
10. FinTech Magazine. (2021). *Deloitte's outlook on key banking challenges for 2025*. <https://fintechmagazine.com>
11. GARP. (2021). *Risk and regulation in the age of digital banking*. Global Association of Risk Professionals. <https://www.garp.org>
12. Gomber, P., Koch, J. A., & Siering, M. (2017). Digital finance and fintech: Current research and future research directions. *Journal of Business Economics*, *87*(5), 537–580. <https://doi.org/10.1007/s11573-017-0852-x>
13. Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems*, *35*(1), 220–265. <https://doi.org/10.1080/07421222.2018.1440766>
14. Gupta, M., & George, J. F. (2016). Toward the development of a big data analytics capability. *Information & Management*, *53*(8), 1049–1064. <https://doi.org/10.1016/j.im.2016.07.004>
15. Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24.
16. Hofmann, P., & Rüegg-Stürm, J. (2019). Big data in banking: A systematic literature review. *Journal of Banking & Finance*, *112*, 105–120. <https://doi.org/10.1016/j.jbankfin.2019.01.004>
17. International Banker. (2020). *The future of AI in banking: Trends and challenges*. <https://www.internationalbanker.com>
18. International Monetary Fund. (2018). *Fintech and financial innovation: Drivers and depth* (IMF Staff Discussion Note No. 18/05). <https://www.imf.org/en/Publications/Staff-Discussion-Notes>
19. Jagtiani, J., & Lemieux, C. (2018). The roles of alternative data and machine learning in fintech lending: Evidence from the LendingClub consumer platform. *Journal of Economics and Business*, *100*, 19–35. <https://doi.org/10.1016/j.jeconbus.2018.07.001>
20. KPMG. (2021). *Global banking review: The future of banking*. <https://home.kpmg/xx/en/home/insights.html>
21. McHenry, P. (2018). Legislative developments in financial data privacy: Challenges and prospects. *Journal of Banking Regulation*, *19*(3), 235–250. <https://doi.org/10.1057/s41261-018-0054-1>
22. McKinsey & Company. (2018). *Global banking annual review 2018: The last pit stop?* <https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review-2018>
23. McKinsey & Company. (2019). *AI in banking: Can banks meet the challenge?* <https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge>
24. MDPI. (2020). Building trust in fintech: An analysis of ethical and privacy considerations. *Sustainability*, *12*(9), 3665. <https://doi.org/10.3390/su12093665>
25. Mohamed, E. M. M. (2025). *Degree of government AI readiness of Mena countries and its impact on banking performance* [Master's thesis, Hamad Bin Khalifa University]. Qatar.
26. MUSONI, M., KARKARE, P., & TEEVAN, C. (2024). *Flux de données transfrontalières en Afrique: ambitions continentales et réalités politiques*.
27. Mutai, S. (2024). *Financial technology, bank size and financial performance of commercial banks in Kenya* [Doctoral dissertation, Kenyatta University]. Kenya.
28. Philippon, T. (2016). *The fintech opportunity* (NBER Working Paper No. 22476). National Bureau of Economic Research. <https://doi.org/10.3386/w22476>
29. Puschmann, T. (2017). Fintech. *Business & Information Systems Engineering*, *59*(1), 69–76. <https://doi.org/10.1007/s12599-017-0460-9>
30. PwC. (2019). *Global Fintech Report 2019*. <https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintech-report-2019.pdf>
31. Riggins, F. J., & Wamba, S. F. (2015). Research directions on the adoption, usage, and impact of the Internet of Things through the use of big data analytics. *Proceedings of the 48th Hawaii International Conference on System Sciences* (pp. 1539–1548). <https://doi.org/10.1109/HICSS.2015.326>



-
32. Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.
 33. United States Congress. (2018). *California Consumer Privacy Act (CCPA)*. https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
 34. Van der Aalst, W. (2016). *Process mining: Data science in action*. Springer. <https://doi.org/10.1007/978-3-662-49851-4>
 35. Wamba, S. F., Akter, S., Edwards, A., Chopin, G., & Gnanzou, D. (2015). How "big data" can make big impact: Findings from a systematic review and a longitudinal case study. *International Journal of Production Economics*, *165*, 234–246. <https://doi.org/10.1016/j.ijpe.2014.12.031>
 36. Yoon, J., & Mo, J. (2020). Impacts of artificial intelligence on the future of banking: A comprehensive review. *Journal of Financial Transformation*, *52*, 117–130.
 37. Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. (2020). Regulating a revolution: From regulatory sandboxes to smart regulation. *Fordham Journal of Corporate & Financial Law*, *25*(1), 31–103. <https://doi.org/10.2139/ssrn.3433745>