



THE 21ST EDITION OF THE INTERNATIONAL CONFERENCE EUROPEAN INTEGRATION REALITIES AND PERSPECTIVES

The New Paradigm of FinTech and CyberSecurity

Balancing Innovation and Responsibility: Ethical and Consumer-Oriented Artificial Intelligence in FinTech

Călin Rangu¹, Carmen Lidia Ioan², Mocanu Andreea-Maria³, Dragomir Florentina Manuela⁴

Abstract: Objectives: This paper looks at the role of artificial intelligence as a financial technology, focusing on ethical considerations and the need for consumer-centric approaches. Its aim is to explore how fairness, transparency, and accountability influence consumer trust and protection in digital financial services. **Previous work:** Existing research highlights the increasing integration of artificial intelligence into financial services, with a focus on risks related to bias, lack of explainability, and data privacy. Studies on responsible machine learning and ethical frameworks in Fintech emphasize the importance of aligning technological innovation with regulatory principles and consumer protection. Existing research highlights efficiency gains and risks, such as algorithmic bias and data privacy issues has explored FinTech and cybersecurity. This work extends to ethical artificial intelligence and consumer protection. **Approach:** The study uses a qualitative methodology based on literature review and comparative analysis of recent academic work, complemented by the author's experience, selected case studies from fintech applications such as credit score and fraud detection. **Results:** The findings indicate that while artificial intelligence increases financial efficiency and inclusion, it also introduces ethical risks, including algorithmic bias and opacity. The implementation of explainable models and ethical governance frameworks significantly improves user trust and transparency of decisions. **Implications:** The study provides insights to researchers and policymakers by highlighting the need for stricter regulatory standards and ethical guidelines to ensure responsible innovation in fintech ecosystems. **Value:** This paper proposes an integrated framework for responsible artificial intelligence and contributes by integrating the ethical principles of artificial intelligence with a consumer-centric perspective, proposing a balanced framework between technological advancement and financial consumer protection.

Keywords: data privacy; fintech ethics; algorithmic bias; digital governance; user trust

JEL classification: G21; O33; D18

1. Introduction

The rapid digitalization of financial services has transformed the architecture of modern financial systems, positioning artificial intelligence (AI) as a central driver of innovation within the FinTech ecosystem. AI-powered applications—including credit scoring, fraud detection, robo-advisory services,

¹ Senior Lecturer, PhD, Danubius International University, Romania, Address: 3 Galați Blvd, Galați, Romania, Corresponding author: calinrangu@univ-danubius.ro.

² Student, Danubius International University, Romania, Address: 3 Galați Blvd, Galați, Romania, E-mail: carmenlidiaioan@yahoo.it.

³ Student, Danubius International University, Romania, Address: 3 Galați Blvd, Galați, Romania, E-mail: andreeamandreea@yahoo.com.

⁴ Student, Danubius International University, Romania, Address: 3 Galați Blvd, Galați, Romania, E-mail: florymicu90@yahoo.com.



Copyright: © 2026 by the authors.
Open access publication under the terms and conditions of the
Creative Commons Attribution-NonCommercial (CC BY NC) license
(<https://creativecommons.org/licenses/by-nc/4.0/>)

and behavioral analytics—have significantly improved operational efficiency, reduced transaction costs, and expanded access to financial products and services (Aldboush & Ferdous, 2023; Ridzuan et al., 2024).

However, the integration of AI into financial decision-making represents more than a technological innovation. It introduces a structural transformation in the relationship between financial institutions and consumers by embedding decision-making processes within complex algorithmic systems. As financial institutions increasingly rely on predictive analytics, automated classification, and large-scale data processing, consumers become subject to decision-making mechanisms that are often difficult to understand, challenge, or contest (Rea, 2020).

A growing body of literature highlights the dual nature of AI in financial services. On the one hand, AI contributes to improved efficiency, enhanced risk management, and greater financial inclusion. On the other hand, algorithmic systems may reproduce historical biases, generate discriminatory outcomes, and create new forms of opacity in financial decision-making (Agu et al., 2024; Rizinski et al., 2022). The increasing reliance on extensive data collection further raises concerns regarding privacy, surveillance, consumer autonomy, and data governance (Moloney et al., 2024).

These developments have significant implications for consumer protection. Traditional consumer protection frameworks were largely designed for environments characterized by human decision-making, contractual transparency, and static information disclosure. AI-driven financial services challenge these assumptions by introducing dynamic personalization, automated profiling, and opaque algorithmic processes that may directly influence consumers' access to credit, pricing conditions, and broader economic opportunities (Aggarwal, 2021; Yang & Lee, 2024).

Within the European Union, these challenges have generated an evolving regulatory response. The Artificial Intelligence Act establishes a risk-based governance framework for AI systems, while complementary instruments such as the Digital Operational Resilience Act (DORA), the NIS2 Directive, the General Data Protection Regulation (GDPR), and the Markets in Crypto-Assets Regulation (MiCA) collectively address operational resilience, cybersecurity, data governance, and consumer protection concerns (Gonçalves, 2024; Jackson & Langenbucher, 2025).

Despite the growing literature on AI governance, existing research frequently examines AI ethics, financial regulation, cybersecurity, and consumer protection as separate domains. Consequently, limited attention has been devoted to understanding how these dimensions interact in practice and how AI-related risks directly affect consumer rights within increasingly automated financial ecosystems (Moloney et al., 2024).

Building on previous research concerning digital financial ecosystems, FinTech innovation, cybersecurity, and cyber risk governance (Badea et al., 2021; Scheau et al., 2022; Rangu et al., 2023; Rangu et al., 2024), this study advances the debate by integrating ethical AI, consumer protection, and European regulatory governance into a unified analytical framework.

1.1. Research Objective and Contribution

The primary objective of this study is to examine how artificial intelligence can be governed in a manner that supports innovation while safeguarding consumer rights and maintaining trust in financial services.

The paper makes five principal contributions:

It conceptualizes AI in FinTech as a potential source of structural consumer risk rather than merely a technological innovation.

It introduces the concept of algorithmic asymmetry to explain emerging power imbalances between financial institutions and consumers.

It links AI-related risks directly to fundamental consumer rights, including fairness, transparency, privacy, autonomy, and access to effective remedies.

It provides an integrated analysis of the European regulatory ecosystem, connecting the AI Act, GDPR, DORA, NIS2, and MiCA.

It proposes a multi-layer governance framework that combines ethical principles, legal obligations, operational safeguards, cybersecurity requirements, and consumer empowerment mechanisms.

1.2. Research Question

The study addresses the following research question:

How can artificial intelligence in FinTech be governed in a manner that promotes innovation while ensuring the effective protection of consumer rights and trust in digital financial services?

1.3. Structure of the Paper

The remainder of the paper is organized as follows. Section 2 reviews literature on AI, ethics, and consumer protection. Section 3 analyzes the principal risks generated by AI-driven financial systems. Section 4 examines the European regulatory framework governing AI in financial services. Section 5 discusses consumer protection mechanisms and ethical implementation requirements. Section 6 develops an integrated governance framework for trustworthy AI in FinTech. Section 7 discusses the theoretical and practical implications of the findings, while Section 8 concludes.

2. Literature Review: Artificial Intelligence, Ethics, and Consumer Protection in the FinTech Era

The growing integration of artificial intelligence into financial services has generated an extensive body of research addressing innovation, operational efficiency, and digital transformation. However, the academic debate remains fragmented, with technological, ethical, legal, and consumer protection perspectives often evolving in parallel rather than through integrated analysis.

2.1. Artificial Intelligence in Financial Services: Efficiency and Structural Risk

Artificial intelligence has become a central component of contemporary financial services, enabling significant improvements in operational efficiency, risk management, fraud detection, customer service, and financial inclusion. AI-driven systems can process large volumes of data, identify patterns beyond human analytical capabilities, and support real-time decision-making across banking, insurance, investment, and digital payment services (Aldboush & Ferdous, 2023; Ridzuan et al., 2024).

The literature, however, increasingly highlights the dual nature of AI deployment in financial services. While AI contributes to innovation and efficiency, it also creates new forms of vulnerability associated

with algorithmic opacity, discriminatory outcomes, privacy risks, and the concentration of informational power within financial institutions (Rea, 2020; Aggarwal, 2021). As AI systems become deeply integrated into financial infrastructures, their impact extends beyond operational performance and directly influences consumers' access to credit, insurance, and broader economic opportunities.

An important limitation in the existing literature is the tendency to evaluate AI primarily through the lens of innovation and efficiency, while insufficient attention is devoted to the structural implications of algorithmic decision-making for consumers. As AI systems increasingly mediate financial interactions, consumers become exposed to algorithmic processes that influence access to financial services through mechanisms that often remain difficult to understand, challenge, or contest (Moloney et al., 2024; Jackson & Langenbucher, 2025).

At the same time, scholars emphasize that algorithmic systems are not neutral instruments. AI models are shaped by the quality of datasets, the assumptions embedded within algorithmic architectures, and the institutional objectives guiding their development and deployment. Consequently, algorithmic systems may reproduce historical inequalities or generate discriminatory outcomes even in the absence of explicit discriminatory intent (O'Neil, 2016; Barocas & Selbst, 2016; Rea, 2020; Rizinski et al., 2022).

Literature increasingly recognizes that algorithmic bias should not be interpreted merely as a technical malfunction, but as a socio-technical governance problem with significant legal, ethical, and societal implications. Within financial services, discriminatory algorithmic outcomes may shape access to credit, insurance, and other forms of economic participation, thereby transforming AI-related risks into broader questions concerning fairness, financial inclusion, and structural inequality (Barocas & Selbst, 2016; Selbst et al., 2019; Agu et al., 2024; Yang & Lee, 2024).

2.2. Ethical AI and the Governance Challenge

The growing influence of AI in financial services has stimulated extensive research on ethical AI and responsible innovation. Despite differences in terminology and methodology, most ethical frameworks converge around several core principles, including fairness, transparency, accountability, privacy protection, human oversight, and non-discrimination (Floridi et al., 2018; Fjeld et al., 2020).

While these principles are widely accepted through academic, regulatory, and industry discussions, a major limitation identified in the literature concerns the persistent gap between normative ethical frameworks and their practical implementation. Many studies formulate high-level ethical principles related to fairness, transparency, accountability, and human oversight, yet provide limited guidance regarding how these principles can be operationalized within complex real-world AI systems characterized by adaptive algorithms, large-scale data processing, and evolving institutional objectives (Mittelstadt, 2019; Morley et al., 2020; Floridi et al., 2018; Fjeld et al., 2020).

One of the major criticisms advanced in recent scholarship is that ethical AI discussions frequently remain at a declarative and aspirational level. Ethical principles are often articulated in broad normative terms, while concrete implementation, monitoring, and enforcement mechanisms remain insufficiently developed. Consequently, several scholars argue that AI ethics frameworks risk becoming forms of “soft governance” or “ethics washing” unless they are supported by operational safeguards, accountability mechanisms, and binding regulatory obligations (Floridi et al., 2018; Mittelstadt, 2019; Morley et al., 2020; Moloney et al., 2024).

Recent studies increasingly advocate for the adoption of concrete governance mechanisms capable of translating ethical AI principles into operational practice. These mechanisms include algorithmic audits, explainable AI systems, mandatory governance procedures, and human oversight requirements designed to strengthen accountability, transparency, procedural fairness, and regulatory compliance in AI-driven decision-making environments (Morley et al., 2020; Doshi-Velez & Kim, 2017; Rizinski et al., 2022; European Parliament & Council of the European Union, 2024).

2.3. Consumer Protection in the Age of Algorithmic Finance

The expansion of AI-driven financial services challenges many of the assumptions underlying traditional consumer protection frameworks. Historically, consumer protection mechanisms have relied on transparency obligations, disclosure requirements, and informed consent to address information asymmetries between financial institutions and consumers.

However, algorithmic systems generate highly personalized and dynamic outcomes, thereby reducing the effectiveness of traditional disclosure-based approaches. Consumers may receive individualized pricing structures, recommendations, or risk assessments generated through opaque computational processes that remain difficult to observe, interpret, or contest. In such environments, the traditional concept of informed consent becomes increasingly problematic because consumers frequently lack the technical understanding necessary to evaluate how algorithmic systems process personal data, generate predictive inferences, and influence financial outcomes (Calo, 2014; Citron & Pasquale, 2014; Rea, 2020; Moloney et al., 2024).

Furthermore, AI systems enable increasingly sophisticated forms of behavioral profiling and personalization. While such capabilities may improve customer experience and service delivery, they may also facilitate manipulative practices, exploit cognitive vulnerabilities, or influence consumer decision-making in ways that challenge traditional notions of autonomy and fairness (Helberger et al., 2022).

As a result, several scholars argue that consumer protection in digital finance must evolve beyond traditional transactional and disclosure-based models toward a broader systemic governance perspective capable of addressing the structural effects of algorithmic decision-making, data asymmetries, behavioral influence, and automated financial profiling within increasingly digitalized financial ecosystems (Helberger et al., 2022; Moloney et al., 2024; Citron & Pasquale, 2014; Zarsky, 2016).

2.4. Research Gap and Positioning of the Study

Although the literature on AI ethics, financial innovation, consumer protection, and digital governance has expanded significantly in recent years, several gaps remain.

First, existing research frequently analyzes AI through either a technological or regulatory perspective, while limited attention is devoted to the direct relationship between AI systems and consumer rights within financial ecosystems (Moloney et al., 2024; Jackson & Langenbacher, 2025).

Second, studies often examine ethical AI, cybersecurity, operational resilience, and consumer protection as separate domains, despite the growing interdependence between these areas in AI-driven financial services.

Third, relatively limited attention has been devoted to the interaction between the emerging European regulatory framework—including the AI Act, GDPR, DORA, NIS2, MiCA, and consumer protection legislation—and the practical governance of AI-related consumer risks.

To address these gaps, this paper develops an integrated governance perspective that connects ethical AI principles, consumer protection requirements, cybersecurity obligations, and financial regulation within a unified analytical framework. The study introduces the concepts of algorithmic asymmetry and systemic consumer risk to explain how AI-driven financial systems may reshape the relationship between financial institutions and consumers, while proposing a multi-layer governance framework for trustworthy and consumer-centric AI deployment in FinTech.

3. Lack of Operational Models

Most studies remain conceptual; there is a lack of integrated governance models capable of connecting: ethical principles, regulatory obligations, operational safeguards, and consumer protection mechanisms.

This paper addresses these gaps by proposing a multi-layer governance framework that links AI ethics directly to consumer rights and integrates the European regulatory ecosystem into a coherent analytical model.

Unlike approaches that analyze AI-related risks primarily from the perspective of institutional compliance or technological efficiency, this study positions consumer protection as the central organizing principle of AI governance in FinTech. In doing so, it reframes AI governance not merely as a technological or regulatory challenge, but as a broader issue of economic fairness and trust in digital financial systems. Thus, it contributes to a more comprehensive understanding of responsible artificial intelligence in the FinTech era as a combined ethical, legal and socio-economic challenge.

3.1. Artificial Intelligence and Consumer Rights in FinTech: Risks, Misuse and Structural Impact

The integration of artificial intelligence into financial services is frequently associated with efficiency, personalization, and innovation. However, beyond these widely discussed benefits, AI systems also transform the relationship between financial institutions and consumers in ways that generate new categories of vulnerability and risk.

Unlike traditional financial technologies, AI-driven systems do not simply automate predefined processes. Instead, they continuously generate predictions, classifications, and decisions based on large-scale data analysis and adaptive learning mechanisms. As a result, consumers are increasingly evaluated, categorized, and influenced through opaque computational processes that operate beyond their visibility or control.

This transformation produces what can be described as algorithmic asymmetry: a structural imbalance in which financial institutions possess superior access not only to information, but also to predictive capabilities, behavioral insights, and automated decision-making infrastructures.

The significance of this asymmetry extends beyond technical complexity. It fundamentally alters the conditions under which consumers access financial services, shifting power toward institutions capable of combining data extraction, predictive analytics, and automated behavioral influence. In this context, AI becomes not only a technological instrument, but also a mechanism capable of shaping economic opportunities and consumer behavior at scale (Rea, 2020).

3.2. Algorithmic Discrimination and Unequal Financial Access

One of the most extensively discussed risks associated with AI in financial services is algorithmic discrimination. Machine learning systems rely on historical data to identify patterns and generate predictions. However, historical datasets often contain embedded socio-economic inequalities, exclusion patterns, or discriminatory outcomes.

Consequently, AI systems may reproduce or amplify such patterns, even in the absence of explicit discriminatory intent.

The implementation of artificial intelligence in financial services does not only introduce new tools, but it also fundamentally reshapes the relationship between financial institutions and consumers. AI systems integrate decision-making processes into complex, data-driven models, shifting control from human actors to algorithmic systems.

This transformation creates a new form of structural asymmetry of power, where financial institutions hold extensive datasets, advanced computational capabilities, proprietary algorithms, while consumers remain largely opaque subjects of algorithmic evaluation.

Unlike traditional financial asymmetries — based on information or expertise — AI introduces algorithmic asymmetry, where decisions are automated, reasoning is inaccessible, results are difficult to dispute (Rea, 2020).

In the context of financial services, this issue is particularly relevant for credit scoring, lending decisions, insurance pricing, and fraud detection systems. AI systems are based on historical data, which can reflect socio-economic inequalities, systemic biases, and historical patterns of exclusion.

This leads to unequal access to credit, higher costs for certain groups, indirect discrimination without explicit intent. From a legal perspective, such results call into question fundamental principles such as non-discrimination and equal access to financial services.

Variables such as geographic location, digital activity patterns, spending behavior, and employment history may function as indirect proxies for protected characteristics, generating discriminatory effects against vulnerable groups (Agu et al., 2024).

Unlike traditional discrimination, algorithmic discrimination is often difficult to identify because it is embedded within complex statistical models rather than explicit institutional policies. This creates a situation in which discriminatory outcomes may appear technically neutral while producing significant social and economic inequalities in practice (Rizinski et al., 2022).

The implications for consumer rights are substantial. Algorithmic bias may restrict access to financial services, increase borrowing costs, and reinforce existing socio-economic disparities.

As a result, AI-related discrimination challenges core principles of equal treatment, fairness, and financial inclusion.

3.3. Opaque Decision-Making and the Erosion of Transparency

A central characteristic of many AI systems is their limited explainability. Complex machine learning models, particularly deep learning architectures, often generate outcomes that are difficult to interpret even for their developers.

In financial services, this lack of transparency directly affects consumers' ability to understand decisions, evaluate fairness, and challenge outcomes

Consumers may receive loan rejections, risk classifications, and differentiated pricing without meaningful explanations regarding the criteria used, the variables influencing decisions, the weighting of data inputs.

This situation creates a significant tension between technological complexity and the practical enforceability of consumer rights. While legal frameworks such as the GDPR formally recognize rights related to automated decision-making and access to meaningful information, the technical opacity of AI systems often limits the effectiveness of these protections in practice.

Furthermore, institutions may invoke trade secrecy, intellectual property concerns, technical complexity as reasons for limiting disclosure.

This creates what may be described as a transparency paradox: the more sophisticated AI systems become, the more difficult it becomes for consumers to understand the mechanisms that shape their financial opportunities (Moloney et al., 2024). Algorithmic discrimination is often difficult to detect due to the complexity of the model, lack of transparency, and absence of audit mechanisms. This creates a situation where discrimination becomes systemic but invisible.

The lack of meaningful explainability may also conflict with broader European consumer protection principles requiring clear and understandable information for consumers. Article 5 of the Consumer Rights Directive (Directive 2011/83/EU) establishes transparency obligations intended to ensure informed consumer decision-making. However, algorithmic systems challenge the practical implementation of these requirements because highly complex AI models often remain inaccessible to ordinary consumers. A defining feature of many AI systems is their opacity, often referred to as the "black box" problem. In financial services, this has direct implications for consumers, who may not be able to understand why a loan application was rejected, how risk scores are calculated, and why different prices apply.

This lack of transparency undermines the right to information, a cornerstone of consumer protection frameworks.

According to the General Data Protection Regulation (GDPR), individuals have the right to meaningful information about automated decisions and the right not to be subject exclusively to automated decision-making in certain contexts.

However, in practice explanations are often superficial, technical complexity limits interpretability, institutions can rely on trade secret arguments (Moloney et al., 2024). Thus, there is a growing gap between formal rights and effective transparency.

3.4. Behavioral Manipulation and Exploitation of Consumer Vulnerability

Artificial intelligence enables financial institutions to move beyond prediction toward behavioral influence. Through behavioral analytics, personalization systems, and predictive profiling institutions

can anticipate consumer preferences and tailor financial interactions accordingly. Although personalization may improve customer experience, it also creates opportunities for manipulative practices, exploitative nudging, and asymmetrical persuasion strategies

AI systems may encourage consumers toward higher-cost products, excessive borrowing, and financially unfavorable decisions by exploiting cognitive biases, emotional triggers, and behavioral vulnerabilities, exploiting cognitive biases (e.g., urgency, loss aversion), reinforcing suboptimal financial decisions. Such practices align with the broader concept of “dark patterns” in digital environments (Ridzuan et al., 2024).

This development represents a significant transformation in the nature of consumer risk. Traditionally, financial consumer protection focuses on misleading information or contractual imbalance. AI-driven systems, however, introduce more subtle forms of influence in which consumer behavior itself becomes an object of algorithmic optimization (Ridzuan et al., 2024).

This raises fundamental questions concerning autonomy, informed consent, freedom of economic choice. In this context, consumers risk becoming not only users of financial services, but also subjects of continuous behavioral monitoring and optimization processes.

AI enables unprecedented levels of personalization in financial services. While personalization can improve the user experience, it also creates the potential for behavioral manipulation.

From a consumer protection perspective, this raises critical concerns. Is the consumer making a free and informed decision? Or is the decision slightly modified?

The risks associated with AI-driven behavioral influence may also be examined through the perspective of European consumer protection law, particularly the Unfair Commercial Practices Directive (Directive 2005/29/EC). The Directive prohibits commercial practices that materially distort consumer behavior through misleading or aggressive mechanisms. In AI-driven financial environments, highly personalized algorithmic systems capable of exploiting cognitive vulnerabilities may generate practices functionally like digital “dark patterns,” thereby raising concerns regarding manipulation, autonomy, and fairness in consumer decision-making (European Parliament & Council, 2005; Helberger et al., 2022).

3.5. Data Exploitation and Surveillance-Oriented Finance

AI-driven financial systems depend heavily on large-scale data extraction and continuous behavioral monitoring.

The range of data processed increasingly includes transactional records, geolocation data, browsing behavior, social media activity, and device interactions. Such practices enable highly granular consumer profiling.

While institutions justify extensive data collection through fraud prevention, personalization, risk assessment, the accumulation of behavioral data also expands institutional surveillance capabilities.

Recent developments suggest the emergence of what may be characterized as “surveillance-oriented finance,” in which continuous data collection becomes structurally integrated into financial decision-making. In such systems, consumers are not assessed solely based on financial indicators, but through broader behavioral and digital profiles that extend far beyond traditional banking relationships (Moloney et al., 2024).

This evolution raises concerns regarding proportionality and data minimization – AI systems often collect more data than necessary, conflicting with GDPR principles; purpose limitation - data collected for a purpose may be reused for risk profiling or marketing; long-term profiling; and consumer autonomy. Moreover, consumers frequently lack genuine understanding of how data is processed, how profiles are generated, how algorithmic conclusions affect financial outcomes. Thus, formal consent mechanisms may provide only limited protection in practice - consumers can give formal consent, but they lack a real understanding of how data is used and how decisions are made (Moloney et al., 2024).

3.6. Accountability Gaps and Automated Governance

AI systems complicate traditional accountability structures because decision-making processes involve multiple actors as financial institutions, AI developers, cloud providers, data aggregators, and third-party vendors. This fragmentation creates uncertainty regarding responsibility for biased outcomes, incorrect decisions, cybersecurity failures, and consumer harm (Rizinski et al., 2022). In practice, this can lead to accountability gaps, where no actor takes full responsibility, consumers face barriers in the search for remedies.

As AI systems become increasingly autonomous and interconnected, accountability risks becoming diluted across technological ecosystems. Consumers may face significant obstacles in identifying responsible actors or obtaining effective remedies, particularly when decisions are generated through proprietary and opaque systems (Rizinski et al., 2022).

This problem is particularly significant in highly automated financial environments where human oversight is limited, decisions occur in real time, algorithms continuously evolve. As a result, traditional ex-post-consumer protection mechanisms may become insufficient.

3.7. Mapping AI risks to Consumer Rights

The risks discussed above directly affect the fundamental rights of consumers according to Table 1. Artificial intelligence transforms consumer risk from isolated incidents into systemic risks, embedded in financial infrastructures.

Table 1. Risks of AI to Fundamental Consumer Rights

Consumer law	AI-related risk
Right to fair treatment	Algorithmic bias, discrimination
Right to information	Lack of transparency, black box models
Right to privacy	Excessive data collection, surveillance
Right to autonomy	Behavioral manipulation
Right to reparation	Lack of responsibility

Traditional consumer risks were generally transactional, isolated, and identifiable after occurrence. AI-related risks are instead systemic, embedded in infrastructures, scalable across populations, and difficult to detect.

This study conceptualizes these dynamics as “systemic consumer risk,” referring to risks generated by algorithmic systems that continuously influence financial access, pricing, and opportunities across large groups of consumers. Unlike isolated cases of misconduct, systemic consumer risks are embedded

within the architecture of digital financial ecosystems themselves (Aldboush & Ferdous, 2023; Rea, 2020).

This perspective implies that consumer protection can no longer focus exclusively on individual transactions or contractual disclosures. Instead, governance must address the design, deployment, and supervision of algorithmic systems at the structural level.

3.8. Synthesis

The analysis demonstrates that artificial intelligence fundamentally transforms the nature of consumer vulnerability in financial services. AI introduces a new risk category that can be described as systemic risk for consumers, characterized by integration into basic financial processes, scalability in large populations, opacity and difficulty of detection, cumulative impact on vulnerable groups. This shifts the focus of consumer protection from individual transactions to system-wide governance of algorithms.

AI-related risks extend beyond operational failures, technical errors, cybersecurity incidents and increasingly affect fairness, autonomy, transparency, and access to economic opportunities.

Consequently, the governance of AI in FinTech should not be approached solely as a matter of technological regulation, but as a broader challenge concerning economic justice, democratic accountability, and trust in digital financial systems.

4. European Regulatory Framework: Integrating AI Governance, Cybersecurity and Consumer Protection

4.1. From Fragmentation to Multi-Level Governance - Integrating AI Governance, Cybersecurity and Consumer Protection

The rapid integration of artificial intelligence into financial services has generated significant regulatory challenges for policymakers and supervisory authorities. Unlike traditional financial technologies, AI systems operate through adaptive, data-intensive, and often opaque mechanisms that simultaneously raise concerns related to consumer protection, cybersecurity, operational resilience, market integrity, and accountability.

As a result, the governance of AI in FinTech cannot be addressed through isolated legal instruments. Instead, it requires interconnected regulatory architecture capable of responding to technological, operational, and societal risks simultaneously.

The European Union has emerged as one of the most proactive jurisdictions in this area through the development of a multi-layer regulatory ecosystem that combines AI governance rules, cybersecurity obligations, operational resilience requirements, and financial market regulations. There are four key frameworks are particularly relevant: AI Act – Governance of Artificial Intelligence Systems, DORA (Digital Operational Resilience Act) – ICT Risk and Resilience, NIS2 Directive – Cybersecurity Obligations, MiCA (Regulation of Markets in Crypto-Assets) – Market Integrity and Consumer Protection (European Union, 2024; European Union, 2022a; European Union, 2022b; European Union, 2023).

While each of these tools addresses distinct risks, their combined effect creates a multi-layered governance architecture.

Rather than creating a single unified framework for digital finance, the EU approach relies on the interaction of complementary regulations that collectively shape the governance environment for AI-driven financial systems. This regulatory model reflects the recognition that AI-related risks cannot be separated from broader concerns regarding cybersecurity, systemic resilience, and consumer trust.

4.2. The AI Act: From Ethical Principles to Binding Obligations

The Artificial Intelligence Act represents the first comprehensive attempt to establish harmonized rules for AI governance within the European Union. Unlike voluntary ethical guidelines, the AI Act transforms normative principles into legally enforceable obligations through a risk-based regulatory framework.

Under the AI Act, AI systems are classified according to their potential impact on health, safety, and fundamental rights. Financial applications such as creditworthiness assessment, credit scoring, and insurance risk evaluation are considered high-risk AI systems because they directly influence individuals' economic opportunities and access to essential financial services (European Parliament & Council of the European Union, 2024).

This classification is particularly relevant in the context of consumer protection because it acknowledges that algorithmic systems may affect fundamental rights through discriminatory outcomes, opaque decision-making, and exclusionary practices.

The significance of the AI Act lies not only in its regulatory scope, but also in its conceptual approach. By linking AI governance to the protection of fundamental rights, the regulation implicitly recognizes that algorithmic systems may generate structural forms of consumer vulnerability that extend beyond traditional financial risks.

AI Act is the cornerstone of AI governance in the European Union, introducing a risk-based classification system.

The European approach to AI governance is strongly connected to the protection of fundamental rights under the Charter of Fundamental Rights of the European Union, including Article 7 (respect for private life), Article 8 (protection of personal data), Article 21 (non-discrimination), and Article 38 (consumer protection).

In this context, the AI Act reflects a broader constitutional approach to digital governance in which consumer protection and fundamental rights are treated as core elements of trustworthy artificial intelligence.

- For high-risk AI systems, financial institutions need to directly address algorithmic discrimination, consumer right to information, address automation risks and liability gaps, connect AI governance with cyber risk frameworks, implementing;
- Risk Management Systems by continuous identification and mitigation of risks; life cycle approach (design - implementation - monitoring);
- Data governance requirements, by high-quality datasets, bias detection and mitigation, relevance and representative;
- Transparency obligations, by clear information for users, explainability of the results;
- Human supervision, by mechanisms for intervention or annulment of decisions;
- Accuracy, Robustness and Cybersecurity, by resilience against manipulation, protection against adversarial attacks.

4.2.1. Risk Management Systems

Organizations must establish continuous risk management mechanisms covering development, deployment, monitoring, and post-market supervision.

These obligations require institutions to identify and mitigate risks throughout the lifecycle of AI systems (European Union, 2024).

4.2.2. Data Governance and Bias Mitigation - Basic Obligations under the AI Act

The AI Act imposes strict requirements concerning data quality, relevance, representativeness, and bias mitigation. These provisions directly address concerns related to algorithmic discrimination and unequal treatment in financial services.

Research on algorithmic bias demonstrates that historical datasets may reproduce socio-economic inequalities and exclusionary patterns if not carefully supervised (Agu et al., 2024; Rizinski et al., 2022).

In practice, these requirements represent an important shift from reactive consumer protection toward preventive governance of algorithmic systems. Instead of addressing discriminatory outcomes only after harm occurs, the AI Act seeks to reduce systemic risks during the design and training stages of AI development.

4.2.3. Transparency and Explainability Requirements

The regulation also introduces obligations regarding transparency, documentation, explainability, and traceability. Consumers affected by AI-driven decisions must receive meaningful information regarding the functioning of such systems. This aligns with broader European data protection principles established under the GDPR, particularly in relation to automated decision-making (Regulation (EU) 2016/679).

However, several scholars note that practical implementation remains difficult due to technical complexity, proprietary algorithms, and limited interpretability of advanced models (Doshi-Velez & Kim, 2017; Moloney et al., 2024).

Article 22 of the General Data Protection Regulation establishes safeguards concerning automated individual decision-making, including decisions based solely on automated processing that significantly affect individuals. These safeguards include the right to obtain human intervention, express one's point of view, and contest decisions. In AI-driven financial services, these protections are particularly relevant for credit scoring and automated risk assessment systems (Regulation (EU) 2016/679).

4.2.4. Human Oversight and Accountability

A central principle of the AI Act is the requirement for human oversight mechanisms capable of supervising AI systems, intervening in automated processes, and overriding algorithmic decisions where necessary. This requirement reflects broader concerns regarding accountability gaps in highly automated financial environments.

The introduction of mandatory human oversight implicitly challenges narratives promoting fully autonomous financial decision-making systems. It acknowledges that human judgment remains

necessary to preserve procedural fairness and prevent excessive dependence on opaque algorithmic processes.

Although the AI Act provides a solid foundation, limitations remain as compliance can become formal (ticking the box), explainability requirements remain technically challenging, law enforcement depends on national authorities. Thus, although the AI Act operationalizes ethical principles, efficiency depends on implementation.

4.3. DORA and Operational Resilience of AI-Driven Financial Systems

While the AI Act focuses primarily on governance and fundamental rights, the Digital Operational Resilience Act (DORA) addresses the operational dimension of digital finance.

DORA establishes comprehensive requirements regarding ICT risk management, incident reporting, resilience testing, and third-party risk supervision (European Union, 2022a).

The relevance of DORA for AI governance is particularly significant because AI systems increasingly depend on cloud infrastructures, external data providers, third-party AI vendors.

As a result, operational disruptions affecting AI systems may generate systemic instability, service interruptions, and cybersecurity vulnerabilities.

DORA therefore complements the AI Act by extending governance beyond algorithmic behavior toward the resilience of the technological infrastructures supporting AI-driven financial services. In this sense, trustworthy AI requires not only fairness and transparency, but also operational continuity and systemic robustness.

While the AI Act governs how AI should behave, DORA regulates how AI systems must remain operational and resilient under pressure.

4.4. NIS2 Directive: Cybersecurity as a Foundation of Trust

The NIS2 Directive strengthens cybersecurity obligations for entities operating critical digital infrastructures, including important financial actors. The directive introduces obligations related to cybersecurity risk management, incident response, supply chain security, and governance accountability (European Union, 2022b).

The connection between NIS2 and AI governance is increasingly important because AI systems create new categories of cyber risk, including adversarial attacks, model manipulation, data poisoning, and unauthorized data extraction.

These risks demonstrate that AI governance cannot be separated from cybersecurity governance. An AI system that is technically accurate but vulnerable to manipulation may still generate harmful outcomes for consumers and financial markets. Consequently, cybersecurity becomes a precondition for trustworthy AI deployment in financial services.

Recent research highlights that cyber resilience is becoming an essential component of AI governance frameworks in digital finance, particularly in highly interconnected financial ecosystems dependent on data-intensive infrastructures (Rangu et al., 2024; Moloney et al., 2024).

Without cybersecurity (NIS2), ethical and transparent AI (AI Act) cannot operate reliably.

4.5. MiCA: Consumer Protection in Crypto and AI-Powered Digital Finance

The Markets in Crypto-Assets Regulation (MiCA) addresses risks associated with crypto-assets and digital financial markets.

Although MiCA does not focus exclusively on artificial intelligence, its relevance for AI governance is growing because AI technologies are increasingly integrated into crypto trading systems, automated investment platforms, and digital asset risk management tools (European Union, 2023).

MiCA introduces requirements regarding transparency, disclosure obligations, governance standards, and consumer protection measures.

The interaction between AI systems and crypto-assets may amplify risks due to the combination of automation, market volatility, and limited consumer understanding of complex digital financial products. In such contexts, algorithmic systems may significantly influence investment behavior and risk exposure without sufficient transparency or accountability mechanisms.

4.6. Regulatory Fragmentation and Governance Challenges

The interaction of these frameworks creates a multidimensional governance structure, presented in Table 2.

Table 2. Multidimensional governance structure

Layer	Regulation	Function
Ethics/AI	AI Act	Fairness, transparency, accountability
Operational	DORA	Resilience, IT process management, risk management, continuity
Cybersecurity	NIS2	Cybersecurity
Financial market	Small	Consumer protection, market integrity

Despite the sophistication of the European regulatory framework, several governance challenges remain.

First, the coexistence of multiple regulatory instruments may generate overlapping compliance obligations, regulatory complexity, and inconsistent supervisory practices.

Second, implementation capacity varies significantly between institutions and jurisdictions.

Third, smaller FinTech firms may face disproportionate compliance burdens due to technical requirements, governance obligations, and reporting standards (Jackson & Langenbucher, 2025).

These challenges illustrate a broader tension between innovation and regulation. While robust governance mechanisms are necessary to protect consumers and maintain trust, excessive regulatory complexity may limit innovation capacity or reinforce the dominance of large technology-intensive financial actors.

4.7. Toward an Integrated Governance Perspective

The analysis demonstrates that no individual regulation can address the full range of risks associated with AI in financial services.

Instead, the AI Act governs algorithmic behavior and fundamental rights, DORA addresses operational resilience, NIS2 focuses on cybersecurity, MiCA strengthens market integrity and consumer protection. Together, these instruments create a multi-layer governance ecosystem.

This paper argues that the effectiveness of AI governance in FinTech depends less on the existence of isolated regulations and more on the degree of coordination between legal, technical, and operational governance mechanisms. Consumer protection emerges not from a single regulatory instrument, but from the interaction of multiple layers of oversight, accountability, and resilience.

5. Mechanisms for Consumer Protection and Ethical Implementation of Artificial Intelligence

5.1. From Risk Identification to Protection Architecture

The analysis of AI-related risks in financial services demonstrates that consumer protection can no longer rely solely on traditional mechanisms. Instead, it requires a multi-layered protection architecture that combines legal rights, technical guarantees and institutional responsibilities.

In contrast to conventional financial risks, AI-related risks are integrated into decision-making systems, are difficult to detect *ex ante*, are scalable across large populations. As a result, effective consumer protection must operate simultaneously at several levels.

5.2. Transparency and Explainability – From Formal Disclosure to Meaningful Understanding

Traditional consumer protection relies heavily on disclosure (terms and conditions, risk statements). However, in AI-based systems, disclosure alone is insufficient because decisions are dynamically generated, models are highly complex, explanations are often unintuitive (Rea, 2020).

Explainable Artificial Intelligence (XAI) must be used as a protection mechanism. Explainability must go beyond formal compliance and allow for understandable explanations of decisions, contextual information relevant to consumers, actionable insights (e.g. how to improve solvency). This aligns with the requirements of the GDPR (right to material information) and transparency obligations in the AI Act.

Practical challenges are generated by trade-offs between accuracy and explainability, technical limitations of complex models, the risk of “pseudo-explanations”.

Transparency must be assessed in terms of its usefulness to consumers, not just its formal existence.

5.3. Human Oversight and Hybrid Decision-Making

There are limits to full automation, fully automated decision-making introduces accountability gaps, inability to address exceptional cases, reduced flexibility.

A Human-in-Loop system must be ensured. Effective governance requires hybrid systems where AI supports decision-making, people retain ultimate control, there are override mechanisms. This is explicitly required by the AI Act for high-risk systems.

The dimension of consumer rights must be clearly identified. Consumers should have the right to request human review, have access to appeal mechanisms and be protected against purely automated decisions. This will strengthen procedural fairness.

5.4. Algorithmic Audits and Accountability Mechanisms

There is a need for independent verification. Given the opacity of AI systems, internal controls are insufficient. External mechanisms such as independent audits, regulatory inspections, third-party verifications are needed (Rizinski et al., 2022).

There can be several types of audits, such as bias audits to detect discrimination, performance audits to assess accuracy, or compliance audits to verify compliance with regulations

Financial institutions need to establish an accountability framework by developing document templates, ensuring the traceability of decisions, and assigning accountability for results. This directly addresses the previously identified accountability gap.

5.5. Data Governance and Consumer Rights over Data

Financial institutions need to strengthen GDPR principles so that AI systems need to minimize the need for data, limit purpose, ensure data accuracy, and comply with security requirements (Moloney et al., 2024).

Consumers need to be empowered so that they can access their data, correct inaccuracies, delete data, and most importantly understand how data is used.

There is often a gap between formal rights and the practical usability of these rights. This requires improved interfaces and communication mechanisms, not just legal provisions.

The Digital Services Act further strengthens the European regulatory approach by prohibiting certain deceptive interface designs and manipulative practices commonly referred to as “dark patterns.” Although primarily focused on digital platforms, the principles established under Regulation (EU) 2022/2065 are increasingly relevant in AI-driven financial services, where algorithmic personalization may influence consumer choices through opaque behavioral targeting mechanisms.

5.6. Institutional Obligations: From Compliance to Accountability

Ethical AI is becoming a corporate obligation. Financial institutions need to go beyond compliance and adopt ethical approaches from the design phase, internal governance frameworks, AI risk management systems/

Institutions using AI must ensure that they comply with some basic responsibilities regarding the correctness of results, transparency of processes, robustness and security, continuous monitoring.

These obligations are strengthened by integration with EU regulations through AI Act – system requirements, DORA – operational resilience, NIS2 – cybersecurity, MiCA – consumer protection. Institutions need to navigate a complex compliance ecosystem, which requires integrated governance.

5.7. Towards a Multi-Layered Consumer Protection Model

Based on the analysis, effective protection requires five interconnected layers:

- Legal layer (AI Act, GDPR, DORA, NIS2, MiCA, Applicable rights and obligations)
- Technical layer (Mitigating bias, Explainability, System robustness)
- Operational layer (Risk management, Monitoring, Audits)
- Cybersecurity Layer (NIS2 compliance, DORA Resilience Requirements)
- Consumer Empowerment Layer (Access to information, Repair mechanisms, Human supervision)

The evolving European regulatory framework increasingly emphasizes consumer empowerment as a central governance objective. This reflects a broader transition from passive consumer protection models toward approaches designed to strengthen consumer agency, transparency, and contestability in highly automated digital environments.

5.8. Restoring Balance: From Asymmetry to Trust

The combination of these mechanisms aims to address the fundamental problem identified in Section 3: power asymmetry. Effective consumer protection in AI-powered finance requires reducing information asymmetry and increasing accountability.

This paper argues that consumer protection in AI-powered financial services must be understood as a system-level governance challenge, which requires the integration of legal rights, technical safeguards and institutional responsibilities.

6. An Integrated Governance Framework for Ethical and Consumer-Centric AI in FinTech

6.1. From Fragmentation to Integration

The analysis developed in the previous sections highlights a fundamental limitation in both the academic literature and regulatory practice: the treatment of artificial intelligence, consumer protection and financial regulation as separate areas.

However, in real-world FinTech ecosystems, AI systems are integrated into financial processes, financial services operate under regulatory constraints, and consumer risks arise at the intersection of these layers.

This fragmentation leads to incomplete risk assessment, inconsistent regulatory enforcement, gaps in consumer protection

Effective AI governance in the FinTech era requires an integrated, multi-layered framework that aligns ethical principles, legal obligations, operational mechanisms and consumer rights.

6.2. Structure of The Proposed Framework

The proposed framework is structured in five interdependent layers, each addressing a specific dimension of AI governance.

6.2.1. The Ethical Layer - Normative Foundation: Ethical Principles and Fundamental Rights

The first layer of the framework consists of ethical and fundamental rights principles that establish the normative foundation for trustworthy AI.

These principles include fairness, transparency, accountability, non-discrimination, human autonomy, and consumer protection (Agu et al., 2024; Rizinski et al., 2022).

Within the European context, these values are reinforced through the Charter of Fundamental Rights of the European Union, particularly Article 7 (respect for private life), Article 8 (protection of personal data), Article 21 (non-discrimination), Article 38 (consumer protection) (European Union, 2012).

The integration of consumer protection into the broader framework of fundamental rights represents a distinctive characteristic of the European approach to AI governance. Rather than treating consumer protection solely as a market regulation issue, the EU increasingly frames algorithmic fairness and transparency as essential conditions for safeguarding democratic values and economic participation in digital societies.

This normative foundation is particularly important because AI systems may influence access to credit, insurance pricing, financial inclusion, economic opportunities, hereby directly affecting individuals' socio-economic position.

6.2.2. Legal and Regulatory Governance Layer

The second layer of the framework consists of binding legal obligations established through the European regulatory ecosystem.

This layer includes the AI Act, GDPR, DORA, NIS2, MiCA, and consumer protection legislation. Together, these instruments create a multi-level governance architecture addressing different dimensions of AI-related risk.

6.2.2.1. AI Act and High-Risk Systems

The AI Act establishes obligations for high-risk AI systems used in areas such as credit scoring, insurance evaluation, and financial profiling (European Parliament & Council of the European Union, 2024)

These obligations include risk management systems, data governance requirements, transparency obligations, human oversight, and cybersecurity safeguards.

Importantly, the AI Act operationalizes ethical principles through enforceable governance obligations. This represents a significant transition from voluntary ethical AI frameworks toward legally binding mechanisms capable of addressing systemic consumer risks associated with automated financial decision-making.

6.2.2.2 GDPR and Automated Decision-Making

The General Data Protection Regulation provides an additional layer of protection concerning personal data processing, profiling, and automated decision-making. Article 22 GDPR establishes safeguards

against decisions based solely on automated processing that produce legal or similarly significant effects on individuals (Regulation (EU) 2016/679).

Consumers also benefit from rights related to access to personal data, rectification, erasure, and transparency regarding processing activities.

These safeguards are particularly relevant in AI-driven financial environments where algorithmic systems continuously process behavioral and transactional data to generate predictive assessments concerning creditworthiness, risk, and consumer behavior.

6.2.2.3 Consumer Protection Legislation

Traditional consumer protection frameworks also remain highly relevant in AI-driven financial ecosystems.

The Consumer Rights Directive (Directive 2011/83/EU) establishes transparency obligations intended to support informed consumer decision-making.

Similarly, the Unfair Commercial Practices Directive (Directive 2005/29/EC) prohibits misleading and manipulative commercial practices capable of distorting consumer behavior (European Parliament & Council, 2011; European Parliament & Council, 2005).

These provisions acquire renewed importance in the context of AI-driven personalization and behavioral targeting. Algorithmic systems capable of exploiting cognitive vulnerabilities or asymmetries of information may generate forms of digital manipulation that challenge the practical effectiveness of consumer autonomy and informed consent.

Recent scholarship increasingly links these risks to the emergence of “dark patterns” and behavioral influence architectures in digital environments (Helberger et al., 2022).

6.3. Operational Governance Layer

The third layer focuses on operational governance mechanisms necessary to implement ethical and legal requirements in practice.

This includes algorithmic audits, compliance monitoring, internal governance procedures, model documentation, and risk assessment systems (Rizinski et al., 2022).

Operational governance mechanisms are essential because AI-related risks are dynamic, adaptive, and continuously evolving. Consequently, static compliance approaches are insufficient.

Operational governance should therefore function as a continuous supervision process rather than a one-time compliance exercise. Financial institutions deploying AI systems must establish governance structures capable of identifying emerging risks, monitoring unintended consequences, and adapting controls as algorithmic systems evolve over time.

6.4. Cybersecurity and Operational Resilience Layer

AI governance also depends on the security and resilience of the digital infrastructures supporting algorithmic systems.

This layer is primarily reinforced through DORA, and NIS2 (European Union, 2022a; European Union, 2022b). These frameworks establish obligations regarding ICT risk management, incident reporting, cyber resilience, supply chain security, and third-party oversight.

The relevance of these requirements for AI systems is particularly significant because algorithmic infrastructures may be vulnerable to adversarial attacks, data poisoning, unauthorized access, and manipulation of training datasets.

In highly automated financial environments, cybersecurity failures may generate not only operational disruptions, but also discriminatory outcomes, inaccurate risk assessments, and systemic consumer harm. Consequently, cybersecurity becomes an integral component of trustworthy and ethical AI governance.

Research on cyber risk governance increasingly highlights the need to integrate operational resilience and AI supervision within financial ecosystems (Rangu et al., 2024).

6.5. Consumer Protection and Empowerment Layer

The final layer of the framework focuses on restoring balance between institutions and consumers through mechanisms aimed at strengthening consumer agency and procedural fairness.

These mechanisms include meaningful transparency, explainability, human review rights, complaint mechanisms, and access to remedies (Regulation (EU) 2016/679; European Parliament & Council of the European Union, 2024).

This layer is particularly important because AI systems increasingly influence financial opportunities in ways that may remain invisible to consumers. Effective consumer protection therefore requires not only formal legal rights, but also practical mechanisms enabling individuals to understand, challenge, and contest algorithmic decisions affecting their economic participation.

The Digital Services Act also reinforces this direction by prohibiting certain manipulative interface designs and deceptive digital practices associated with algorithmic influence and dark patterns (European Parliament & Council, 2022).

6.6. Dynamics of the Integrated Governance Framework

The framework proposed in this study is not static. Instead, it functions as a dynamic governance ecosystem in which multiple layers interact continuously.

The relationship between layers may be summarized as follows in Tabel 3.

Tabel 3. Layers' Relationships

Layer	Regulation	Function
Ethics/AI	AI Act	Fairness, transparency, accountability
Operational	DORA	Resilience, IT process management, risk management, continuity
Cybersecurity	NIS2	Cybersecurity
Financial market	MiCa	Consumer protection, market integrity

The effectiveness of the framework depends not only on the existence of individual safeguards, but also on the degree of coordination between governance layers. Weaknesses in one dimension—such as insufficient explainability or inadequate cybersecurity—may undermine the overall trustworthiness of AI-driven financial systems.

As a key insight, consumer trust only occurs when all layer's work coherently. The framework is structured as a multi-tiered system where ethical principles, regulatory requirements, operational mechanisms, cybersecurity measures and consumer protection interact dynamically to ensure a reliable and sustainable implementation of AI in financial services.

The framework directly addresses the previously identified structural problem: algorithmic power asymmetry.

Without governance we have opaque decisions, unaccounted systems, and vulnerable consumers

With integrated governance we benefit from transparent processes, accountable institutions, and empowered consumers

Thus, we will have a transformation described in Table 4.

Table 4. Evolution of the Benefits of the New Framework

From the	To
Algorithmic asymmetry	Balanced governance
Decisions in the black box	Explainable systems
Passive consumers	Active participants

6.7. Original Contribution of the Framework

The framework proposed in this paper differs from existing approaches in several respects.

First, it conceptualizes AI-related risks as systemic consumer risks embedded within financial infrastructure rather than isolated technical failures.

Second, it explicitly integrates the ethical AI principles, financial regulation, cybersecurity governance, and consumer protection law within a unified analytical model.

Third, it positions consumer protection not as a secondary compliance objective, but as a central organizing principle of AI governance in financial services.

By connecting AI governance directly to consumer rights and European digital regulation, the framework contributes to emerging debates concerning the future of trustworthy AI, economic fairness, and democratic accountability in digital financial ecosystems.

6.8. Synthesis

The proposed framework demonstrates that trustworthy AI in financial services cannot be achieved solely through technological innovation or isolated regulatory compliance mechanisms.

Instead, sustainable governance requires integrated oversight, continuous accountability, operational resilience, consumer-centered safeguards, and the alignment with fundamental rights principles.

This paper therefore argues that the future legitimacy of AI-driven financial systems will depend not only on their technical performance, but also on their capacity to preserve fairness, transparency, consumer autonomy, and trust within increasingly automated economic environments.

Responsible artificial intelligence in FinTech is not achieved through isolated controls, but by aligning ethical, legal, operational and consumer-centric mechanisms in a unified governance architecture.

7. Discussion: Reframing AI Governance Through a Consumer-Centric Perspective

The findings of this study indicate that the governance of artificial intelligence in financial services cannot be approached solely as a technological or compliance-related issue. Instead, AI deployment in FinTech generates broader implications concerning consumer autonomy, economic fairness, institutional accountability, and democratic governance of digital infrastructures.

While current industry narratives frequently emphasize efficiency, innovation, and financial inclusion, the analysis developed throughout this paper demonstrates that these benefits coexist with significant structural risks capable of reshaping the balance of power between financial institutions and consumers.

The increasing dependence on algorithmic systems transforms financial services from environments primarily governed by contractual and informational relationships into ecosystems structured around data extraction, predictive analytics, and automated behavioral influence. In this context, consumer vulnerability becomes embedded within the architecture of digital financial systems rather than emerging solely from isolated instances of misconduct.

This paper demonstrates that AI is not a neutral tool, but a structuring force that reshapes financial interactions, redistributes decision-making authority, and redefines the boundaries of consumer protection.

7.1. From Information Asymmetry to Algorithmic Asymmetry

Traditional financial regulation has historically focused on reducing information asymmetry between financial institutions and consumers through disclosure obligations, transparency requirements, contractual fairness mechanisms.

However, the emergence of AI-driven financial systems introduces a qualitatively different form of asymmetry.

Consumers are no longer disadvantaged merely because institutions possess superior information. Instead, institutions increasingly control algorithmic infrastructures, predictive models, behavioral data, and automated decision-making mechanisms.

This creates what this paper conceptualizes as algorithmic asymmetry (Rea, 2020; Aggarwal, 2021).

Algorithmic asymmetry differs from traditional informational imbalance because it affects not only what consumers know, but also how financial opportunities are generated, filtered, and distributed through automated systems that remain largely inaccessible to public scrutiny.

This transformation is particularly significant because consumers often lack technical expertise, bargaining power, and meaningful negotiation capacity in relation to AI-driven financial processes.

7.2. AI and the Transformation of Consumer Vulnerability

The study also demonstrates that artificial intelligence fundamentally alters the nature of consumer vulnerability in financial services.

Traditional forms of vulnerability were generally associated with lack of financial literacy, contractual imbalance, and misleading information.

AI-driven systems introduce additional vulnerabilities related to opacity of algorithmic decisions, behavioral profiling, automated classification, and continuous data surveillance (Moloney et al., 2024; Ridzuan et al., 2024).

Importantly, these vulnerabilities are often systemic rather than individualized. Consumers may be exposed to algorithmic discrimination or manipulative personalization without being aware that such processes are occurring. Consequently, harm generated by AI systems may remain invisible, difficult to contest, and distributed across large populations.

This reinforces the argument advanced throughout the paper that AI-related risks should be understood as forms of systemic consumer risk embedded within digital financial infrastructures.

This has several implications, harm is often diffuse, not isolated, consumers may not be aware that they are affected, and traditional complaint-based protection mechanisms become insufficient. This finding aligns with emerging literature suggesting that digital systems require ex-ante governance, not ex-post correction.

7.3. The Limits of Existing Governance Approaches

The findings suggest that many existing governance approaches remain insufficient because they focus on isolated dimensions of AI-related risk.

For example, the ethical AI frameworks frequently lack enforceability, technical governance approaches may overlook consumer rights implications, and traditional consumer protection rules were not designed for adaptive algorithmic systems.

Similarly, purely compliance-oriented approaches risk reducing AI governance to formal procedural obligations rather than substantive consumer protection (Jackson & Langenbacher, 2025).

This limitation is particularly evident in highly automated financial environments where compliance with formal transparency obligations does not necessarily guarantee meaningful consumer understanding or effective contestability of algorithmic decisions.

As a result, the study supports growing academic arguments advocating governance models capable of integrating ethical principles, operational safeguards, legal obligations, cybersecurity resilience, and consumer empowerment mechanisms within coherent supervisory structures.

A key idea from this research is that effective governance of artificial intelligence cannot be based on a single dimension. Ethics alone is not applicable, law alone can lag technological developments, and technology alone cannot guarantee fairness or accountability.

The proposed framework addresses this issue by integrating ethical principles (normative guidance), legal frameworks (mandatory obligations), operational mechanisms (practical implementation), positioning the study in an emerging interdisciplinary field that combines financial regulation, data governance and AI ethics.

7.4. The European Union as a Global Regulatory Laboratory

The European Union currently represents one of the most advanced regulatory environments for AI governance. The interaction between the AI Act, GDPR, DORA, NIS2, MiCA, and consumer protection legislation creates a multi-dimensional governance ecosystem addressing both technological and societal dimensions of AI deployment (European Parliament & Council of the European Union, 2024; European Union, 2022a; European Union, 2022b; European Union, 2023).

A distinctive characteristic of the European approach is the integration of fundamental rights and consumer protection principles into the governance of digital technologies. Rather than treating AI solely as an innovation policy issue, the EU increasingly frames algorithmic governance as a matter of democratic accountability, economic fairness, and protection of individual autonomy in digital environments.

This rights-based approach differentiates the European model from more market-driven or innovation-centered regulatory strategies adopted in other jurisdictions.

The analysis of the EU regulatory framework reveals both strengths and limitations.

Strengths relate to comprehensive risk coverage, proactive regulatory approach (AI Act), cybersecurity and resilience integration (DORA, NIS2). Limitations relate to complexity and overlap between frameworks, risk of inconsistent application and challenges for smaller market participants.

7.4.1. Critical Understanding

The effectiveness of the EU regulatory approach does not depend on the existence of several frameworks, but on their coordination and operational integration. This highlights the need for coordination between regulations, harmonized supervisory mechanisms and practical implementation guidelines.

7.5. Tensions between Innovation and Regulation

Despite the strengths of the European regulatory framework, the study also identifies several tensions and practical challenges.

First, the coexistence of multiple regulatory instruments may generate complex compliance, overlapping obligations, fragmented supervisory practices.

Second, smaller FinTech firms may face disproportionate implementation burdens due to governance requirements, documentation obligations, and the cybersecurity standards.

Third, excessive formalism may create the risk of “checklist compliance”, symbolic transparency, procedural governance without substantive fairness.

These tensions illustrate the broader challenge of balancing innovation and consumer protection in rapidly evolving digital financial ecosystems. Overregulation may constrain technological experimentation and market entry, while insufficient governance may undermine public trust and expose consumers to systemic risks.

Consequently, effective AI governance requires adaptive regulatory approaches capable of combining flexibility with enforceable safeguards.

7.6. Consumer Protection as a Governance Principle

A central argument of this paper is that consumer protection should not be treated merely as a secondary outcome of AI governance, but as a core organizing principle of digital financial regulation.

This perspective implies that trustworthy AI systems should be evaluated not only according to technical performance, operational efficiency, and predictive accuracy, but also according to their impact on fairness, transparency, contestability, consumer autonomy, and economic participation.

Such an approach reflects an important conceptual shift from technology-centered governance toward human-centered and consumer-centered governance models. In this framework, the legitimacy of AI systems depends not solely on their functionality, but also on their compatibility with broader societal values and fundamental rights protections.

This aligns closely with the European regulatory philosophy underpinning the AI Act, GDPR, consumer protection acquis, and the Charter of Fundamental Rights of the European Union (European Union, 2012).

Traditional financial systems treat consumers as beneficiaries of services and subject to regulation. However, AI-based systems require a new perspective in which the consumer is an active interesting party. This implies meaningful access to information, the ability to challenge decisions, participation in governance processes. This change is essential for restoring balance and trust in AI-based financial ecosystems.

7.7. Theoretical and Practical Contributions

Study contributes to existing literature in several ways.

- Theoretical Contributions.

It conceptualizes algorithmic asymmetry as a structural governance issue, develops the concept of systemic consumer risk, and integrates AI governance with consumer protection theory.

- Regulatory Contributions

It connects fragmented EU legal frameworks into a unified analytical model, links AI governance directly to consumer rights protections.

- Practical Contributions

It proposes a multi-layer governance framework, identifies operational safeguards for trustworthy AI deployment, and highlights the importance of explainability, audits, and human oversight mechanisms.

By combining ethical, legal, operational, and consumer-centered dimensions, the paper contributes to the emerging interdisciplinary field focused on the governance of AI-driven economic systems and digital financial infrastructures.

7.8. Limitations and Future Research

Despite its contributions, the study has several limitations. First, the research is primarily conceptual and regulatory in nature. Second, empirical testing of the proposed governance framework remains necessary. Third, the analysis focuses predominantly on the European regulatory context.

Future research could therefore explore empirical assessments of algorithmic discrimination in financial services, comparative studies between EU and non-EU governance models, sector-specific AI applications in banking, insurance, and digital assets, and consumer perceptions of AI-driven financial decision-making.

Further research may also examine how emerging generative AI systems and autonomous financial agents could intensify existing governance challenges related to transparency, accountability, and consumer autonomy.

7.9. Synthesis

The discussion developed throughout this section reinforces the central conclusion of the paper: artificial intelligence in financial services should not be governed solely as a technological innovation, but as a broader socio-economic and regulatory phenomenon capable of reshaping consumer rights, institutional accountability, and economic participation.

The long-term legitimacy of AI-driven financial ecosystems will therefore depend not only on innovation capacity, but also on the ability to maintain fairness, transparency, procedural justice, and trust within increasingly automated and data-intensive economic environments.

The challenge is not to regulate AI as a technology, but to govern its impact on human and economic relations.

8. Conclusions

The accelerated integration of artificial intelligence into financial services represents one of the most significant transformations affecting contemporary financial ecosystems. AI technologies are increasingly embedded within processes such as credit assessment, fraud detection, insurance underwriting, personalized financial services, and digital asset management.

This transformation offers important opportunities for innovation, efficiency, and financial inclusion. However, as demonstrated throughout this study, the deployment of AI in FinTech also generates profound ethical, legal, operational, and societal challenges that directly affect consumer rights and economic participation.

The analysis developed in this paper shows that AI-related risks extend beyond traditional concerns regarding operational efficiency or cybersecurity. Artificial intelligence fundamentally reshapes the relationship between financial institutions and consumers by introducing opaque algorithmic decision-

making, large-scale behavioral profiling, predictive consumer analytics, automated classification systems, and intensified asymmetries of power and information (Rea, 2020; Moloney et al., 2024).

These developments indicate that consumer vulnerability in digital financial environments can no longer be understood solely through traditional concepts such as informational imbalance or contractual inequality. Instead, AI systems generate structural forms of vulnerability embedded within the architecture of data-driven financial ecosystems themselves.

A central contribution of this study is the conceptualization of these dynamics as forms of systemic consumer risk. Unlike isolated instances of misconduct or individual transactional disputes, AI-related risks are scalable, adaptive, embedded within algorithmic infrastructures, and difficult for consumers to identify or challenge.

This perspective highlights the limitations of conventional consumer protection approaches based primarily on disclosure obligations and ex-post remedies.

The study further demonstrates that algorithmic systems increasingly influence access to financial opportunities, pricing conditions, and economic participation in ways that may remain insufficiently transparent and only partially contestable for consumers. Consequently, trustworthy AI governance requires not only technological reliability, but also meaningful safeguards capable of preserving procedural fairness, consumer autonomy, and democratic accountability within digital financial markets.

The paper also examined the evolving European regulatory framework governing AI-driven financial systems. The interaction of regulations illustrates the emergence of a complex and multi-layer governance ecosystem designed to address algorithmic risks, cybersecurity threats, operational resilience challenges, consumer protection concerns (European Parliament & Council of the European Union, 2024; European Union, 2022a; European Union, 2022b; European Union, 2023).

Importantly, the European approach reflects a distinctive regulatory philosophy grounded in fundamental rights protection, consumer-centric governance, and accountability of digital systems (European Union, 2012).

By integrating ethical principles, data governance, cybersecurity obligations, and consumer protection mechanisms, the European regulatory model increasingly positions trustworthy AI as a prerequisite for sustainable digital finance rather than merely a condition of technological compliance.

Building on these findings, the paper proposed an integrated governance framework structured around five interconnected layers: ethical and fundamental rights principles, legal and regulatory obligations, operational governance mechanisms, cybersecurity and resilience safeguards, and consumer empowerment and procedural fairness mechanisms.

The proposed framework contributes to existing literature by linking AI governance directly to consumer rights, integrating fragmented European regulatory instruments into a coherent analytical perspective, conceptualizing algorithmic asymmetry and systemic consumer risk as central governance challenges in FinTech.

Unlike approaches focused primarily on technological performance or regulatory compliance, this framework emphasizes that the legitimacy of AI-driven financial systems ultimately depends on their capacity to maintain fairness, transparency, explainability, accountability, and trust in increasingly automated economic environments.

The study also highlights several broader implications.

For regulators, the findings suggest the importance of coordinated supervisory approaches, integrated governance mechanisms, adaptive regulatory frameworks capable of addressing rapidly evolving AI technologies.

For financial institutions, the research demonstrates that trustworthy AI governance requires continuous oversight, explainability mechanisms, robust cybersecurity safeguards, and ethical governance structures embedded within organizational processes.

For consumers, the analysis reinforces the importance of meaningful transparency, access to remedies human oversight mechanisms, stronger protections against algorithmic manipulation and discriminatory outcomes.

More broadly, the findings suggest that the future sustainability of digital finance will depend not only on innovation capacity, but also on the ability of institutions and regulators to preserve public trust and ensure that technological transformation remains aligned with societal values and consumer interests.

Despite its contributions, the study has limitations. The analysis is primarily conceptual and focused on the European regulatory context. Further empirical research is necessary to evaluate the practical effectiveness of AI governance mechanisms, the real-world impact of algorithmic decision-making on consumers, comparative regulatory approaches across jurisdictions.

Future research may also explore the implications of generative AI systems, autonomous financial agents, AI-driven behavioral finance models, and emerging forms of digital financial manipulation.

As AI technologies continue to evolve, the challenge for policymakers, financial institutions, and society will not be merely to regulate increasingly sophisticated algorithms, but to ensure that the digital transformation of finance remains compatible with human dignity, consumer autonomy, economic fairness, and democratic accountability.

9. Final Reflection

Ultimately, the long-term legitimacy and sustainability of AI-driven financial ecosystems will depend not only on technological innovation, but on the capacity to ensure that artificial intelligence operates within a framework of transparency, accountability, resilience, and genuine protection of consumer rights.

References

- Aggarwal, N. (2021). The norms of algorithmic credit scoring. *The Cambridge Law Journal*, 80(1), 42–73. <https://doi.org/10.1017/S0008197320000584>
- Agu, E. E., Abhulimen, A. O., & Obiki-Osafiele, A. N. (2024). Ethical considerations and solutions for ensuring fairness in AI-driven financial services. *Journal of Financial Regulation and Compliance*.
- Aldboush, H. H. H., & Ferdous, M. (2023). Building trust in fintech: An analysis of ethical and privacy considerations. *International Journal of Financial Studies*, 11(3), 90. <https://doi.org/10.3390/ijfs11030090>
- Badea, L., Rangu, C. M., & Scheau, M. C. (2021). Considerations regarding the digital financial ecosystem. *Proceedings of the 23rd RSEP International Conference*. <https://doi.org/10.13140/RG.2.2.25828.50565>
- Badea, L., Rangu, C. M., & Scheau, M. C. (2021). FinTech – Financial innovation enablers. *Acta Universitatis Danubius (Economica)*, 17(3), 301–316.

- Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), 671–732. <https://doi.org/10.15779/Z38BG31>
- Bauer, K., Gill, A., Langenbucher, K., & Franke, L. (2025). Institutionalizing explainability: On credit scoring, AI, and consumer agency. *SAFE Working Paper Series*. <https://www.econstor.eu/handle/10419/334497>
- Calo, R. (2014). Digital market manipulation. *George Washington Law Review*, 82(4), 995–1051.
- Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, 89(1), 1–33.
- Doshi-Velez, F., & Kim, B. (2017). *Towards a rigorous science of interpretable machine learning*. arXiv preprint arXiv:1702.08608.
- European Parliament & Council of the European Union. (2022a). *Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA)*.
- European Parliament & Council of the European Union. (2022b). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*.
- European Parliament & Council of the European Union. (2023). *Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA)*.
- European Parliament & Council of the European Union. (2024). *Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*.
- European Parliament & Council. (2005). *Directive 2005/29/EC concerning unfair business-to-consumer commercial practices*.
- European Parliament & Council. (2011). *Directive 2011/83/EU on consumer rights*.
- European Parliament & Council. (2022). *Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act)*.
- European Union. (2012). Charter of Fundamental Rights of the European Union. *Official Journal of the European Union*, C 326, 391–407.
- Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., & Srikumar, M. (2020). *Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI*. Berkman Klein Center for Internet & Society.
- Floridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Gonçalves, M. J. (2024). Regulating artificial intelligence in the European Union: A risk-based approach. *European Review of Commercial Law*.
- Helberger, N., Hosanagar, K., van der Nagel, E., & Poell, T. (2022). The political economy of AI and dark patterns. *Internet Policy Review*, 11(3). <https://doi.org/10.14763/2022.3.1681>
- Jackson, J., & Langenbucher, K. (2025). Regulating artificial intelligence in finance: Challenges and opportunities. *Journal of Financial Regulation*.
- Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1(11), 501–507. <https://doi.org/10.1038/s42256-019-0114-4>
- Moloney, N., Coita, I., & Paschalidou, E. G. (2024). Ethical AI, fintech and data protection in Europe. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4885037>
- Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2020). From what to how: An overview of AI ethics tools, methods and research to translate principles into practices. *Science and Engineering Ethics*, 26(4), 2141–2168. <https://doi.org/10.1007/s11948-019-00165-5>
- O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing Group.
- Rangu, C. M., Badea, L., Scheau, M. C., Găbudeanu, L., Panait, I., & Radu, V. (2024). Cyber insurance risk analysis framework considerations. *The Journal of Risk Finance*. <https://doi.org/10.1108/JRF-10-2023-0245>

- Rangu, C. M., Pană, N., & Scheau, M. C. (2023). Cyber risk insurance framework considerations. In M. V. Achim (Ed.), *Economic and Financial Crime, Sustainability and Good Governance*, 383–401. Springer. https://doi.org/10.1007/978-3-031-34082-6_15
- Rea, S. C. (2020). *A survey of fair and responsible machine learning and artificial intelligence: Implications for consumer financial services*. Berkeley Center for Law and Technology.
- Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016, April 27). *On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. *Official Journal of the European Union*, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Ridzuan, N. N., Masri, M., Anshari, M., & Fitriyani, N. L. (2024). AI in the financial sector: The line between innovation, regulation and ethical accountability. *Information*, 15(8), 432. <https://doi.org/10.3390/info15080432>
- Rizinski, M., Peshov, H., Mishev, K., & Chitkushev, L. T. (2022). Ethically responsible machine learning in fintech. *IEEE Access*, 10, 89721–89734. <https://doi.org/10.1109/ACCESS.2022.3198765>
- Sargeant, H. (2023). Algorithmic decision-making in financial services: Economic and normative outcomes in consumer credit. *AI and Ethics*, 3, 1041–1055. <https://doi.org/10.1007/s43681-022-00236-7>
- Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 59–68. <https://doi.org/10.1145/3287560.3287598>
- Yang, Q., & Lee, Y. C. (2024). Ethical AI in financial inclusion: The role of algorithmic fairness. *Big Data and Cognitive Computing*, 8(9), 105. <https://doi.org/10.3390/bdcc8090105>
- Zarsky, T. Z. (2016). The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making. *Science, Technology, & Human Values*, 41(1), 118–132. <https://doi.org/10.1177/0162243915605575>