Volume 3, Issue 12, December - 2025 **ISSN (E):** 2938-3811

AI AND FINTECH'S EFFECT ON THE DEVELOPMENT OF MODERN LAW

Amrulloev Miraziz Nurmatovich
LLM Graduate of Penn State Dickinson Law, Pennsylvania State University
Email: nurmatovich0505@gmail.com
Orcid: https://orcid.org/0009-0003-5371-1244

Abstract
This article examines how artificial intelligence and financial technology are reshaping modern law across public regulation, private law, and procedural justice. The core claim is that AI and FinTech do not merely introduce new products and services. They alter institutional roles, redefine legal categories, and compress the time between innovation and harm, forcing legal systems to move from episodic rulemaking toward continuous governance. The article develops a conceptual framework that links technological capabilities to legal functions, then maps concrete pathways of legal change in financial regulation, consumer protection, competition law, data governance, cybersecurity, anti money laundering, and dispute resolution. Comparative attention is given to the European Union's risk based approach to AI and its operational resilience regime for finance, the evolving international standards on virtual assets, and the emerging policy architecture in developing jurisdictions. The article argues that the most durable legal responses combine three elements: ex ante obligations for high impact uses, measurable accountability tools such as auditability and incident reporting, and procedural safeguards that protect due process when automated systems affect rights and access to essential services. The conclusion proposes a set of legally implementable design principles for regulators, courts, and market actors, emphasizing proportionality, transparency, contestability, and resilience as the shared grammar of future legal development.

Keywords: Artificial intelligence, FinTech, financial regulation, algorithmic accountability, consumer protection, operational resilience, virtual assets, data governance, due process, legal innovation.

Introduction

Artificial intelligence and financial technology have become central drivers of institutional change in contemporary legal systems. FinTech began as a market phenomenon characterized by new payment rails, digital lending, and platform based financial services. AI then intensified this shift by enabling prediction, personalization, and automated decision making at scale. Together, they change not only what financial markets do but also how legal institutions allocate risk, assign responsibility, and protect rights.

Web of Scientists and Scholars: Journal of Multidisciplinary Research

Three research questions guide this article. First, what is distinctive about the combined impact of AI and FinTech on modern law, compared with earlier waves of digitization. Second, which legal domains experience the most structural pressure, and through which mechanisms. Third, what regulatory and doctrinal strategies are most likely to produce stable, legitimate, and innovation compatible outcomes.

A key premise is that legal development is not simply a reaction to technology. Law is also a design environment that shapes incentives, constraints, and trust. When AI systems influence credit eligibility, insurance pricing, fraud detection, or market surveillance, they become part of the infrastructure of opportunity. That makes legal governance inseparable from questions of fairness, transparency, and resilience. At the same time, financial innovation moves quickly, and cross border scaling is easier than in most regulated sectors. This combination produces an increasingly common pattern: legal systems must regulate processes rather than single products, and must manage systemic risk created by interconnected platforms, cloud dependencies, and concentrated technology providers. Modern law has long responded to technological change. Yet AI and FinTech exert a distinct kind of pressure because they transform decision processes rather than merely replacing analog tools with digital ones. Two conceptual features are central.

First, AI systems reorganize epistemic authority. In classical legal reasoning, responsibility often rests on a chain of human judgments: a bank officer evaluates risk, a regulator inspects compliance, and a court reviews decisions after the fact. AI inserts statistical inference into these steps. The output may be accurate on average, yet hard to explain in individual cases. This creates a new governance question: how should law treat decisions that are rational in aggregate but potentially arbitrary in a single human life. This question is amplified when decisions affect access to essential services such as payments, credit, or insurance.

Second, FinTech changes market structure and regulatory boundaries. Many FinTech models rely on platforms that intermediate between consumers, merchants, banks, and non bank service providers. This blurs the perimeter that historically separated banking from commerce and technology. It also creates hybrid entities that are neither purely financial institutions nor purely technology firms. As a result, legal categories based on institutional form become less predictive of risk. Regulation must often become activity based rather than entity based.

These features push law toward continuous oversight. Traditional compliance models rely on periodic reporting and ex post enforcement. But AI models can drift, data can shift, and automated systems can scale harm quickly. Legal systems therefore increasingly require operational accountability, monitoring, and incident reporting to detect problems early. This shift is visible in the European Union's emphasis on operational resilience in finance, with legal duties for digital resilience across financial entities and critical ICT service providers. The Digital Operational Resilience Act entered into application in January 2025 and formalizes governance duties for ICT risk management, incident reporting, testing, and third party risk oversight.[1]

[1] European Insurance and Occupational Pensions Authority. (n.d.). Digital Operational Resilience Act,

The regulatory object problem: defining AI systems, digital finance, and responsibility chains. Legal governance begins with definition. Yet definitions become contested when technology evolves. A persistent challenge is what can be called the regulatory object problem: regulators must define what is being regulated in a way that is durable, enforceable, and aligned with risk. In AI governance, a major policy choice is whether to regulate by technology type, by function, or by risk. The European Union's Artificial Intelligence Act embodies a risk based architecture that classifies certain AI uses as prohibited, high risk, or subject to transparency duties. The Act entered into force in August 2024, signaling a move toward harmonized rules for AI across a major market.[2] The regulatory logic is not that all AI is dangerous, but that some uses are structurally capable of producing severe harm, especially when deployed in contexts that affect rights or access to essential services.

In FinTech regulation, definitions face a similar challenge. A digital lender may look like a technology firm, yet it performs credit intermediation. A crypto asset service provider may not be a bank, yet it provides custody and transfer functions. Stablecoins can resemble payments instruments, and their legal classification affects whether they are treated as e money, securities, commodities, or something else.

Responsibility chains are the second part of the object problem. AI systems are produced and maintained across multiple actors: data providers, model developers, deployers, cloud vendors, and business units that operationalize outputs. In finance, outsourcing and cloud adoption create complex webs of dependency. When harm occurs, traditional negligence or breach of duty analysis may struggle to locate the accountable party. This has accelerated the emergence of governance obligations that focus on lifecycle management, auditability, and third party risk controls.

The result is that modern legal development increasingly treats AI and FinTech as socio technical systems. Liability and compliance attach not only to discrete events but also to ongoing governance choices: training data quality, model monitoring, bias testing, incident response, and human oversight.

Financial regulation historically rests on three pillars: prudential oversight to maintain stability, conduct rules to protect consumers and integrity, and market structure regulation to prevent monopolization and abuse. AI and FinTech pressure each pillar.

Yet it also introduces new systemic risk channels. Model monoculture is one risk: if many institutions rely on similar models, they may respond to market signals in correlated ways, amplifying volatility. Another risk is third party concentration: many firms rely on a small number of cloud providers or AI toolchains. This creates common points of failure.

Central bank and supervisory discussions increasingly treat AI as relevant to financial stability. The Bank for International Settlements has highlighted that AI can affect core financial system dynamics and price adjustment behavior.[3] These concerns align with the broader move toward

[2] European Commission. (2024, August 1). AI Act enters into force.

[3] Bank for International Settlements. (2024). Annual report 2023 2024: Artificial intelligence and the economy.

operational resilience duties in finance, where regulators emphasize the ability to withstand ICT disruption and cyber incidents.[4]

A legal implication is that prudential supervision must evolve from institution level solvency metrics toward system level technology dependencies. This includes legal standards for model risk management, validation, and governance. It also includes expectations for scenario testing and stress testing that incorporate ICT and AI related failures.

Conduct regulation, consumer protection, and fairness Consumer protection faces a dual challenge: product complexity and automated personalization. FinTech interfaces can be highly persuasive, and AI can tailor offers, pricing, and nudges in ways that exploit behavioral biases. When consumers receive individualized pricing or credit terms, the fairness of those terms becomes harder to assess. The traditional disclosure model, which assumes rational consumers reading standardized terms, becomes less effective.

Law therefore shifts toward duties of suitability, explainability, and restrictions on manipulative design. In practice, this includes requirements for transparency when interacting with automated systems, and mechanisms for contesting decisions. While the details vary by jurisdiction, a broad legal trend is that the right to meaningful explanation is becoming intertwined with due process and non discrimination values, especially when automated decisions can exclude individuals from financial participation.

Market integrity, surveillance, and high frequency dynamics AI also changes market integrity. Algorithmic trading, automated market making, and surveillance systems can detect manipulation faster than humans. But they can also create new manipulation strategies. As markets become more automated, the line between legitimate high speed activity and abusive conduct becomes harder to draw.

Regulators increasingly deploy supervisory technology to process large datasets and detect anomalies. This changes administrative law in subtle ways: enforcement decisions may rely on probabilistic detection tools, raising questions about evidentiary standards and the transparency of investigative methods.

Data is the currency of AI enabled finance. Open banking, digital identity, and platform models depend on data portability and sharing. Yet the legal model of privacy based primarily on individual consent is strained under the weight of complex data ecosystems.

First, consent is often not meaningful in practice. Users face long terms and conditions, repeated prompts, and opaque downstream uses. Second, AI systems infer new information from existing data. Even if a consumer does not disclose a sensitive attribute, models can infer it from behavioral patterns.

Law thus moves toward governance frameworks that emphasize accountability, purpose limitation, data minimization, security, and risk assessment. In the European Union, the broader digital regulatory ecosystem includes rules on fair access to and use of data, reinforcing the idea that data governance is structural rather than purely individual.[5]

[4] European Insurance and Occupational Pensions Authority. (n.d.). Digital Operational Resilience Act.

[5] EUR Lex. (2024). Regulation (EU) 2024 1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

Web of Scientists and Scholars: Journal of Multidisciplinary Research

In financial services, data governance also intersects with anti discrimination law. If models infer proxies for protected characteristics, disparate impact can occur even without explicit intent. This pressures legal systems to clarify what constitutes discrimination in algorithmic contexts and what level of explainability is needed to prove or rebut claims.

A practical legal implication is that firms must document data lineage, model features, and decision logic. Regulators and courts increasingly expect demonstrable controls rather than generic compliance statements. This aligns with widely used AI governance frameworks, such as the NIST Artificial Intelligence Risk Management Framework, which emphasizes mapping, measuring, and managing AI risks across the lifecycle of AI systems.[6] It also resonates with international soft law principles such as the OECD Recommendation on Artificial Intelligence, which promotes trustworthy AI, accountability, and respect for human rights and democratic values.[7]

Operational resilience and cybersecurity: legal duties for continuity, incident reporting, and third party risk. Operational resilience has become a central legal theme because the financial sector is now inseparable from digital infrastructure. Cloud outages, ransomware attacks, data exfiltration, and software supply chain compromises can disrupt critical services.

The European Union's Digital Operational Resilience Act represents a prominent legal response by creating uniform requirements for ICT risk management, incident reporting, resilience testing, and oversight of critical ICT third party providers. The regime entered into application in January 2025.[8] The broader legal significance is that operational resilience becomes a regulatory objective comparable to solvency and consumer protection.

This approach also shifts contract law in practice. Outsourcing contracts are no longer private allocations of risk alone. They become part of compliance architecture. Firms must ensure contractual rights to audit, access, and incident notification. Third party concentration risk becomes a supervisory concern, and the legal relationship between regulated entities and technology vendors becomes a lever for systemic stability.

For developing jurisdictions, operational resilience requirements provide a structured template. Yet transplanting them requires local calibration: firms may have different levels of technological maturity, and regulators may have limited supervisory technology capacity. The legal design challenge is to adopt core principles, such as incident reporting and minimum controls, while avoiding excessive complexity that creates paper compliance without real resilience.

FinTech expands access and efficiency, but it also creates channels for financial crime. Instant payments, peer to peer transfers, and virtual asset ecosystems can move value quickly across borders. AI is used to detect suspicious patterns, but criminals also use automation to evade detection.

[6] National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework 1.0.

[7] OECD. (2019). Recommendation of the Council on Artificial Intelligence.

[8] European Insurance and Occupational Pensions Authority. (n.d.). Digital Operational Resilience Act.

International standards play a central role here. The Financial Action Task Force has repeatedly updated its standards and guidance on virtual assets and virtual asset service providers, emphasizing that AML and CFT obligations should apply to the sector and that jurisdictions should implement a risk based approach. These standards influence national legislation, licensing frameworks, and supervisory expectations.

A legal implication is that compliance becomes more analytics driven. Institutions deploy transaction monitoring systems, sanctions screening, and customer due diligence tools that rely on machine learning. This raises legal questions about false positives, de risking, and access to financial services. If automated monitoring leads to widespread account closures without meaningful explanation, due process and consumer protection concerns emerge. In some contexts, these practices can disproportionately affect vulnerable groups, triggering equality and discrimination considerations.

There is also a governance paradox. More automation can reduce costs and detect novel patterns, yet it may also reduce interpretability. Regulators must decide how to evaluate the adequacy of automated AML controls. The legal trend is toward documented model governance, validation, and audit trails, coupled with regulatory expectations for human oversight and the ability to explain key decisions to supervisors.

Private law transformation: contracts, tort, fiduciary duties, and platform governance. Digital finance often uses click based contracting and embedded finance, where financial services are integrated into non financial platforms. This changes the consumer's perception of who the counterparty is. It also increases the importance of information duties and clear allocation of responsibility among platform operators, banks, and service providers.

AI adds a second layer. Many firms use automated underwriting and dynamic pricing. In contract terms, the question is whether the consumer can understand the basis of key contractual terms, such as interest rates or insurance premiums. If the basis is an opaque model, the adequacy of disclosure becomes contested. Tort liability and standards of care for AI driven decisions

When AI assisted decisions cause harm, tort law must decide what constitutes reasonable care. Traditional negligence analysis uses a standard of the reasonable person or reasonable professional. In an AI context, the standard may become the reasonable organization that deploys AI. This may include duties to test for bias, ensure data quality, monitor drift, and provide human review for high impact decisions.

A key issue is foreseeability. AI systems may behave unpredictably under distribution shift or adversarial manipulation. Legal systems may need to treat certain risks as foreseeable once a technology is known to exhibit them. This is where governance frameworks become legally relevant: if a widely recognized framework such as the NIST AI RMF recommends specific risk management steps, failure to implement comparable steps may influence judgments about reasonableness.[9]

[9] National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework 1.0.

Fiduciary like duties and platform power. Some FinTech actors occupy positions of informational and behavioral influence. They mediate access to financial products and may steer consumers via recommendations. This can resemble fiduciary influence even if no formal fiduciary relationship exists. Law may respond by imposing duties of loyalty, avoidance of conflicts, or at least enhanced transparency around incentives and recommendation logic.

Competition law also becomes relevant. Data network effects and platform lock in can create durable market power. Legal systems may need to ensure interoperability, prevent abusive tying, and monitor self preferencing by dominant intermediaries. Modern law is not only about market rules. It is also about legitimacy and rights. AI and FinTech become constitutional problems when they affect access to essential services, public benefits, or legally protected interests.

Due process and contestability. When decisions are automated, the right to be heard and the right to reasons become harder to operationalize. Contestability requires more than a complaint channel. It requires that decisions can be meaningfully reviewed, that evidence can be examined, and that errors can be corrected within reasonable time. This affects both private and public settings. A bank's account closure can have consequences similar to administrative sanctions if it effectively excludes a person from economic participation.

The legal response often involves procedural safeguards: notice, explanation, opportunity to contest, and human review for high impact decisions. These safeguards can be implemented through regulation, consumer protection statutes, and contractual obligations enforced by courts.

Non discrimination and algorithmic bias. Discrimination law faces methodological challenges in AI contexts. Bias may arise from historical data, feature proxies, or structural inequalities reflected in data. Legal proof may require access to model documentation and aggregate outcomes, which can conflict with trade secrecy claims.

A credible legal approach must balance transparency with legitimate confidentiality. One solution is the use of regulated audits and confidential supervisory access. Another is the development of standardized impact assessments for high risk uses. The European Union's AI governance model reflects an emphasis on risk classification and obligations that scale with impact.[10]

The legitimacy of automated public functions. FinTech increasingly intersects with public functions such as digital identity, welfare payment distribution, and tax administration. AI can support fraud detection and allocation efficiency, yet it risks errors that affect rights. Administrative law may need to clarify when automated tools are permissible and what safeguards are mandatory. This includes transparency about the use of automated tools, record keeping, and judicial review standards.

Evidence and expert testimony. As AI becomes part of financial decision making, disputes increasingly require technical evidence: model governance documentation, feature importance analyses, validation reports, and incident logs. Courts may need to adapt evidentiary doctrines

[10] EUR Lex. (2024). Regulation (EU) 2024 1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

to handle complex system evidence. This may increase reliance on court appointed experts, specialized chambers, or technical standards as reference points.

Arbitration and cross border enforcement. FinTech disputes are often cross border, involving payment service providers, platforms, and investors. Arbitration remains attractive due to neutrality and enforceability. Yet AI raises new issues: document production from machine learning systems, explainability demands, and the handling of proprietary models in confidential proceedings.

A broader procedural challenge is speed. Digital harms can escalate quickly, and interim relief becomes crucial. Legal systems may need to streamline injunction procedures, ensure rapid access to payment data under lawful conditions, and enable targeted freezes to prevent dissipation of digital assets.

AI in justice systems. Some jurisdictions explore AI tools to increase access to justice, including assistance in drafting, triage, and case management. Uzbekistan, for example, has adopted policy measures to expand the use of AI in justice related contexts, including access to justice initiatives.[11] These developments raise governance questions: procurement standards, accountability for errors, and protection of confidential data. Even when AI is used only as decision support, it can shape outcomes by influencing what judges or officials see first.

Comparative and institutional models: European Union, international standards, and emerging economies with a focus on Uzbekistan's policy trajectory. Comparative analysis matters because AI and FinTech are inherently cross border. Regulatory divergence can create compliance fragmentation, arbitrage opportunities, and conflicts of laws.

European Union: risk based AI governance and operational resilience. The European Union has pursued a comprehensive governance approach that combines AI specific regulation with finance specific resilience rules. The Artificial Intelligence Act entered into force in August 2024 and sets harmonized obligations aligned to risk categories.[12] In parallel, the Digital Operational Resilience Act entered into application in January 2025 and sets detailed requirements for ICT risk management and incident reporting across financial entities.[13]

For crypto assets, the EU has implemented a dedicated legal framework. MiCA became applicable in phases, with stablecoin related provisions applying earlier and broader service provider rules applying later. National and EU level sources indicate key application dates in 2024, while additional technical requirements such as white paper formatting standards have had later operational start points.[14] The legal significance is that crypto regulation is moving from fragmented national rules toward a more uniform market regime, with disclosure, authorization, and supervision requirements.

These regimes embody a general pattern: legal systems are increasingly comfortable regulating processes and governance systems, not only products. They rely on documentation, audits,

[11] Lex.uz. (2024, October 14). Resolution RP 358: On the approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030.
[12] European Commission. (2024, August 1). AI Act enters into force.
[13] European Insurance and Occupational Pensions Authority. (n.d.). Digital Operational Resilience Act.
[14] Central Bank of Ireland. (n.d.). Markets in Crypto Assets Regulation.

incident reporting, and supervisory access, aiming to convert technological uncertainty into manageable legal duties.

International standards: AML, risk management frameworks, and soft law. In global finance, international standards often drive convergence. FATF standards and guidance influence licensing and compliance for virtual asset service providers.[15] Soft law frameworks, such as the OECD AI principles and the NIST AI RMF, influence what counts as responsible practice and therefore affect regulatory expectations and negligence standards over time.

The Financial Stability Board and other bodies have also monitored AI adoption and its implications for financial stability and regulation, signaling that GenAI and automation are viewed as cross sector risk factors.

Emerging economies and Uzbekistan: policy momentum and legal design choices. Emerging economies face a dual imperative. They seek innovation and investment, but they must also protect consumers and manage stability risks. Legal systems in these contexts can benefit from adopting clear licensing and governance frameworks that are proportionate and enforceable.

Uzbekistan has adopted a Strategy for the Development of Artificial Intelligence Technologies until 2030, which provides a state level roadmap for AI development. Additional policy measures have been adopted to further develop AI, reflecting active governmental engagement with the AI sector. International reporting also indicates that Uzbekistan has pursued investment oriented incentives for AI and data infrastructure, including tax related incentives in designated zones, which illustrates an economic development dimension of AI policy.[16]

For legal development, the main question is how to align innovation policy with enforceable safeguards. The most important design choices include: First, whether to regulate AI in finance through general AI governance duties, finance specific rules, or both. Second, how to structure accountability when financial services are delivered through platforms and third party technology vendors. Third, what dispute resolution and supervisory tools are needed so that rights remain protected when decisions are automated.

A pragmatic pathway is to combine a baseline of operational resilience and cybersecurity duties for all regulated financial entities, targeted rules for high impact automated decision making such as credit and insurance underwriting, and AML oriented supervision adapted to digital payments and virtual assets.

Policy recommendations: a coherent toolbox for lawful innovation. A coherent legal response requires a toolbox rather than a single statute. The toolbox should be unified by clear principles. Legal duties should scale with impact, exposure, and reversibility. High impact uses that determine eligibility for credit, insurance, or access to payment rails should face stronger obligations for documentation, fairness testing, human review, and contestability. This aligns with the risk based logic visible in the EU approach to AI governance. Accountability through measurable governance. Accountability should not be limited to abstract ethics language. It should be measurable. Three governance instruments are particularly effective: documentation, auditability, and incident reporting. Documentation should include data lineage, model

[15] Financial Action Task Force. (2023). Virtual assets: Targeted update on implementation of the FATF standards.
[16] Reuters. (2025, November 7). Uzbekistan sets up tax free zone for AI to attract foreign investors.

purpose, validation results, and monitoring plans. Auditability requires the ability to test the system and evaluate outcomes. Incident reporting creates incentives to detect and remediate failures early, and it supports systemic learning, a logic reflected in operational resilience regimes such as DORA.[17]

Contestability and procedural safeguards. Contestability should be designed as a legal right and as an operational process. A consumer should be able to challenge an adverse automated decision and receive a reasoned explanation that is understandable and actionable. For high impact cases, human review should be meaningful rather than symbolic. These safeguards protect legitimacy and reduce the risk that automated systems quietly erode equality and due process. Financial entities increasingly depend on technology providers. Law should require robust third party risk management, including contractual rights to audit, clear incident notification duties, and exit strategies that prevent lock in. Concentration risk should be monitored at the system level, since too many institutions may depend on the same vendors. AML obligations should be risk based and should avoid unnecessary exclusion. Automated monitoring must be calibrated to minimize false positives that cause unjustified account closures. Supervisors should require validation and governance of transaction monitoring models, consistent with international expectations for virtual asset risks. Regulators need capacity. This includes skilled staff, supervisory technology tools, and data access frameworks. Sandboxes can help, but they must not become exemption zones. A well designed sandbox should be paired with clear consumer safeguards, reporting, and learning objectives.

Conclusion

AI and FinTech accelerate the development of modern law by transforming the object, tempo, and institutional context of regulation. They change decision making, not only delivery channels. That shift forces legal systems to build governance around processes: model lifecycle controls, data governance, operational resilience, and contestability.

The emerging legal architecture suggests a future where trust is operationalized through measurable duties. Risk based classification, incident reporting, auditability, and third party governance become the backbone of legitimate innovation. At the same time, constitutional values remain central. When automated systems shape access to essential financial services, due process, transparency, and equality are not optional. They are the conditions for sustainable modernization.

In comparative perspective, the most effective legal responses combine general AI governance with sector specific resilience and integrity rules, and they draw on international standards for financial crime and risk management. For jurisdictions pursuing rapid digitalization, including Uzbekistan, the policy opportunity is to align investment and innovation strategies with clear safeguards that protect consumers, strengthen stability, and build institutional trust.[18]

[17] European Insurance and Occupational Pensions Authority. (n.d.). Digital Operational Resilience Act.

[18] Lex.uz. (2024, October 14). Resolution RP 358: On the approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030.

REFERENCES:

1. European Commission. (2024, August 1). AI Act enters into force. European Commission
2. European Insurance and Occupational Pensions Authority. (n.d.). Digital Operational Resilience Act. EIOPA
3. Commission de Surveillance du Secteur Financier. (2025, January 17). Entry into application of DORA regulation on 17 January 2025. CSSF
4. EUR Lex. (2024). Regulation (EU) 2024 1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. EUR-Lex
5. Central Bank of Ireland. (n.d.). Markets in Crypto Assets Regulation. Central Bank of Ireland - English
6. European Securities and Markets Authority. (2025). Markets in Crypto Assets Regulation: Interim register and implementation materials. ESMA
7. Financial Action Task Force. (2023). Virtual assets: Targeted update on implementation of the FATF standards. FATF
8. Financial Action Task Force. (2025). Targeted update on implementation of the FATF standards for virtual assets and virtual asset service providers. FATF
9. National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework 1.0. NIST Publications+1
10. OECD. (2019). Recommendation of the Council on Artificial Intelligence. legalinstruments.oecd.org+1
11. Bank for International Settlements. (2024). Annual report 2023 2024: Artificial intelligence and the economy. Bank for International Settlements+1
12. Financial Stability Board. (2025). Monitoring adoption of artificial intelligence and related technologies in financial services. Financial Stability Board
13. Lex.uz. (2024, October 14). Resolution RP 358: On the approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030. Lex.uz
14. Lex.uz. (2025, October 22). Decree DP 189: On additional measures for the further development of artificial intelligence. Lex.uz
15. Reuters. (2025, November 7). Uzbekistan sets up tax free zone for AI to attract foreign investors. Reuters.

Web of Scientists and Scholars: Journal of Multidisciplinary Research