EISSN: 2623-274X|PISSN: 2623-1603
Volume 8 Nomor 2 Agustus 2025: 207-219
DOI: 10.30996/jhmo.v8i2.13102

Jurnal Hukum Magnum Opus

Post-Quantum Cryptography and Legal Frameworks: Strengthening Uzbekistan's Cybersecurity and Intellectual Property Protection

Islombek Abdikhakimov[1*]
[1]Tashkent State University of Law, Uzbekistan
*Corresponding Author: islombekabduhakimov@gmail.com

Article History:
Submitted:
22-03-2025
Received:
08-04-2025
Accepted:
29-04-2025

Keywords:
quantum technology; cybersecurity; post-quantum cryptography

Abstract

The rapid development of quantum technology has significant implications for legal systems, particularly in the areas of cybersecurity, intellectual property, and digital sovereignty. The computational power of quantum computing to decrypt conventional encryption systems poses serious challenges to national information security. Developed countries have adopted post-quantum cryptographic policies to protect their data, while Uzbekistan still faces regulatory gaps in transitioning to more secure encryption systems. Furthermore, the increasing number of patents in quantum technology may create innovation barriers due to the phenomenon of patent thickets, which limit access to strategic technologies. The lack of regulatory clarity regarding legal liability for quantum-based artificial intelligence also creates uncertainty within Uzbekistan's legal system, particularly in terms of transparency and accountability. Without adaptive regulations, Uzbekistan risks strategic data leaks and dependence on foreign actors in quantum technology development. Therefore, policy reforms are necessary, including post-quantum cryptography-based cybersecurity regulations, harmonization of intellectual property laws with international standards, and the implementation of regulatory sandboxes to test policies before widespread adoption. This study emphasizes that without concrete steps in quantum technology regulation, Uzbekistan risks falling behind in the global competition. A more flexible and progressive legal approach is required to ensure digital sovereignty, data security, and protection of domestic innovation. With the right policies, Uzbekistan can leverage quantum technology to drive its digital economy without compromising its strategic national interests.

1. Introduction

The development of quantum technology has introduced a new paradigm across various sectors, ranging from secure communication and cryptography to pharmaceutical design and AI-driven legal analysis.[1] These innovations challenge existing legal frameworks, most of which are still rooted in the classical or early digital era.[2] The phenomenon of "quantum advantage," where quantum computers surpass classical machines in solving complex tasks, has prompted policymakers, academics, and industry leaders to urgently develop a regulatory framework specifically for quantum technology.[3]

---

[1] Dandison Ukpabi et al., "Framework for Understanding Quantum Computing Use Cases from a Multidisciplinary Perspective and Future Research Directions," *Futures* 154 (December 2023): 103277, https://doi.org/10.1016/j.futures.2023.103277.

[2] Geoff Gordon, "Digital Sovereignty, Digital Infrastructures, and Quantum Horizons," *AI & SOCIETY* 39, no. 1 (February 13, 2024): 125–37, https://doi.org/10.1007/s00146-023-01729-7.

[3] Anushka Mittal, "Probing the Production of Quantum Technologies to Imagine Its Legal Framework," *Research Directions: Quantum Technologies* 3 (January 8, 2025): 1, https://doi.org/10.1017/qut.2024.6; Virginia D'Auria and Marina Teller, "What Are the Priorities and the Points to Be Addressed by a Legal

The concept of "quantum law," which was once speculative, has now evolved into an academic field that identifies various legal gaps in intellectual property[4], national security[5], data protection[6], and artificial intelligence regulation[7]. Moreover, the cross-border nature of quantum research presents new challenges in global governance, as no single country can fully control this inherently international technology[8].

Compared to previous technological revolutions, such as the internet or artificial intelligence, quantum computing operates based on the principles of superposition and entanglement[9], challenging the fundamental assumptions of determinism and linear causality in legal systems[10]. Consequently, scholars have proposed a more integrative legal framework that considers the "quantum" dimensions of uncertainty, entanglement, and non-locality.[11] This issue is particularly urgent for developing countries like Uzbekistan, which aims to

---

Framework for Quantum Technologies?," *Research Directions: Quantum Technologies* 1 (June 6, 2023): e9, https://doi.org/10.1017/qut.2023.3.

[4] R. Grant Hammond, "Quantum Physics, Econometric Models and Property Rights to Information," *McGill Law Journal* 27, no. 1 (September 1981): 47–72, https://lawjournal.mcgill.ca/article/quantum-physics-econometric-models-and-property-rights-to-information/; Mauritz Kop, "Establishing a Legal-Ethical Framework for Quantum Technology," *Yale Journal of Law & Technology*, March 2021, 1–16, https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology; Mateo Aboy, Timo Minssen, and Mauritz Kop, "Mapping the Patent Landscape of Quantum Technologies: Patenting Trends, Innovation and Policy Implications," *IIC - International Review of Intellectual Property and Competition Law* 53, no. 6 (July 6, 2022): 853–82, https://doi.org/10.1007/s40319-022-01209-3.

[5] Miriam Wimmer and Thiago Guimarães Moraes, "Quantum Computing, Digital Constitutionalism, and the Right to Encryption: Perspectives from Brazil," *Digital Society* 1, no. 2 (September 12, 2022): 12, https://doi.org/10.1007/s44206-022-00012-4; A. Minbaleev, S. Zenin, and K. Evsikov, "Prospects for Legal Regulation of Quantum Communication," *BRICS Law Journal* 11, no. 2 (July 29, 2024): 11–54, https://doi.org/10.21684/2412-2343-2024-11-2-11-54.

[6] Elija Perrier, "The Quantum Governance Stack: Models of Governance for Quantum Information Technologies," *Digital Society* 1, no. 3 (December 12, 2022): 22, https://doi.org/10.1007/s44206-022-00019-x; Said Gulyamov, "Quantum Law: Navigating the Legal Challenges and Opportunities in the Age of Quantum Technologies," *Uzbek Journal of Law and Digital Policy* 1, no. 1 (February 28, 2023): 1–11, https://doi.org/10.59022/ujldp.54.

[7] Jeffery Atik and Valentin Jeutner, "Quantum Computing and Computational Law," *Law, Innovation and Technology* 13, no. 2 (July 3, 2021): 302–24, https://doi.org/10.1080/17579961.2021.1977216; Mauritz Kop, "Quantum-ELSPI: A Novel Field of Research," *Digital Society* 2, no. 2 (August 26, 2023): 20, https://doi.org/10.1007/s44206-023-00050-6.

[8] Kaya DeRose, "Establishing the Legal Framework to Regulate Quantum Computing Technology," *Catholic University Journal of Law and Technology* 31, no. 2 (2023): 145–72, https://scholarship.law.edu/cgi/viewcontent.cgi?article=1143&context=jlt; Elif Kiesow Cortez, Jane R. Yakowitz Bambauer, and Saikat Guha, "A Quantum Policy and Ethics Roadmap," *SSRN Electronic Journal*, 2023, https://doi.org/10.2139/ssrn.4507090.

[9] R. George Wright, "Should the Law Reflect the World?: Lessons for Legal Theory from Quantum Mechanics," *Florida State University Law Review* 18, no. 3 (1991): 877–905, https://ir.law.fsu.edu/lr/vol18/iss3/7/; David Orrell, "The Value of Value: A Quantum Approach to Economics, Security and International Relations," *Security Dialogue* 51, no. 5 (October 27, 2020): 482–98, https://doi.org/10.1177/0967010620901910.

[10] Wright, "Should the Law Reflect the World?: Lessons for Legal Theory from Quantum Mechanics."

[11] James Der Derian and Alexander Wendt, "'Quantizing International Relations': The Case for Quantum Approaches to International Theory and Security Practice," *Security Dialogue* 51, no. 5 (October 5, 2020): 399–413, https://doi.org/10.1177/0967010620901905; Valentin Jeutner, "Addressing the Legal Dimensionof Quantum Computers," *Morals & Machines* 1, no. 1 (2021): 52–59, https://doi.org/10.5771/2747-5174-2021-1-52.

leverage quantum technology for economic growth but still lacks a robust policy infrastructure to manage its associated risks.[12]

The legal challenges in the implementation of quantum technology stem from the absence of a comprehensive theoretical and regulatory framework to encompass quantum computing, quantum cryptography, and quantum-based artificial intelligence. Existing legal instruments, such as intellectual property regulations, data protection laws under frameworks like the European Union's GDPR, or national cybersecurity laws, are inadequate to anticipate the speed, complexity, and global nature of quantum technological disruption.[13] Furthermore, legal preparedness varies significantly across jurisdictions, creating a new form of digital divide known as the "quantum gap," where developed nations and large corporations can monopolize quantum resources and expertise.[14]

The operational demands of quantum technology, particularly in secure communication (quantum key distribution/QKD), cryptographic analysis (breaking classical encryption), and AI-driven analytics (quantum machine learning), pose existential vulnerabilities if not promptly addressed through legal and policy regulations.[15] Countries that fail to update their cryptographic standards with post-quantum methods risk large-scale data breaches, digital signature forgery, and potential infiltration of critical infrastructure. Moreover, the interaction between quantum technology and artificial intelligence, known as "Quantum AI," raises concerns regarding accountability, bias, and fairness in automated decision-making.[16]

This study seeks to address the urgent question of how to construct a comprehensive legal framework for quantum technology, balancing the acceleration of innovation with the protection of social values such as privacy, equality, and security.[17] By drawing on various legal sources, technical analyses, and comparative perspectives[18], this article contributes to the emerging discipline of "quantum law." In the context of Uzbekistan, the urgency of quantum technology regulation is increasing in line with the country's ambitions to develop a digital economy. While Uzbekistan has adopted various digital transformation policies, it still faces

---

[12] Gulyamov, "Quantum Law: Navigating the Legal Challenges and Opportunities in the Age of Quantum Technologies."

[13] Minbaleev, Zenin, and Evsikov, "Prospects for Legal Regulation of Quantum Communication"; E. V. Kholodnaya, "Quantum Technology as an Object of Law," *Courier of Kutafin Moscow State Law University (MSAL))*, no. 4 (July 10, 2022): 38–45, https://doi.org/10.17803/2311-5998.2022.92.4.038-045.

[14] Wimmer and Moraes, "Quantum Computing, Digital Constitutionalism, and the Right to Encryption: Perspectives from Brazil"; D'Auria and Teller, "What Are the Priorities and the Points to Be Addressed by a Legal Framework for Quantum Technologies?"

[15] Cortez, Bambauer, and Guha, "A Quantum Policy and Ethics Roadmap"; E. A. Gromova and S. A. Petrenko, "Quantum Law: The Beginning," *Journal of Digital Technologies and Law* 1, no. 1 (March 14, 2023): 62–88, https://doi.org/10.21202/jdtl.2023.3.

[16] Atik and Jeutner, "Quantum Computing and Computational Law"; Mauritz Kop, "Quantum-ELSPI: A Novel Field of Research," *Digital Society* 2, no. 2 (August 26, 2023): 20, https://doi.org/10.1007/s44206-023-00050-6.

[17] Orrell, "The Value of Value: A Quantum Approach to Economics, Security and International Relations"; Hammond, "Quantum Physics, Econometric Models and Property Rights to Information."

[18] M. B. Dobrobaba, S. E. Channov, and A. V. Minbaleev, "Quantum Communications: Prospects for Legal Regulation," *Courier of Kutafin Moscow State Law University (MSAL))*, no. 4 (July 10, 2022): 25–37, https://doi.org/10.17803/2311-5998.2022.92.4.025-037; Gromova and Petrenko, "Quantum Law: The Beginning"; Kop, "Quantum-ELSPI: A Novel Field of Research," August 26, 2023.

significant challenges in establishing specialized regulations that can accommodate quantum-based technologies. Therefore, this article not only aims to enrich the global legal discourse on quantum regulation but also provides concrete recommendations for policymakers in Uzbekistan to develop a futuristic and adaptive legal framework.

2. Methods

This research utilized a multi-stage qualitative methodology, anchored in doctrinal, comparative, and interdisciplinary legal analysis.[19] The methodological framework draws inspiration from prior attempts to examine emerging technologies through both doctrinal legal study and socio-legal inquiry.[20]

3. Results and Discussion

3.1. The Urgency of Post-Quantum Cryptography Regulation: Challenges and Cybersecurity Strategies in the Republic of Uzbekistan

The rapid development of quantum computing technology has significant implications for national security systems, particularly in the fields of cryptography and the protection of strategic data.[21] The ability of quantum computing to break conventional cryptographic algorithms, including RSA and Elliptic Curve Cryptography (ECC), has created an urgent need for nations to design encryption systems that are resistant to quantum attacks. Countries with well-established legal infrastructures, such as the United States through the National Quantum Initiative Act, the European Union with the Quantum Technologies Flagship, and China, which has developed a communication network based on Quantum Key Distribution (QKD), have adopted progressive measures to ensure their data security in the face of threats posed by advancements in quantum technology.

Conversely, countries that lack a comprehensive regulatory framework for managing cryptography, including the Republic of Uzbekistan, face serious threats to the integrity, confidentiality, and sovereignty of national data. Although Uzbekistan has enacted the Law on Information Security and the Regulation on Encryption and Information Protection, which provide a legal basis for cybersecurity management, regulations specifically governing the transition to post-quantum cryptography have yet to be adopted into national legislation. First, the Law of the Republic of Uzbekistan on Informatization establishes a framework for the development and use of information technology, including aspects of information security. Second, the Law on Principles and Guarantees of Freedom of Information regulates rights and obligations related to information access and distribution while setting standards for information protection. Third, the Law on Information Protection in Information Systems specifically governs measures for safeguarding information within information systems,

---

[19] Wright, "Should the Law Reflect the World?: Lessons for Legal Theory from Quantum Mechanics"; Sieg Eiselen, "Proving the Quantum of Damages," *Journal of Law and Commerce* 25, no. 1 (2005): 375–84, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/eiselen.pdf.

[20] Andrea K. Bjorklund, "Causation, Morality, and Quantum," *Suffolk Transnational Law Review* 32, no. 2 (2009): 435–50, https://law-journals-books.vlex.com/vid/causation-morality-and-quantum-191967911; Hammond, "Quantum Physics, Econometric Models and Property Rights to Information."

[21] Rafiul Azim Jowarder and Sawgat Jahan, "Quantum Computing in Cyber Security: Emerging Threats, Mitigation Strategies, and Future Implications for Data Protection," *World Journal of Advanced Engineering Technology and Sciences* 13, no. 1 (September 30, 2024): 330–39, https://doi.org/10.30574/wjaets.2024.13.1.0421.

including the use of cryptographic technology to ensure data confidentiality and integrity. Additionally, the Government Regulation on Cryptographic Tool Certification outlines the procedures for certifying and utilizing cryptographic tools in Uzbekistan. Together, these regulations form the legal framework for information security and cryptographic applications in Uzbekistan. However, the absence of regulations addressing post-quantum cryptography creates a legal gap that could be exploited by malicious actors, both domestically and internationally, to exploit vulnerabilities in Uzbekistan's digital security infrastructure. Concrete steps must be taken to update cybersecurity regulations to accommodate post-quantum cryptographic standards in alignment with international legal developments. The harmonization of national laws with cryptographic standards established by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) is a fundamental step in ensuring that Uzbekistan's data protection systems remain resilient against threats posed by quantum computing.

In the Republic of Uzbekistan, regulations on information security and cryptography are still in the development stage, although several legal instruments have established fundamental aspects of data protection and digital communication. The Law of the Republic of Uzbekistan on Informatization sets out the basic principles for managing information systems, including technical and legal requirements to ensure data integrity and confidentiality. Additionally, the Law on Information Protection in Information Systems regulates data protection mechanisms, including security requirements for entities processing strategic information related to national interests. The importance of cryptographic regulations in addressing quantum computing threats has become increasingly relevant as Uzbekistan adopts digital transformation across various public and private sectors. The Government Regulation on Cryptographic Tool Certification establishes technical standards for the development, certification, and implementation of cryptographic devices to ensure data protection against advanced technological threats. However, existing regulations have yet to explicitly accommodate the concept of post-quantum cryptography, which has become a central concern in global cybersecurity frameworks. Compared to the United States' approach through the National Quantum Initiative Act or the post-quantum cryptographic standardization policies of the National Institute of Standards and Technology (NIST), Uzbekistan must adopt similar policies to safeguard national data security. Likewise, the harmonization of cryptographic standards, as pursued by the European Union, and the development of quantum key distribution (QKD)-based communication networks, as implemented in China, can serve as references for drafting national regulations. Regulatory revisions that are more adaptive to quantum technological threats are necessary to ensure digital sovereignty and the protection of Uzbekistan's strategic interests.

The implementation of post-quantum cryptography in the Republic of Uzbekistan faces several complex legal and technical challenges. One of the primary obstacles is the limited technological infrastructure, which hinders the modernization of encryption systems that currently rely on classical algorithms such as RSA and Elliptic Curve Cryptography (ECC). From a legal perspective, the Law of the Republic of Uzbekistan on Information Security does not explicitly regulate the transition from conventional encryption systems to post-quantum cryptography, creating a regulatory gap that could jeopardize national cybersecurity integrity.

Additionally, the Regulation on Encryption and Information Protection only governs the use of encryption algorithms certified by national authorities, without accounting for the possibility that these algorithms may become obsolete due to advancements in quantum computing. The absence of specific regulations governing the migration to post-quantum cryptographic systems creates legal uncertainty, which could be exploited by malicious actors to take advantage of vulnerabilities within Uzbekistan's national data security framework.

Furthermore, the Uzbekistan Digital Strategy 2030, despite setting policy directions for strengthening digital infrastructure, has not specifically addressed the threats posed by quantum computing or the need for investment in research and the development of new cryptographic standards[22]. The limited availability of human resources with expertise in quantum technology and cybersecurity also presents a significant challenge to the implementation of these policies.[23] In the long term, the establishment of more comprehensive regulations is necessary to enhance national capacity in addressing quantum-based cyber risks. This includes the integration of post-quantum cryptographic standards into government communication systems and other strategic sectors.

The rapid advancement of quantum technology has led to an increase in the number of patent applications, which in turn has introduced legal complexities in the realm of intellectual property rights (IPR). One of the primary challenges is the phenomenon of patent thickets, where overlapping patents in a specific technological field hinder innovation and restrict access to post-quantum cryptographic technologies. Within Uzbekistan's legal framework, the protection of innovations in quantum technology, particularly in quantum cryptography, still contains regulatory gaps that could lead to legal uncertainty for researchers and industry stakeholders.[24] The Patent Law of the Republic of Uzbekistan establishes procedures for patent registration and protection but does not specifically address the unique characteristics of quantum technology patents.[25] Moreover, the Regulation on the Protection of Intellectual Property Rights in the Field of Information and Communication Technology only covers general aspects of software ownership and licensing without considering the competitive dynamics of the high-tech quantum-based industry. This regulatory vacuum may create legal barriers in the development and implementation of post-quantum cryptographic technology in Uzbekistan, particularly regarding the certainty of patent ownership and utilization by both the public and private sectors.[26] To mitigate the negative effects of patent thickets and

---

[22] Chithralekha Balamurugan et al., "Post-Quantum and Code-Based Cryptography—Some Prospective Research Directions," *Cryptography* 5, no. 4 (December 20, 2021): 38, https://doi.org/10.3390/cryptography5040038.

[23] Said Gulyamov and Islombek Abdikhakimov, "The Quantum Threat: Examining The Impact of Quantum Computing on International Cybersecurity and the Urgent Need for New Legal Frameworks," *Jurisprudence* 4, no. 2 (April 23, 2024): 102–12, https://doi.org/10.51788/tsul.jurisprudence.4.2./XOTJ9919.

[24] Akhmedov Azizkhon, "Patent Law and Innovation Implementation: Fostering Grant Projects and Technological Advancement in Uzbekistan," *Uzbek Journal of Law and Digital Policy* 1, no. 2 (April 30, 2023), https://doi.org/10.59022/ujldp.77.

[25] Azizkhon.

[26] Madinabonu Yakubova, "The Legal Challenges of Regulating AI in Cybersecurity: A Comparative Analysis of Uzbekistan and Global Approaches," *International Journal of Law and Policy* 2, no. 7 (July 30, 2024): 7–10, https://doi.org/10.59022/ijlp.202.

technological monopolies, more progressive legal policies are needed, including the implementation of compulsory licensing mechanisms for patents deemed essential to national security. Furthermore, strengthening international cooperation in the management of quantum technology patents has become a legal imperative to ensure innovation accessibility and to prevent exclusive domination by certain entities in this industry.[27]

3.2. Legal Implications for Cybersecurity, Intellectual Property, and Digital Sovereignty

The advancement of quantum technology presents significant challenges to legal systems, particularly in the areas of intellectual property protection and cybersecurity regulation. In the context of Uzbekistan, the absence of regulations specifically anticipating the impact of quantum technology creates legal gaps that could affect both innovation protection and national information security.[28] The imbalance between the rapid progression of technology and a legal response that remains reactive highlights weaknesses in a legislative system that has yet to fully adapt to the quantum-driven digital revolution. Existing regulations, such as the Law of the Republic of Uzbekistan on Information Security and the Regulation on Encryption and Information Protection, remain limited in addressing the threats posed by quantum computing. The vulnerability to "harvest now, decrypt later" attacks—where encrypted data using classical methods can be stored and later decrypted by quantum computers—underscores the urgency of formulating post-quantum cryptographic policies. Without regulations governing the transition from conventional cryptography to post-quantum standards, Uzbekistan faces the risk of strategic data breaches that could threaten national security.[29] In terms of intellectual property rights, the increasing number of patents related to quantum technology may give rise to legal challenges, particularly in the form of patent thickets, which can hinder innovation and research collaboration. The lack of specific regulations governing the ownership, licensing, and exploitation of patents in the field of quantum technology calls for legal reforms to ensure that innovators' rights are protected without obstructing broader research advancements.[30] Therefore, aligning domestic regulations with international standards is an essential step for Uzbekistan to guarantee legal certainty in the face of the quantum technology era.

Quantum technology introduces complex legal implications for classical encryption systems, which have long served as the foundation of digital transactions and government communications. One of the primary risks emerging from this development is the harvest now, decrypt later threat, in which malicious actors collect data encrypted using conventional algorithms, intending to decrypt it in the future with quantum computing capabilities.[31] In the context of strategic information protection, the lack of legal preparedness to anticipate this

---

[27] Yakubova.
[28] Gulyamov, "Quantum Law: Navigating the Legal Challenges and Opportunities in the Age of Quantum Technologies."
[29] N. Umarova, "Information Security in the Context of Ensuring National Security of Uzbekistan," *International Relations and International Law Journal* 104, no. 4 (December 2023), https://doi.org/10.26577/IRILJ.2023.v104.i4.05.
[30] Karshieva Nilufar Tovboy Kizi, "Cybersecurity in Uzbekistan: Protecting the Digital Economy," *International Journal of Economic Integration and Regional Competitiveness* 1, no. 6 (June 17, 2024): 53–61, https://doi.org/10.61796/ijeirc.v1i6.139.
[31] Kizi.

threat poses a significant risk to national security and undermines the state's ability to safeguard data integrity and cyber sovereignty. As of now, Uzbekistan's legal framework has yet to explicitly accommodate post-quantum cryptographic (PQC) standards, despite their growing global urgency in ensuring the resilience of digital security systems against quantum-driven threats. This regulatory gap heightens the risk of sensitive data leaks across both governmental and private sectors and may create legal loopholes exploitable by actors seeking to conduct increasingly sophisticated cyberattacks. Beyond cybersecurity concerns, the absence of regulations regarding the adoption of quantum technology in Uzbekistan's legal system also creates legal uncertainty for industries such as banking and digital commerce, which rely on encryption reliability to ensure transaction validity and security.[32]

The increasing number of patents in the field of quantum technology presents complex legal implications for intellectual property protection, particularly in patent law. One of the main issues arising from this development is the phenomenon of patent thickets, a situation where overlapping patent ownership hinders innovation due to excessive fragmentation of exclusive rights. In the context of Uzbekistan's legal system, the absence of specific regulations governing patent management and licensing in quantum technology poses the risk of innovation monopolization by entities with dominant capital and technological capabilities. This situation may limit access for small and medium-sized enterprises (SMEs) and independent research institutions in developing and implementing quantum technology. The lack of legal norms regulating the boundaries and mitigation mechanisms for patent thickets could lead to innovation stagnation, as the high risk of legal disputes over alleged patent infringements discourages further technological advancement. Furthermore, without clear regulations on compulsory licensing for quantum technology, dominant patent holders may restrict the use of this technology to select entities, contradicting the principles of fair competition and the fundamental purpose of the patent system as a tool for promoting technological progress.

The evolving landscape of quantum technology within Uzbekistan's legal system brings significant juridical consequences, one of which is the creation of an access gap to this technology—commonly referred to in legal and technological discourse as the quantum divide. Globally, only nations with substantial human resources, infrastructure, and capital can independently develop and implement quantum technology. This situation has direct implications for Uzbekistan, increasing its dependence on foreign actors for technology transfer, quantum device procurement, and national data security management, all of which intersect with the country's cyber sovereignty. Reliance on foreign entities for quantum technology development presents serious legal risks, particularly concerning the protection of strategic data and control over technology used in both the public and private sectors. Without adequate regulations, access to quantum infrastructure may become contingent upon the political and economic interests of more technologically advanced nations. Moreover, in the absence of legal norms governing equitable technology transfer, Uzbekistan may find itself in a weak bargaining position when negotiating technology contracts with foreign entities,

[32] Kizi.

potentially jeopardizing the country's digital sovereignty.[33] The existing domestic regulatory framework, including laws on technology investment and cybersecurity, has yet to incorporate legal mechanisms that facilitate the strengthening of national capacity in quantum technology development.[34]

Addressing the legal complexities arising from the development of quantum technology requires a regulatory framework that is not only responsive but also adaptive and integrative. Overly rigid regulations may stifle innovation, while excessively lax regulations can create legal uncertainty, potentially allowing certain actors to exploit gaps in ways that conflict with national interests. Therefore, a flexible legal approach is essential, such as the implementation of regulatory sandboxes, which provide controlled environments for policy experimentation to assess the effectiveness of regulations before they are widely implemented. Additionally, a progressive regulatory incentive scheme is needed to foster the growth of Uzbekistan's quantum technology ecosystem. A more inclusive patent policy should be developed to prevent the monopolization of innovation by dominant entities, which could hinder the participation of local actors. Legal protections for domestic research outcomes must also be strengthened through mechanisms that ensure adequate intellectual property rights protection, both at the national and international levels. Furthermore, regulations that promote research collaboration and technology transfer should be incorporated into national policies to address domestic resource constraints in quantum technology development. Harmonizing policies between the public and private sectors, as well as fostering cooperation with academic institutions and international research centers, should be formulated within a clear legal framework. This will enable Uzbekistan to actively engage in the global quantum technology landscape while maintaining control over its strategic interests. Ultimately, the regulations established must not only focus on mitigating legal risks but also serve as strategic instruments to accelerate the sovereign and sustainable mastery of quantum technology.

Regulatory ambiguity regarding legal liability for the use of quantum-based artificial intelligence (AI) poses significant legal uncertainty within Uzbekistan's judicial system and public policy framework.[35] With computational power surpassing conventional systems, quantum AI can generate complex decisions that are not fully auditable under the current legal mechanisms.[36] The absence of legal standards governing accountability for decisions made by quantum AI presents serious challenges, particularly in sectors with broad implications for human rights and public interests. Uzbekistan's legal system has yet to establish explicit regulations defining the legal subject responsible for errors or biases in decision-making by quantum AI. This raises fundamental questions about the allocation of legal responsibility among software developers, system owners, end users, and even the AI itself. Without clear

[33] Yakubova, "The Legal Challenges of Regulating AI in Cybersecurity: A Comparative Analysis of Uzbekistan and Global Approaches."
[34] Ruziev Rustam, "Property Rights in Uzbekistan: A Comprehensive Analysis of the Legal Framework and Its Implications for the Digital Age," *Uzbek Journal of Law and Digital Policy* 1, no. 2 (April 30, 2023), https://doi.org/10.59022/ujldp.78.
[35] Saidov Maksud, "Legal Frameworks for the Implementation of AI: Safeguarding Legal Entities," *Uzbek Journal of Law and Digital Policy* 2, no. 1 (November 2, 2023), https://doi.org/10.59022/ujldp.141.
[36] Finale Doshi-Velez et al., "Accountability of AI Under the Law: The Role of Explanation," *SSRN Electronic Journal*, 2017, https://doi.org/10.2139/ssrn.3064761.

legal certainty, there is a substantial risk that certain actors could evade accountability for the adverse consequences of quantum AI decisions, including those affecting the judiciary, public policy formulation, and the management of critical national infrastructure.

The ethical and social implications of quantum technology must be a primary concern in the design of responsive and adaptive legal policies. While law is inherently normative and prescriptive, technological advancements often progress at a pace that outstrips the legal system's ability to accommodate these dynamics. This disparity can create regulatory gaps that impact justice, privacy, and social welfare. In the context of Uzbekistan, there is currently no explicit legal framework addressing the social consequences of quantum technology implementation, particularly regarding individual rights and corporate responsibilities in its utilization. A more principle-based and flexible legal approach is needed to anticipate the yet-to-be-fully-understood consequences of quantum technology.[37] One potential method is the implementation of a Quantum Technology Impact Assessment (QTIA) as an evaluative instrument to assess the social, economic, and legal effects of quantum technology adoption. QTIA could serve as a reference for formulating legal policies grounded in substantive justice, ensuring that regulations are not merely reactive but also capable of progressively and sustainably accommodating technological advancements.[38] Moreover, integrating QTIA into Uzbekistan's national regulatory framework would help ensure that every quantum technology implementation adheres to the principles of fairness, proportionality, accountability, and transparency. Consequently, evidence-based decision-making can be conducted more comprehensively, safeguarding justice, personal data protection, and social welfare in the era of quantum technology.

Considering the various legal aspects examined, Uzbekistan must develop a more comprehensive regulatory framework to address the challenges posed by the quantum technology revolution. A proactive legal approach, grounded in the precautionary principle and aligned with international standards, should be prioritized in the formulation of legal policies related to this technology. Without decisive and well-structured measures, risks related to information security, unequal access to technology, and the monopolization of innovation in intellectual property will further widen the gap between technological advancements and legal regulations in Uzbekistan.

4. Conclusions

The rapid advancement of quantum technology necessitates urgent legal regulation, particularly in the Republic of Uzbekistan. With its capability to decrypt conventional cybersecurity systems and impact various legal domains, quantum technology poses significant challenges in information security, intellectual property, and digital sovereignty. Leading nations such as the United States, the European Union, and China have already adopted post-quantum cryptography policies to safeguard their data. In contrast, Uzbekistan lags in developing regulations that specifically accommodate this technology, despite having existing laws related to information security and data protection. Uzbekistan's regulatory shortcomings in anticipating security risks from quantum computing pose a major threat,

[37] Kop, "Establishing a Legal-Ethical Framework for Quantum Technology."
[38] Azizkhon, "Patent Law and Innovation Implementation: Fostering Grant Projects and Technological Advancement in Uzbekistan."

particularly regarding potential strategic data leaks and cyberattacks. Without regulations facilitating the transition to post-quantum cryptography, Uzbekistan may become vulnerable to "harvest now, decrypt later" attacks, where encrypted classical data can be collected and later decrypted by quantum computers. In the realm of intellectual property, quantum technology also presents complex legal challenges. The growing number of quantum-related patents raises concerns about "patent thickets", an accumulation of overlapping patents that could hinder innovation and restrict access for research institutions and technology firms in Uzbekistan. The absence of clear regulations governing quantum patent management and licensing could lead to the monopolization of innovation by entities with technological and financial dominance. To prevent this, Uzbekistan must develop more inclusive legal policies, including mandatory licensing mechanisms for patents essential to national interests. Furthermore, the social and ethical implications of quantum technology must be considered in legal policymaking. The lack of regulatory clarity regarding liability for quantum-based artificial intelligence (AI) decision-making creates legal uncertainty within the judicial system and public policy framework. Without clear legal provisions governing accountability in automated AI-driven decisions, Uzbekistan faces significant risks related to transparency, fairness, and legal accountability. To address these challenges, Uzbekistan must swiftly adopt a more adaptive and integrative legal approach. Overly stringent regulations could stifle innovation, while excessively lax regulations could create legal uncertainty. Therefore, regulatory sandboxes could serve as a viable solution, allowing policies to be tested on a small scale before broader implementation. Additionally, Uzbekistan should strengthen international cooperation in quantum technology governance to avoid technological dependence on other nations that could threaten its digital sovereignty.

5. References

Aboy, Mateo, Timo Minssen, and Mauritz Kop. "Mapping the Patent Landscape of Quantum Technologies: Patenting Trends, Innovation and Policy Implications." *IIC - International Review of Intellectual Property and Competition Law* 53, no. 6 (July 6, 2022): 853–82. https://doi.org/10.1007/s40319-022-01209-3.

Atik, Jeffery, and Valentin Jeutner. "Quantum Computing and Computational Law." *Law, Innovation and Technology* 13, no. 2 (July 3, 2021): 302–24. https://doi.org/10.1080/17579961.2021.1977216.

Azizkhon, Akhmedov. "Patent Law and Innovation Implementation: Fostering Grant Projects and Technological Advancement in Uzbekistan." *Uzbek Journal of Law and Digital Policy* 1, no. 2 (April 30, 2023). https://doi.org/10.59022/ujldp.77.

Balamurugan, Chithralekha, Kalpana Singh, Ganeshvani Ganesan, and Muttukrishnan Rajarajan. "Post-Quantum and Code-Based Cryptography—Some Prospective Research Directions." *Cryptography* 5, no. 4 (December 20, 2021): 38. https://doi.org/10.3390/cryptography5040038.

Bjorklund, Andrea K. "Causation, Morality, and Quantum." *Suffolk Transnational Law Review* 32, no. 2 (2009): 435–50. https://law-journals-books.vlex.com/vid/causation-morality-and-quantum-191967911.

Cortez, Elif Kiesow, Jane R. Yakowitz Bambauer, and Saikat Guha. "A Quantum Policy and Ethics Roadmap." *SSRN Electronic Journal*, 2023. https://doi.org/10.2139/ssrn.4507090.

D'Auria, Virginia, and Marina Teller. "What Are the Priorities and the Points to Be Addressed by a Legal Framework for Quantum Technologies?" *Research Directions: Quantum Technologies* 1 (June 6, 2023): e9. https://doi.org/10.1017/qut.2023.3.

Derian, James Der, and Alexander Wendt. "'Quantizing International Relations': The Case for Quantum Approaches to International Theory and Security Practice." *Security Dialogue* 51, no. 5 (October 5, 2020): 399–413. https://doi.org/10.1177/0967010620901905.

DeRose, Kaya. "Establishing the Legal Framework to Regulate Quantum Computing Technology." *Catholic University Journal of Law and Technology* 31, no. 2 (2023): 145–72. https://scholarship.law.edu/cgi/viewcontent.cgi?article=1143&context=jlt.

Dobrobaba, M. B., S. E. Channov, and A. V. Minbaleev. "Quantum Communications: Prospects for Legal Regulation." *Courier of Kutafin Moscow State Law University (MSAL))*, no. 4 (July 10, 2022): 25–37. https://doi.org/10.17803/2311-5998.2022.92.4.025-037.

Doshi-Velez, Finale, Mason Kortz, Ryan Budish, Christopher Bavitz, Samuel J. Gershman, David O'Brien, Stuart Shieber, Jim Waldo, David Weinberger, and Alexandra Wood. "Accountability of AI Under the Law: The Role of Explanation." *SSRN Electronic Journal*, 2017. https://doi.org/10.2139/ssrn.3064761.

Eiselen, Sieg. "Proving the Quantum of Damages." *Journal of Law and Commerce* 25, no. 1 (2005): 375–84. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/eiselen.pdf.

Gordon, Geoff. "Digital Sovereignty, Digital Infrastructures, and Quantum Horizons." *AI & SOCIETY* 39, no. 1 (February 13, 2024): 125–37. https://doi.org/10.1007/s00146-023-01729-7.

Gromova, E. A., and S. A. Petrenko. "Quantum Law: The Beginning." *Journal of Digital Technologies and Law* 1, no. 1 (March 14, 2023): 62–88. https://doi.org/10.21202/jdtl.2023.3.

Gulyamov, Said. "Quantum Law: Navigating the Legal Challenges and Opportunities in the Age of Quantum Technologies." *Uzbek Journal of Law and Digital Policy* 1, no. 1 (February 28, 2023): 1–11. https://doi.org/10.59022/ujldp.54.

Gulyamov, Said, and Islombek Abdikhakimov. "The Quantum Threat: Examining The Impact of Quantum Computing on International Cybersecurity and the Urgent Need for New Legal Frameworks." *Jurisprudence* 4, no. 2 (April 23, 2024): 102–12. https://doi.org/10.51788/tsul.jurisprudence.4.2./XOTJ9919.

Hammond, R. Grant. "Quantum Physics, Econometric Models and Property Rights to Information." *McGill Law Journal* 27, no. 1 (September 1981): 47–72. https://lawjournal.mcgill.ca/article/quantum-physics-econometric-models-and-property-rights-to-information/.

Jeutner, Valentin. "Addressing the Legal Dimensionof Quantum Computers." *Morals & Machines* 1, no. 1 (2021): 52–59. https://doi.org/10.5771/2747-5174-2021-1-52.

Jowarder, Rafiul Azim, and Sawgat Jahan. "Quantum Computing in Cyber Security: Emerging Threats, Mitigation Strategies, and Future Implications for Data Protection." *World Journal of Advanced Engineering Technology and Sciences* 13, no. 1 (September 30, 2024): 330–39. https://doi.org/10.30574/wjaets.2024.13.1.0421.

Kholodnaya, E. V. "Quantum Technology as an Object of Law." *Courier of Kutafin Moscow State Law University (MSAL))*, no. 4 (July 10, 2022): 38–45. https://doi.org/10.17803/2311-5998.2022.92.4.038-045.

Kizi, Karshieva Nilufar Tovboy. "Cybersecurity in Uzbekistan: Protecting the Digital Economy." *International Journal of Economic Integration and Regional Competitiveness* 1, no. 6 (June 17, 2024): 53–61. https://doi.org/10.61796/ijeirc.v1i6.139.

Kop, Mauritz. "Establishing a Legal-Ethical Framework for Quantum Technology." *Yale Journal of Law & Technology*, March 2021, 1–16. https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology.

———. "Quantum-ELSPI: A Novel Field of Research." *Digital Society* 2, no. 2 (August 26, 2023): 20. https://doi.org/10.1007/s44206-023-00050-6.

Maksud, Saidov. "Legal Frameworks for the Implementation of AI: Safeguarding Legal Entities." *Uzbek Journal of Law and Digital Policy* 2, no. 1 (November 2, 2023). https://doi.org/10.59022/ujldp.141.

Minbaleev, A., S. Zenin, and K. Evsikov. "Prospects for Legal Regulation of Quantum Communication." *BRICS Law Journal* 11, no. 2 (July 29, 2024): 11–54. https://doi.org/10.21684/2412-2343-2024-11-2-11-54.

Mittal, Anushka. "Probing the Production of Quantum Technologies to Imagine Its Legal Framework." *Research Directions: Quantum Technologies* 3 (January 8, 2025): 1. https://doi.org/10.1017/qut.2024.6.

Orrell, David. "The Value of Value: A Quantum Approach to Economics, Security and International Relations." *Security Dialogue* 51, no. 5 (October 27, 2020): 482–98. https://doi.org/10.1177/0967010620901910.

Perrier, Elija. "The Quantum Governance Stack: Models of Governance for Quantum Information Technologies." *Digital Society* 1, no. 3 (December 12, 2022): 22. https://doi.org/10.1007/s44206-022-00019-x.

Rustam, Ruziev. "Property Rights in Uzbekistan: A Comprehensive Analysis of the Legal Framework and Its Implications for the Digital Age." *Uzbek Journal of Law and Digital Policy* 1, no. 2 (April 30, 2023). https://doi.org/10.59022/ujldp.78.

Ukpabi, Dandison, Heikki Karjaluoto, Astrid Bötticher, Anastasija Nikiforova, Dragoş Petrescu, Paulina Schindler, Visvaldis Valtenbergs, and Lennard Lehmann. "Framework for Understanding Quantum Computing Use Cases from a Multidisciplinary Perspective and Future Research Directions." *Futures* 154 (December 2023): 103277. https://doi.org/10.1016/j.futures.2023.103277.

Umarova, N. "Information Security in the Context of Ensuring National Security of Uzbekistan." *International Relations and International Law Journal* 104, no. 4 (December 2023). https://doi.org/10.26577/IRILJ.2023.v104.i4.05.

Wimmer, Miriam, and Thiago Guimarães Moraes. "Quantum Computing, Digital Constitutionalism, and the Right to Encryption: Perspectives from Brazil." *Digital Society* 1, no. 2 (September 12, 2022): 12. https://doi.org/10.1007/s44206-022-00012-4.

Wright, R. George. "Should the Law Reflect the World?: Lessons for Legal Theory from Quantum Mechanics." *Florida State University Law Review* 18, no. 3 (1991): 877–905. https://ir.law.fsu.edu/lr/vol18/iss3/7/.

Yakubova, Madinabonu. "The Legal Challenges of Regulating AI in Cybersecurity: A Comparative Analysis of Uzbekistan and Global Approaches." *International Journal of Law and Policy* 2, no. 7 (July 30, 2024): 7–10. https://doi.org/10.59022/ijlp.202.