JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(4), 4843-4850
ISSN: 2589-1316

Securing the Digital Future: A Proactive Legal Framework for Quantum Computing Challenges

Shereen Abu Ghazaleh[1], Hassan Sami Alabady[2], Inas Al-Khaldi[3*], Mohannad Azmi Masod Abu-Moghli[4]

[1]*Associate Professor of Private Law, Faculty of Law, Amman Arab University, Amman, Jordan, shereen@aau.edu.jo*
[2] *Associate Professor of Law, Faculty of Business, Amman Arab University, Amman, Jordan, h.alabady@aau.edu.jo*
[3]*Professor of Law, Faculty of Law, Amman Arab University, Amman, Jordan, i.alkhaldi@aau.edu.jo*
[4] *Professor of Law, Faculty of Law, Amman Arab University, Amman, Jordan, dr.mohannad.azmi@aau.edu.jo*

*__Corresponding Author:__ i.alkhaldi@aau.edu.jo

Citation: Ghazaleh, S. A., Alabady, H. S., Al-Khaldi, I. & Abu-Moghli, M. A. M. (2025). Securing the Digital Future: A Proactive Legal Framework for Quantum Computing Challenges, *Journal of Cultural Analysis and Social Change*, 10(4), 4843-4850. https://doi.org/10.64753/jcasc.v11i1.4044

Published: December 30, 2025

ABSTRACT

Quantum computing is transitioning rapidly from theoretical possibility to practical capability, generating unprecedented legal and regulatory challenges across intellectual property, cybersecurity, data protection, and contractual liability. Despite early governmental initiatives, including the European Union's Quantum Flagship, the U.S. National Quantum Initiative Act, and the G7's 2025 Kananaskis Common Vision, existing governance efforts remain fragmented, programmatic, and insufficiently attuned to the systemic risks posed by quantum technologies. This article employs a doctrinal, comparative, and policy-analytic methodology to evaluate the preparedness of current legal frameworks and to identify the structural gaps that emerge when quantum capabilities threaten cryptographic stability, undermine data-protection assumptions, and strain patent doctrines. The findings show that quantum risks are foreseeable, cross-domain, and capable of rendering existing compliance mechanisms ineffective. The study's novel contribution lies in synthesizing these insights into an integrated governance model that mandates quantum-resistant cryptography, modernizes intellectual property standards, recalibrates data-protection obligations, and incorporates quantum-specific contingencies into contractual risk management. The article argues that only a proactive, harmonized, and anticipatory regulatory architecture can ensure that quantum technologies develop in accordance with the rule of law, global security, and the public interest.

Keywords: Quantum Computing Law, Post-Quantum Cryptography, Technology Governance, Data Protection, Legal Risk Management

INTRODUCTION

Quantum computing is bringing into the theoretical world a new technological reality that changes the law, governance, and global security dramatically. As the U.N. declares 2025 as International Year of Quantum Science and Technology, quantum technologies are now gain prominence and will become a central part of economic systems, national security agencies and global data networks, quantum shifts. Quantum computing powers through quantum mechanical phenomena such as superposition and entanglement that allow it to process more complex tasks than conventional machines, and the new regulatory frameworks are unable to deal with issues that existing regulatory structures do not want to be faced (Wright 2024; Gent 2021).

In addition, quantum capabilities pose systemic risks to cloud-based infrastructures that continue to support government, financial and commercial digital transactions. The cloud is controlled by distributed encryption and remote key-management systems, which are especially vulnerable to quantum-enabled attacks that threaten

confidentiality and authentication at scale. The constraints on cloud computing, which remain the dominant paradigm in international data storage and processing, further raise the alarm for regulatory strategies that would require the transition to quantum-resilient cryptographic standards (Frankenfield, 2021).

While governments and institutions are responding, the regulatory landscape is fragmented. The European Union has stepped forward long-term strategic plans such as the Quantum Flagship and aims to implement a coherent European quantum policy in the next few years, but legislation is not yet clear (European Commission, 2018). In the US, quantum infrastructure and quantum-resistant cryptography are growing national investment for the United States, with NIST's National Quantum Initiative Act and the technical standardization efforts of NIST. In the world, the 2025 Kananaskis Common Vision, made the first coordinated commitment by major economies to pursuing collective control over quantum technologies, acknowledging their importance to economic resilience and national security (G7, 2025). While such developments have come, no jurisdiction has established a comprehensive regulatory regime that addresses the legal implications of quantum computing in intellectual property, cybersecurity, data protection or contractual liability. Law scholars have begun to address the destructive nature of quantum computing across several different areas. Cybersecurity researchers note that quantum machines may compromise most public key encryption systems and expose historical and future communications once sufficiently powerful quantum devices can function as "harvest now, decrypt later" (Buchholz et al., 2020). This commentary on intellectual property highlights the absence of practical patent doctrines that can be used to accommodate quantum algorithms, which can often use mathematical structures or quantum-state manipulations that challenge the normal definitions of clarity, novelty, and industrial utility (Wagner & Mazarakis, 2021; Kop, 2020; Kop, 2021). Just as structural issues regarding data protection regimes such as the EU General Data Protection Regulation, which cannot afford to maintain its encryption and accountability mechanisms, quantum mechanisms are likely to pose. These concerns show the vastly increasing divide between technological progress and legal preparedness.

From that perspective, this article follows a view of reactive governance as lack of evidence, and the quantum era calls for a proactive interdisciplinary legal strategy. The Article outlines the legal structure, approaches to governance and new research, that it has taken, to identify gaps and propose future regulatory solutions through doctrinal and policy-analytic analysis. This study addresses the following questions:

1. What core legal challenges does quantum computing pose to existing frameworks governing intellectual property, cybersecurity, data protection, and contractual risk allocation?
2. To what extent do current national and international initiatives provide a coherent foundation for quantum governance, and where do critical regulatory gaps remain?
3. What proactive regulatory strategies can be formulated to ensure that quantum technologies evolve in a manner consistent with the rule of law, global security, and the public interest?

The article addresses these questions by describing quantum technologies as demanding new and anticipatory regulatory architecture, new intellectual property doctrine, increased obligations for data-protection, and contracts with explicitly quantum risks. It thus contributes to an increasing body of scholars that see quantum computing as not only a technical innovation in the realm of science but also a mechanism that transforms legal regimes to their foundational principles.

LITERATURE REVIEW

Quantum computing has become a field that is increasingly increasingly specialized, theoretically and conceptually oriented with new controversies regarding quantum computing, as well as the implications for law, cybersecurity, intellectual property, and global governance. The primary principles of quantum theory are superposition and entanglement, which dominate quantum systems with computational advantages over classical ones in early scientific literature. Gent (2021) and Flynn (2020) also note that the development of quantum error correction, hybrid quantum–classical systems, and the rapid migration of theoretical model into practice, leads to technical and regulatory consequences. While quantum computing is integrated into digital infrastructures, much has emerged that such a proactive governance model is necessary to tackle the transformative and disruptive challenges of technology.

This is especially relevant because existing cryptographic systems cannot be used to face quantum attacks. Small numbers suggest that quantum algorithms, such as Shor's algorithm scales massive numbers of integers and compute discrete logarithms, may compromise the principles of public-key encryption that is used worldwide in secure communications, financial systems and blockchain. This is also a national security concern, Buchholz et al. (2015) stating: 'Quantum enabled attackers can attack sensitive data, steal authentication and threaten digital transactions.' These concerns are further expressed in a research paper by Long, Liu, Wang (2022) who claims that the "harvest-now, decrypt-later" strategy already being practiced by sophisticated actors is not sustainable on the

long term with long-term structural implications of data protection policies. These analyses suggest that technology is needed to improve and that legal institutions should be tailored for quantum resilient cryptography and accountability standards.

Another interesting study is the relationship between quantum computing and data protection regulations. It is expected that the existing compliance systems, but could become poor under quantum-capable threats in Fogg (2022), Langeland (2025). De Schrijver (2018) describes the complexity at stake to regulators in exploring the complexities of GDPR principles of data minimization and encryption and the fear of a quantum attack that might compromise protected systems. In addition, a chapter on cross-border data transfer has been cited, in which quantum threats complicate the understandings of fairness, risk assessment, and accountability in changing digital sovereignty policies (Cowie, 2023; Irion & De Hert, 2021).

The most complex topic discussed in quantum governance is intellectual property law. Wagner and Mazarakis (2021) conclude that patent systems are not sufficiently sophisticated to deal with quantum algorithms, as structures often overlap to what would be considered mathematical practices that are not patentable. Kop also questions existing IP doctrines that quantum inventions are not subject to standard disclosure formats because they lack standard disclosure formats, hindering examinations of novelty, inventive practice and industrial usefulness. Recent literature such as Abbott (2018) and Contreras (2023) shows conflicting lines between a willingness to cooperate with scientists and that suggest premature or too broad patents can undermine innovation.

Additionally, besides the philosophical aspects of IP, governance research increasingly is grounded in the geopolitical and strategic perspective of quantum technology regulation. While legislation is slow to develop, the Quantum Flagship is an example of regional efforts to combine quantum innovation within a strategic and ethical framework. His new book, 2025 Kananaskis Common Vision, discusses the first major international commitment to coordinated quantum governance in international governance literature. As long as these aspects are addressed, the US still stresses these aspects through the National Quantum Initiative Act and NIST's post-quantum cryptography program (NIST, n.d., 19). Van de Poel and Stilgoe argue that quantum technologies are part of a larger sociotechnical ecosystem, which requires anticipatory regulation based on risk governance theory, technological due process, and responsible innovation.

The criticism of these government initiatives, and other government programs, highlights geopolitical competition over quantum innovation. Lehot (2020) shows. and how this movement is a technology arms race fueled by states and private actors, financed through quantum research into strategic and economic prosperity. Likewise, this competitive environment will always shape legal requirements, market incentive and governance issues. In these reflections and analysis, fragmented national policies are not just a complication of regulatory confusion but they are not just a complication of judicial divergence. Nevertheless, they could also compromise collective security, particularly if states are unwilling to control worldwide connectivity and the rules themselves, to control global rules.

Law and technology claim that quantum computing will require a reconsideration of regulatory assumptions. While quantum technologies show structural deficiencies in existing cybersecurity, intellectual property, and algorithmic accountability, Levinson (2021) demonstrates what is still present in cybersecurity, intellectual property, and algorithms, whose transparent regulatory framework is open and technologically neutral. While these developments are in fact happening, the principles of digital constitutionalism and procedural fairness that are required to be integrated into quantum framework should remain embedded in both digital and procedural framework, as technology improves. The view of quantum computing as being not a new novelty but an inherent tendency among law to require laws to adopt new forms of foresight, standardization and international cooperation is consistent with this position.

But literature contains three intersecting insights. First, quantum computing will likely destroy existing technical and legal infrastructure such as encryption, data protection, and cybersecurity. For example, today intellectual property regimes lack conceptual tools to assign quantum algorithms and hardware. Third, governance efforts are fragmented at the national and international levels, and show the need to develop more balanced regulatory models to manage cross-border risk, and the safe and equitable development of quantum technologies. Among this scholarship, this theory argues that there must be a proactive legal system, as discussed later in this text.

METHODOLOGY

1. Research Design and Scholarly Orientation

This paper adopts a doctrine and policy analysis research design, accompanied by selective comparative insights and interdisciplinary engagement with science and technology studies (STS). The practice of documenting legal principles, regulatory tools and case-based reasoning allows for a systematic examination of the governance

mechanisms that structure the emerging technologies. This is a very good approach to quantum computing where legislation is still premature and the interpretation of existing norms must apply to new technologies. Political analysis complements doctrine in its examination of how regulatory reform practices, government strategies, and international governance strategies emerged from the European Union, the United States, and the G7.

2. Scope of Legal Materials and Primary Sources

A wide range of major legal papers is examined, including U.S. National Quantum Initiative Act; data-protection laws like the EU General Data Protection Regulation; and governments or intergovernmental documents, such as the G7's 2025 Kananaskis Common Vision for the Future of Quantum Technologies and the European Commission's quantum governance communications. They provide the basis for reviewing the legal situation in the present to address future challenges to quantum technology, including cryptographic disruption, data security threats, intellectual-property uncertainty, and contractual liability.

3. Use of Secondary Literature and Scholarly Interpretation

This article incorporated the broad array of secondary publications, including peer-reviewed legal work, technology policy, and interdisciplinary studies related to quantum science to regulatory theory. The study of cybersecurity and governance problems will include Kop, Wagner and Mazarakis, Abbott (2018), Contreras (2023), Levinson (2021) and Buchholz et al. (2014). Long et al. (2022), Long et al. (2022). Stilgoe (2023). The research also includes scientific and technical studies, such as the initial description of quantum mechanics and quantum computing architecture (Gent, 2021; Wright, 2024) that ensures that legal assessment is accurate for the underlying technologies.

4. Comparative and Cross-Jurisdictional Assessment

As quantum computing is global, it employs comparative legal analysis to examine regulatory developments in key jurisdictions. NIST evaluates U.S.-wide measures of standardization and quantum resistance cryptography, looking at European Union policy. This has been examined in the context of international coordination, especially in the G7, examining evolving norms and governance approaches. This contrast illustrates the fragmentation of contemporary regulatory responses as well as the potential for common global standards to be unified.

5. Analytical Framework and Evaluation Criteria

This analysis develops an anticipatory governance framework based on STS literature and current risk-governance models. This means that innovative technologies like quantum computing require regulatory protocols that reflect scientific uncertainty, nonlinear development, and systemic vulnerability. Therefore, it focuses on legal and policy considerations regarding coherence, adaptability, enforceability, international compatibility, and compliance with basic rights in consistency and flexibility, as well as compliance with fundamental rights in conformity and flexibility. This model is based on what is needed for proactive recommendations beyond incremental or reactive regulatory changes in this context.

6. Limitations of the Study

Given the lack of quantum-specific legislation and decisions, quantum law studies present here are narrowly limited in scope. The article thus uses similar practices in cybersecurity, encryption, intellectual property law and, to an extent, to acknowledge the future legal practices will refine or rework them. The evidence provided in this study is empirical data for technological readiness or economic impact; it does contain normative and doctrinal skepticism for prediction of legal problems and regulatory responses.

RESULTS

1. Fragmentation and Immaturity of the Current Quantum Regulatory Landscape

The doctrine and comparisons support the notion that quantum governance is in an early stage but is fragmented rather than coherent. But, the European Union, as well as its best-seller Quantum Flagship project and new quantum policies and instruments, has not yet issued binding legislation regarding quantum technologies. This is more strategic than regulatory because it calls for research coordination and standardization but not political governance. The U.S. has had coherent quantum legislation and does not have any coherent quantum legislation other than the National Quantum Initiative Act, which was a research investment and coordination bill that is about research and coordination rather than legal obligations or compliance. So, the G7's 2025 Kananaskis Common Vision is not a normative is not a normative moment, and does not have standards or enforcement

mechanisms that are agreed upon. Each of these results suggests that existing programs are lacking the legal complexity needed to overcome quantum risks.

2. Rising Urgency in Addressing Cryptographic Vulnerability and Data-Security Risks

The analysis suggests that legal security is mostly a common phenomenon in cryptographic infrastructure destabilization. Quantum computers have always been the source for espionage of the digital world, an issue that exists in industry, state, and people, including privacy protection. What is already legislation, such as GDPR that identifies the security of data and confidentiality, depends on encryption systems likely to fail. While NIST is developing post-quantum cryptographic standards, no jurisdiction has locked them in, or defined liability standards for non-changing agents. This is apparent, given that countries that have established quantum threats that do recognize quantum threats have no mandate or responsibility to secure systems to counter quantum enabled attacks.

3. Intellectual Property Regimes Are Not Adequately Equipped for Quantum Innovation

The results also show that it is conceptually and practically difficult to control quantum algorithms, devices and processes. In patent doctrines calling for novelty, inventive step, and industrial application, quantum-state manipulation is not often encoded in standardized representations and may look like abstract mathematical processes that have been laced together into a loop. But, in some cases patent examiners are unable to determine inventiveness without knowledge of quantum mechanics; the disclosure requirements would not be consistent with limited memory of quantum processes or with the definition of entangled states of deterministic properties. This may also mean inconsistent patent results or patents excessively broad that essentially inhibit downstream innovation as research has demonstrated. The analysis suggests that the size of this structure must be tight to allow it to move forward rather than hinder its own development of quantum technologies.

4. Data Protection, Privacy, and Digital Rights Are at Risk of Doctrinal Obsolescence

Today's data protection systems are protected by many security concepts such as encryption, pseudonymization, and securing key management. This illustrates how quantum computing has a complex relation to the assumptions of these mechanisms. If encryption can be breached by a third party, this principle of "continuing confidentiality" is no longer valid and an existing data subject may be in danger of security breaches that can only be detected if quantum encryption is applied. This retroactive vulnerability further limits accountability, risk assessment, and data protection law. It also demonstrates the basic concerns of digital rights that can never be fully understood by anyone on the asphyxiable scale. These results suggest quantum-resilient security standards must align with data-protection obligations and liability in post-quantum computing scenarios.

5. Contractual Risk Management Remains Underdeveloped Despite Foreseeable Threats

This research highlights quantum risks are not easily added into contracts. Most commercial agreements and service level contracts also use standard force majeure clauses and liability in the absence of quantum-enabled disruptions. Perhaps quantum threats will not be predicted, and may also affect encryption-tied systems, but a lack of knowledge of quantum threats may prevent liability or breach-of-contract claims against liability or breach-of-contract claims. Yet few industries have started to adopt contractual risk allocation frameworks, as scholars and government guidelines have warned. This shows a constant decrease in technological risk awareness and contractual risk preparedness - therefore, contract doctrines must change, and quantum contingencies must be added to contracts.

6. Emerging International Governance Efforts Lack Enforcement and Harmonization

While the G7, EU and U.S. efforts are becoming increasingly aware of the geopolitical potential of quantum technologies, the study suggests they are not aligned with or focused on their own ambitions. There is no global institution that regulates quantum technologies now. Unlikely, if standards regulatory analogues could be created and the imbalances are created, then states can manipulate jurisdictions to undermine interoperability and undermine global digital economy. This also requires supranational governance, or superpowers to coordinate standards, monitor compliance and react to cross-border quantum risk.

DISCUSSION

With quantum power in abundance, the legal apparatus is at increased risk of being subjected to the inevitable threat that existing regulatory systems no longer serve to keep digital infrastructures secure, to protect rights, or to sustain innovation. It was based on assumptions of computational limits and cryptographic stability, which quantum machines sought to counter. This thesis is a contribution to the emerging field of quantum law by

articulating a single legal concept that considers quantum computing not as a unique technological challenge, but as the structural transformation of the digital order. By combining the information on intellectual property, cybersecurity, data protection and contractual liability, the article provides a holistic view of quantum governance as a multidimensional problem that demands interdisciplinary solutions and global regulatory coordination. Thus, it is current scholarship that fragmented, sector-specific reforms cannot safeguard legal certainty in the quantum era, and that only anticipatory, cross-domain governance can guide the technology to safe, ethical and socially supported deployment.

1. Legal Implications Across Intellectual Property, Cybersecurity, Data Protection, and Contractual Liability

This analysis presents an empirical and comparative analysis of quantum computing, which challenges existing intellectual property, cybersecurity, data protection and contractual liability as its primary research question. This thesis holds in common with earlier works (Buchholz et al., 2020; Long et al., 2022) that quantum computing creates new security vulnerabilities in cryptographic systems, currently the central unit of modern digital security. While previous research focused on the technical impact of quantum decryption, the results represent legal uncertainty as the "appropriate security measure" will no longer be guaranteed as "appropriate security measure" under regulatory standards such as the GDPR. This directly affects the requirements of confidentiality, data integrity as well as accountability and shows how quantum technology intrudes on normative assumptions embedded in the existing law on data protection.

Their conclusions, in relation to intellectual property, complement Kop (2020; 2021) and Abbott (2022) whose concerns related to quantum algorithms cross the boundaries between patentable inventions and unpatentable mathematical practices. This report further underscores RQ1, as it shows that patent examiners may not have the expertise necessary to inspect quantum-state manipulations, which produces uncertainty and doctrine incompatible. As noted above, this work emphasizes the global implications of such uncertainty: differing national approaches could fragment early-stage quantum innovation ecosystems.

The findings also show that contractual doctrines must change to overcome foreseeable quantum threats, the aspect that had only been briefly discussed in prior research. Addressing RQ1, the study shows that as quantum-enabled breaches are now likely to occur rather than speculatively, existing contractual clauses in force, such as force majeure, liability, and security obligations, may also permit parties to owe damages or breach-of-warranty lawsuits. This provides a new extension to recent research by situating quantum threats within private-law analysis, and by demonstrating how commercial relationships must respond to technological risk.

2. Strengths and Limitations of Emerging Governance Efforts

The second question on RQ2 is whether national and international efforts contribute to an overall sense of quantum governance. However, such research as De Schrijver and Contreras 2023, has pointed out that existing initiatives tend to favor strategic ambitions rather than legal obligations. This view is supported by the present results in that while the EU Quantum Flagship, the U.S. National Quantum Initiative Act and the G7's 2025 Kananaskis Common Vision are all indicating increasingly political and scientific engagement, they are mostly programmatic. They do not regulate binding regulations, make quantum resilient security practices mandatory, or have monitoring mechanisms.

The study expands the institutional constraint of these actions by focusing more fully on RQ2. They are significant milestones in the international recognition of quantum technology but do not meet the criteria for anticipatory governance, which requires combined foresight, standardization, enforcement capacity and continuous monitoring (Stilgoe 2023; Van de Poel 2021). Thus, it extends other studies that show that regulatory interoperability is a huge challenge. As Cowie writes in Data sovereignty, fragmented practices undermine security and serve jurisdiction shopping. This conclusion further complements our findings showing that incompatible quantum standards could undermine global cybersecurity and intellectual property policies worldwide.

3. Proactive and Future-Oriented Regulatory Strategies

The third research question is to develop regulatory practices for quantum technology that can be used to maintain public interest, security and basic rights. It is primarily unique about this research because it does not touch the aspect of anticipatory regulation of new technologies: quantum computing that might potentially modify regulatory infrastructures in particular is. If the findings were explicitly addressed, RQ3 should be controlled instead of fixed. This research is done in several areas of cryptography, IP law, data protection law, contract law in which quantum legal requirements exist. Quantum resistance cryptography is not a technical recommendation for technical matters but, rather, legal guidelines for confidentiality and compliance. Results also serve to extend and improve patent doctrines by adding quantum-specific disclosure and evaluation requirements to enable innovation to emerge while not overheating the substance. This is what studies have done but quantum governance is not part

of the equation. While the previous works have dealt with a few IP problems, data protection and cybersecurity, this paper traces them into a common legal framework. This suggests that both sectors can use the opportunity to create integrated regulatory systems before quantum capabilities are fully viable.

4. Integrating Findings with Broader Governance Theory

The results place quantum computing in the context of technology governance, including anticipatory regulation and responsible innovation. Along with these results, such as RQ1, RQ2, and RQ3, quantum computing is simply the type of dynamics, uncertainty, systemic risk, and transformational potential that is necessary anticipatory governance. As evidence, they also show that the future should be practiced more broadly, including doctrinal interpretation, contracting, and cross-border standardization, with the help of evidence. Previous research on new technologies such as AI, biotechnology or platform governance has already focused on these technologies. This research is an improvement in the field in that quantum computing brings a more complex legal procedures that disrupts the mechanical assumptions of cybersecurity law, data protection systems, and digital trust. Their results also bolster the literature by making quantum governance legalized by demanding both conceptual and institutional change.

CONCLUSION

This study shows that quantum computing not only disrupt elite laws of logic, but also unveil conceptual and operational assumptions used today in law systems. Regarding the impact of quantum technologies on intellectual property, cybersecurity, data protection, and contractual liability this paper addresses this research question in the context that it shows the lack of regulation in existing regulatory bodies capable of adequately addressing quantum technologies. While previous studies have focused on topics of interest, this study provides a new learning opportunity to make the observations into a wider, cross-domain framework of quantum governance. This implies not unique or incremental risks, but systemic or predictable risks, resulting in the replacement of existing compliance arrangements.

The study further augments the literature by demonstrating that, while highly important national and international programs are structured, the context of national and international programs is more conventional. Failure of international governance requires coordinated global governance over fragmented national plans to provide sustainable standards, interoperability requirements, and controls. The third research question, on which the paper calls for a common legal structure, proposes that successful quantum governance requires a common legal structure: legally mandated quantum resistant cryptography, modernized IP doctrines for quantum inventions, recommending in-depth data-protection obligations regarding post-quantum risk, and contractual arrangements that expressly assign quantum-related liabilities.

The study provides a new perspective of emerging discourses of anticipatory governance and imagines quantum computing as a disruptive technology that brings us a new paradigm at the intersection of primary legal categories. By continuing to develop quantum capabilities, the legal system must shift from critical recognition to normative action, and provide for quantum technology to emerge in terms of rights, security, and pursuit of equitable and responsible innovation.

REFERENCE

Abbott, R. B. (2018). *Everything is obvious*. UCLA Law Review, 66(2), 401–458. https://doi.org/10.2139/ssrn.3056915

Buchholz, S., McKinney, B., & West, S. (2020). *The realist's guide to quantum technology and national security*. Deloitte. https://www.ndtahq.com/the-realists-guide-to-quantum-technology-and-national-security/

Calo, R. (2017). *Artificial intelligence policy: A primer and roadmap*. https://doi.org/10.2139/ssrn.3015350

Contreras, J. (2023). Open innovation and standardization in quantum technologies. *Journal of Law and the Biosciences, 10*(1), lsad003.

Cowie, G. (2023). Data sovereignty and the quantum threat: Reconsidering GDPR adequacy. *International Data Privacy Law, 13*(2), 97–112.

De Schrijver, S. (2019). Quantum computing: The certainty of the uncertain. *Who's Who Legal*.

European Commission. (2018). *Quantum Flagship initiative*. European Commission Publications.

Flynn, S. (2020). What is quantum computing and how is it disrupting law firms? *Law Technology Today*. https://www.americanbar.org/groups/law_practice/resources/law-technology-today/2020/what-is-quantum-computing-and-how-is-it-disrupting-law-firms/

Fogg, S. (2022). What is GDPR? The basis of the EU's General Data Protection Regulation. *Termly*. https://termly.io/resources/articles/what-is-gdpr/

Frankenfield, J. (2021). *What is cloud computing?* Investopedia. https://www.investopedia.com/terms/c/cloud-computing.asp

Lehot, L. (2020). *Bring on the qubits: How the quantum computing arms race affects legal.* LegalTech News. https://www.law.com/legaltechnews/2020/08/19/bring-on-the-qubits-how-the-quantum-computing-arms-race-affects-legal/

G7. (2025). *Kananaskis Common Vision for the Future of Quantum Technologies*. G7 Leaders' Summit.

Gent, E. (2021). How quantum computers can be used to build better quantum computers. *Singularity Hub*. https://singularityhub.com/2021/10/04/how-quantum-computers-can-be-used-to-build-better-quantum-computers/

Irion, K., & De Hert, P. (2021). The future of data protection: Towards an international framework. *Computer Law & Security Review, 41*, 105523.

Kaminski, M. E. (2022). Technological due process and emerging technologies. *Florida Law Review, 74*(3), 321–380.

Kop, M. (2020). Regulating transformative technology in the quantum age: Intellectual property, standardization & sustainable innovation. *Stanford–Vienna Transatlantic Technology Law Forum*. https://airecht.nl/blog/2020/regulating-transformative-technology-in-the-quantum-age-intellectual-property-standardization-sustainable-innovation

Kop, M. (2021). Quantum computing and intellectual property law. *Berkeley Technology Law Journal, 25*, 101–109. https://law.stanford.edu/wp-content/uploads/2021/06/Mauritz-Kop_Quantum-Computing-and-Intellectual-Property-Law_BTLJ.pdf

Lehot, L. (2020). Bring on the qubits: How the quantum computing arms race affects legal. *LegalTech News*. https://www.law.com/legaltechnews/2020/08/19/bring-on-the-qubits-how-the-quantum-computing-arms-race-affects-legal/

Levinson, B. (2021). Regulating magic: Why we need to establish a regulatory framework for quantum computing and artificial intelligence. *CircleID*. https://circleid.com/posts/20211028-why-we-need-to-establish-regulatory-framework-for-quantum-computing-artificial_intelligence

Long, Y., Liu, Q., & Wang, Y. (2022). Quantum threats to contemporary cryptographic infrastructures. *IEEE Security & Privacy, 20*(4), 40–50.

National Institute of Standards and Technology (NIST). (n.d.). *National Metrology Institute of the United States*. https://www.nist.gov

National Quantum Initiative Act, Pub. L. No. 115-368, 132 Stat. 5092 (2018).

Langeland, J. (2025, December 5). *GDPR in the US: Compliance simplified for businesses*. Termly. https://termly.io/resources/articles/gdpr-in-the-us/

Stilgoe, J. (2023). Anticipatory governance for emerging technologies. *Research Policy, 52*(7), 104789.

United Nations. (n.d.). *International Year of Quantum Science and Technology*. https://www.un.org

Van de Poel, I. (2021). The governance of emerging technologies: Aligning innovation and public values. *Science and Engineering Ethics, 27*, 14.

Wagner, B. L., & Mazarakis, G. (2021). How to protect quantum computing innovations with IP rights. *Bloomberg Law*. https://news.bloomberglaw.com/ip-law/how-to-protect-quantum-computing-innovations-with-ip-rights-5

Wright, G. (2024, December 23). *What is quantum theory?* TechTarget.

