Asian Journal of Law and Policy
Vol. 6 No. 2 (July 2026) eISSN: 2785-8979

The Tortoise, the Hare, and the Harvest: Rethinking Legal Frameworks in Post-Quantum Malaysia

Karisma Karisma
Independent Researcher, Sydney, Australia
karisjay@outlook.com
ORCID iD: 0000-0001-9783-9504
(Corresponding author)

ABSTRACT

Quantum computation unsettles the boundary between theoretical possibility and applied infrastructure, altering how value, knowledge, and strategic power circulate within national economies. While many jurisdictions pursue self-reliant quantum strategies to minimise dependence on foreign actors, Malaysia has adopted a partnership-driven model that integrates international expertise into its emerging quantum ecosystem. Recent developments, including the establishment of Malaysia's Quantum Computing Centre, reflect an ambition to position the country as a regional quantum hub within ASEAN. Notwithstanding these developmental strides, this trajectory generates a core governance tension: reliance on foreign quantum infrastructure risks entrenching technological dependence and information asymmetry, weakening Malaysia's capacity to shape the regulatory conditions under which quantum innovation is deployed. This paper maps the legal vulnerabilities quantum computing presents within Malaysia, focusing on limitations of patent protection for quantum software, the layered operation of copyright across software abstractions, and emerging privacy and cybersecurity challenges. It further examines competition law risks arising from early market dominance and innovation control. By synthesising technical quantum concepts with Malaysian legal frameworks, this analysis advances an adaptive regulatory perspective beyond reactive governance and proposes targeted enhancements.

Keywords: Quantum computing; Legal frameworks; Technology; Malaysia

Received: 22 February 2026, **Accepted:** 29 April 2026, **Published:** 31 July 2026

MULTIMEDIA UNIVERSITY

(2026) Asian Journal of Law and Policy, 6(2), 325–348
https://doi.org/10.33093/ajlp.2026.16

Published by MMU Press. URL: https://journals.mmupress.com/ajlp

1. Introduction

Quantum computation fundamentally reconfigures the relationship between theoretical possibility and practical implementation, creating new pathways through which knowledge, authority, and economic resources flow. Nation-states worldwide have responded by crafting autonomous strategies, committing substantial financial resources toward research infrastructure and capability development to secure domestic competencies (*National Quantum Strategy*, 2023; Organisation for Economic Co-operation and Development, 2025). Malaysia's approach diverges from this self-sufficiency paradigm, instead pursuing a collaborative framework designed to harness expertise from established international actors while securing a position within the nascent quantum landscape. Recent developments demonstrate an expanding quantum infrastructure presence within Malaysia's borders. SDT Inc., acknowledged among South Korea's foremost developers of comprehensive quantum computing systems, entered into a partnership with MIMOS Technology Solutions Sdn. Bhd., culminating in the establishment of Malaysia's inaugural Quantum Computing Centre (Cierra Choucair, 2024). This Quantum Intelligence Centre is a central pillar of Malaysia's National Science, Technology, and Innovation Policy (2021–2030), reinforcing the country's strategic objective of emerging as a regional quantum nexus throughout the ASEAN region (Quantum Computing Report, 2025). SDT, distinguished for its proficiency in quantum hardware architecture and integrated software frameworks, plays a pivotal role in establishing and maintaining operational oversight of the facility (Cierra Choucair, 2024). This development underscores Malaysia's determination to advance quantum technological capabilities while simultaneously enhancing knowledge and technical transfer mechanisms through bilateral engagement, consistent with its comprehensive innovation framework.

Nevertheless, substantial concerns arise from the absence of technological autonomy and the resulting escalation of information asymmetry, potentially culminating in heightened dependence on externally controlled infrastructure. Absent the capacity to determine governing frameworks and operational parameters, Malaysia faces genuine exposure to competitive disadvantage within the quantum development trajectory, a strategic imperative carrying significant implications for essential sectors, including financial services, healthcare delivery, cybersecurity protocols, logistics networks, and data analytics. Additionally, this transformation produces fundamental juridical tensions: As computational architectures become more complex and indeterminate, legal frameworks struggle to maintain relevance. Principal challenges encompass (a) resolving intellectual property disputes arising from quantum software and infrastructure development, (b) addressing heightened data privacy and cybersecurity vulnerabilities under quantum-era threat conditions, (c) preventing anti-competitive conduct and early market dominance from distorting innovation and technological development, while still enabling deployment within Malaysia's regulatory framework.

This paper endeavours to delineate the legal vulnerabilities introduced by quantum computing across diverse application scenarios, thereby informing subsequent governance structures. While existing scholarship has initiated this conversation, the present analysis

extends discourse by synthesising disparate quantum concepts to establish coherent connections among their legal dimensions (Atik and Jeutner, 2021; Balarabe, 2025). Given the technology's nascent state and accelerated development trajectory, considerable uncertainty remains about the likelihood and scale of these vulnerabilities (Scholten et al., 2024). Consequently, this analysis may potentially underrepresent particular challenges or fail to anticipate risks that will manifest subsequently. Nonetheless, through systematic documentation of current legal vulnerabilities and governance deficiencies, this paper establishes groundwork for responsive regulation throughout the quantum epoch, transcending passive observational strategies.

1.1 Research Questions

The existing legal and regulatory frameworks governing emerging technologies frequently demonstrate structural inadequacy, requiring comprehensive revision and recalibration to accommodate the distinctive demands of quantum implementation. Against this backdrop of regulatory insufficiency, this dissertation addresses the following research questions:

i. What governance gaps emerge in Malaysia's legal framework as quantum computing infrastructure is deployed, particularly across (i) the limits of patent protection for quantum software under the Patents Act 1983, (ii) copyright's layered protection of quantum software expressions under the Copyright Act 1987, (iii) personal data protection compliance pressures generated by quantum-era security risks under the retention, notice and choice, disclosure, and security principles of the Personal Data Protection Act 2010, and (iv) competition risks under the Competition Act 2010 relating to restrictions on technological development and the early entrenchment of market dominance?

ii. What regulatory design most effectively addresses quantum-related legal vulnerabilities without impeding technological innovation?

1.2 Research Methodology

In addressing these research questions, the author employed exploratory desk research to generate substantive insights at the intersection of law and quantum technology. Within an emerging field characterized by the rapid adoption of transformative computational paradigms, desk research provides a structured and analytically rigorous methodology for obtaining detailed and impartial information. Complementing this primary approach, the paper further employs doctrinal legal research and textual analysis to identify, interpret, and critically evaluate the legal rules and regulatory instruments governing quantum computing within the Malaysian jurisdiction. This methodological combination enables systematic examination of both the technical dimensions of quantum computing and the normative architecture of Malaysian law, facilitating coherent analytical linkages between quantum concepts and their attendant legal implications.

2. Quantum Computing Fundamentals

Quantum computing represents a computational paradigm harnessing quantum mechanical phenomena, specifically superposition, entanglement, and interference, to execute complex computational operations and address intricate problem sets (Marella and Parisa, 2020). These quantum mechanical characteristics enable quantum systems to approach highly complex computational challenges with substantially greater efficacy than conventional classical computing architectures (Nagy and Akl, 2007). Superposition denotes the capacity of a quantum bit (qubit), constituting the fundamental informational unit for data encoding, to inhabit multiple states or assume numerous distinct values concurrently (Chicano et al., 2025). Diverging from classical bits, which represent exclusively binary values of 0 or 1, qubits maintain simultaneous representation of both 0 and 1, each associated with distinct probability amplitudes (Liu et al., 2025). Consequently, qubits exist within a Hilbert space, a mathematical construct employed to characterise quantum system states, comprising a vector space equipped with an inner product facilitating probability calculations and state overlap determinations (Man'ko and Man'ko, 2023; Newton, 2012).

The superposition characteristic constitutes the fundamental property conferring quantum computers their exponential computational advantage relative to classical systems (Columbus Chinnappan et al., 2025. Entanglement represents a foundational quantum mechanical concept describing how two or more particles establish a correlated state whereby alterations to one particle instantaneously influence the other, irrespective of spatial separation {Columbus Chinnappan, 2025 #115). Within quantum computing contexts, entanglement interconnects qubits, treating their states as singular, unified quantum configurations. This phenomenon permits quantum computers to execute operations across multiple qubits simultaneously while preserving intricate correlations among them (Kundu et al., 2025). Interference permits quantum computers to combine and manipulate probability amplitudes through mechanisms unavailable to classical architectures (Gui-Lu, 2006). Each potential qubit state is associated with a complex number containing both magnitude and phase components. When qubits occupy superposition states, these amplitudes undergo either constructive or destructive interference, reinforcing or diminishing one another (Kovachy et al., 2015). Strategic manipulation enables amplification of correct computational outcomes while reducing probabilities of incorrect results.

Quantum advantage designates the threshold at which quantum computers execute computational tasks with superior effectiveness, exponentially accelerated processing or diminished resource requirements, compared to optimal classical computing systems. This concept does not necessarily imply that classical computers cannot accomplish the task, merely that quantum architectures achieve superior performance, evidencing a fundamental transformation in hardware and software capabilities. Quantum advantage transcends theoretical abstraction, emerging as an imminent commercial reality offering competitive advantages across sectors, spanning molecular simulation for pharmaceutical discovery and materials engineering to real-time adaptive financial systems benefiting from enhanced portfolio optimisation and risk assessment modelling. Additional prominent applications

include supply chain optimisation through route and resource allocation enhancement. Furthermore, quantum systems accelerate pattern recognition capabilities and artificial intelligence model training performance. Quantum supremacy establishes a more stringent benchmark than quantum advantage, denoting computational performance practically unattainable for classical computers within realistic temporal constraints. In 2019, Google announced the achievement of quantum supremacy through its capacity to execute specific computational tasks within 200 seconds compared to the estimated 10,000 years required for classical supercomputers performing identical operations.

Qubits constitute the fundamental operational core of quantum computing. Unlike classical bits maintaining discrete 0 or 1 states, qubits occupy superposition, simultaneously inhabiting both states, and through entanglement mechanisms, establish connections across spatial distances to generate exponential computational capacity by maintaining correlated states. Their physical manifestations vary superconducting qubits maintained near absolute zero temperatures; trapped ions controlled through laser manipulation; photons conveying information via light; electron or nuclear spins confined within quantum dots; and hypothetical topological qubits, theorised to exhibit error resistance.

Quantum logic gates constitute the essential operational architecture of quantum computation, functioning as unitary transformations manipulating qubit states through controlled rotations and entanglement processes. Pauli-X, Y, and Z gates execute specific single-qubit rotations (Mitarai and Fujii, 2021), whereas the Hadamard gate generates superposition by transforming fundamental states into probabilistic combinations (Wong, 2022). The Controlled-NOT (CNOT) gate operates as a two-qubit mechanism establishing entanglement relationships between qubits (Wang et al., 2013). T-gates, comprising single-qubit quantum gates, introduce complex phase rotations, enabling universality throughout the quantum gate configuration (Casas et al., 2026; Prasad, 2026). Sequential arrangement of these gates produces quantum circuits, representing algorithmic processes at the physical implementation level.

Shor's algorithm comprises a quantum computing methodology for integer factorisation, determining prime factors of large composite numbers (Kumar and Mondal, 2024). This capability directly threatens classical cryptographic frameworks, including the Rivest-Shamir-Adleman (RSA) algorithm. RSA encryption fundamentally depends upon the computational intractability of factorising large integers, a task practically infeasible for classical computers within reasonable temporal parameters (Dasari and Dondeti, 2023). However, Shor's algorithm, exploiting quantum superposition and entanglement phenomena, can determine these prime factors in polynomial time, effectively compromising RSA key security (Singh and Sakk, 2024). Conversely, Grover's algorithm represents a quantum methodology designed to accelerate searches in unstructured search problem resolution compared to classical approaches (Shrivastava et al., 2019).

2.1 Quantum Software Stack

A quantum software stack functions as the intermediary between high-level programming constructs and quantum hardware architectures. It commences with quantum programming languages, including Qiskit, Q#, and Cirq, enabling quantum developers to design and implement algorithmic structures (Tripathi et al., 2025). These programs subsequently undergo processing by quantum compilers, which are critical components translating abstract source codes into hardware-specific instructions executable by quantum computers (Schmid et al., 2024). This translation process proves essential in rendering quantum computing accessible. Optimisers embedded within the software stack refine circuits by reducing gate counts, ensuring efficient utilisation of limited qubit resources (Li et al., 2024). Additionally, quantum operating systems manage hardware resource scheduling and error correction protocols. Collectively, these architectural layers enable reliable and efficient communication between software and quantum processors, establishing the foundational infrastructure of quantum computing.

2.2 Quantum Hardware Infrastructure

Quantum hardware infrastructure provides the physical environment required for operating and stabilising quantum processors. Given qubits' extreme sensitivity to thermal fluctuations, electromagnetic interference, and mechanical vibrations, they require maintenance within cryogenic chambers operating near absolute zero to minimise thermal disruption (Baruah et al., 2025; Saklakov, 2025). Vacuum chambers eliminate atmospheric molecules that potentially interfere with qubit coherence, while electromagnetic shielding and vibration isolation mechanisms protect against external perturbations (Brown et al., 2016; Root et al., 2025). Collectively, these systems ensure qubit stability and reduce decoherence, enabling precise quantum state control. This infrastructure constitutes the foundation of reliable quantum computing.

Before proceeding to a detailed examination of each legal framework, it is necessary to briefly map the regulatory terrain within which quantum computing operates in Malaysia. The legal challenges posed by quantum innovation do not fit within a single traditional silo; rather, they intersect four distinct but interrelated domestic frameworks and are further shaped by emerging international standards. An examination of the Patents Act 1983 and the Copyright Act 1987 reveals a fundamental incongruence between the structural requirements of these regimes and the current pace of quantum development. Data privacy concerns are addressed by the Personal Data Protection Act 2010, particularly as quantum computing threatens the integrity of existing data privacy and security standards, compromising classical encryption algorithms, undermining digital signature schemes, and exposing sensitive information across critical sectors. Finally, the Competition Act 2010 addresses competition risks arising from restrictions on technological development and the early entrenchment of market dominance in the quantum computing sphere.

3. Limits of Patent Protection of Quantum Software in Malaysia

Having established quantum computing's foundational architecture, this section examines the extent to which Malaysian patent law accommodates innovations within this domain. Within the quantum computing sphere, patenting quantum technologies presents distinct and multifaceted challenges. These challenges emerge not solely from quantum systems' scientific complexity, but additionally from structural misalignments between patent law's traditional requirements and the manner through which quantum innovation develops and disseminates.

The Patents Act 1983 (PA 1983) establishes patentability through cumulative statutory criteria. Generally, quantum hardware inventions integrate more readily within the Act's framework because they typically manifest as tangible products or technically grounded processes. Conversely, software-related innovations, including quantum software, encounter greater difficulty where patent claims risk classification as abstract or mathematical methods possessing non-deterministic characteristics (Kop et al., 2022). This analysis, therefore, explores how quantum computing inventions can be coherently situated within Malaysia's patentability framework.

Section 12 of the PA 1983 mandates that inventions must constitute ideas capable of resolving specific problems within technological fields through practical application.[1] Within quantum computing contexts, this requirement signifies that purely abstract developments in quantum theory or algorithmic logic prove insufficient for patentability absent manifestation as practical technological applications, for instance, methodologies for controlling qubits, executing quantum gates, or enhancing system stability and coherence (Shahshahani, 2025).

Furthermore, Section 13 imposes critical constraints by excluding discoveries, scientific theories, and mathematical methods from patent protection.[2] This provision directly impacts quantum computing innovations because numerous foundational advances, particularly quantum algorithms and optimisation techniques, initially undergo formulation and expression as mathematical constructs (Kop et al., 2022). Such subject matter falls squarely within statutory exclusions unless the invention receives claims as an integral component of concrete technical processes or physical implementations producing tangible technological effects.

Regarding novelty pursuant to Section 14, assessment occurs against prior art disclosed globally.[3] This criterion proves particularly challenging within quantum computing, given the field's robust culture of early and open dissemination through academic journals, international conferences, and preprint servers. Theoretical disclosures and preliminary literature can therefore readily compromise novelty before formal patent application filing. Inventors must remain acutely aware that public presentations or publications, even those

[1] Patents Act 1983, s 12.

[2] Patents Act 1983, s. 13.

[3] Patents Act 1983, s. 14.

intended exclusively for academic audiences, may constitute novelty-destroying prior art under this absolute novelty standard. Section 15 demands an inventive step, requiring courts to evaluate whether claimed inventions would have been obvious to persons possessing ordinary skill within the relevant art.[4] Within the quantum computing domain, this hypothetical skilled person likely receives characterisation as a highly specialised practitioner possessing advanced knowledge of quantum physics, quantum information theory, and engineering principles. Consequently, incremental refinements to existing quantum architectures or algorithms may receive determinations of obviousness and thus unpatentability. By contrast, solutions overcoming fundamental technical barriers, including novel error-correction schemes, unexpected improvements in qubit coherence times, or innovative methodologies for mitigating decoherence, demonstrate substantially greater likelihood of satisfying inventive step requirements by evidencing non-obvious advances over prior art.

Finally, Section 16 requires industrial applicability, demanding inventions demonstrate capacity for manufacture or industrial use.[5] This requirement thereby excludes purely speculative concepts or laboratory-bound demonstrations lacking practical reproducibility. Numerous quantum computing inventions remain confined to highly controlled laboratory environments, dependent upon specialised conditions including ultra-low cryogenic temperatures, custom-fabricated hardware, and fragile quantum states not yet amenable to reliable reproduction or scaling for routine industrial deployment (De Leon et al., 2021; Fu et al., 2021).

Although quantum inventions may possess scientific significance or theoretical validity, they may nevertheless fail to demonstrate the practical operability and industrial reproducibility levels that Section 16 demands. Where invention utility remains probabilistic or contingent upon future technological breakthroughs not yet achieved, substantiating claims that inventions can presently undergo manufacture or industrial use as the statute requires becomes difficult. Consequently, for numerous quantum computing innovations, the industrial applicability criterion operates as a substantial patentability barrier. This reflects the legal system's fundamental preference for protecting technologies progressing beyond proof-of-concept stages and entering phases of practical, commercially viable industrial deployment.

4. Copyright Protection for Quantum Software in Malaysia

Within Malaysia, categories of works eligible for copyright protection receive primary definition under Section 7(1) of the Copyright Act 1987 (CA 1987), which expressly includes literary works.[6] Significantly, this category encompasses computer programs, thereby extending copyright protection to software-based creations. To understand how quantum

[4] Patents Act 1983, s. 15.

[5] Patents Act 1983, s. 16.

[6] Copyright Act 1987, s. 7(1).

software integrates within this framework, examining the statutory definition of 'computer program' provided in Section 3 of the CA 1987 proves instructive:[7]

> *'An expression, in any language, code or notation, of a set of instructions (whether with or without related information) intended to cause a device having an information processing capability to perform a particular function either directly or after either or both of the following: (a) conversion to another language, code or notation; (b) reproduction in a different material form.'*

This statutory definition encompasses quantum software innovations, quantum arithmetic circuits (including quantum addition, multiplication, and exponentiation), quantum programming paradigms and application programming interfaces (APIs), alongside quantum error correction protocols and stabilisation codes. Quantum software receives expression in source code written in quantum programming languages (Fingerhuth et al., 2018), circuit descriptions specifying quantum gates and measurement operations, or other structured notations designed to instruct information-processing devices. These expressions satisfy the statutory requirement of materialisation in tangible form.

Analogous to classical software, copyright protection attaches to original expression embodied in quantum programs, provided they reflect sufficient authorial effort and skill, and have been fixed in writing, recorded digitally, or otherwise reduced to material form as required by Section 7(1)(b) of the CA 1987. The critical consideration remains not the functional capability of quantum software but rather the originality and effort reflected in its expression.

Quantum software characteristically exists across multiple layers of abstraction and representation. These layers include high-level quantum source code written in languages including Qiskit, Cirq, or Q#,(Tripathi et al., 2025), intermediate circuit representations specifying quantum gate sequences and qubit interactions, and lower-level compiled instructions optimised for specific quantum hardware architectures(Chong et al., 2017). Each stage in this development and compilation process may involve instruction transformation into alternative languages, codes, or notational systems within the meaning of Section 3 of the CA 1987.[8]

Consequently, each representational layer may potentially constitute a derivative work pursuant to Section 8 capable of independent copyright protection, provided the requisite originality threshold receives demonstration. Copyright may subsist separately in these intermediate representations where sufficient intellectual effort, skill, and judgment have been exercised in their creation, even though they remain functionally equivalent or derive from common underlying algorithms.[9] The multiplication of protectable expressions across these abstraction layers creates a layered copyright architecture that can provide comprehensive protection for quantum software innovations.

[7] Copyright Act 1987, s. 3.

[8] Copyright Act 1987, s. 3.

[9] Copyright Act 1987, s. 8.

Conversely, unauthorised reverse-engineering of a substantial part of a protected expression at any developmental stage may constitute copyright infringement under Malaysian law, notwithstanding achievement of functional equivalence through different code implementations. This principle establishes that even where competing quantum programs produce identical computational results or implement identical quantum algorithms, copyright infringement may still occur if the expression, the specific arrangement of code, circuit topology, or notation, has been substantially copied. Functional equivalence alone does not provide a defence to infringement where protected expression itself has been appropriated without authorisation.

5. Emerging Data Privacy and Security Issues in the Quantum Landscape

The emergence of quantum computing capabilities significantly amplifies risks associated with data privacy and cybersecurity breaches. These advanced computational systems possess the potential to compromise classical encryption algorithms, thereby exposing sensitive information across critical sectors, including healthcare, financial services, and governmental operations. Communications previously considered secure through conventional encryption methods could become vulnerable to exploitation by malicious actors. Additionally, quantum computing threatens the integrity of digital signature schemes and authentication protocols, potentially enabling sophisticated fraud and forgery attacks. Although practical, large-scale quantum computing remains a distant prospect, adversaries are already employing 'harvest now, decrypt later' strategies, systematically collecting encrypted data in the present with the objective of decrypting it once quantum computational capabilities become sufficiently advanced (Singh, 2024).

5.1 Retention Principle

Section 10 of Malaysia's Personal Data Protection Act 2010 (PDPA 2010) establishes the retention principle, which mandates that personal data must not be kept longer than necessary for its designated purpose, accompanied by an affirmative obligation to ensure prompt destruction or permanent deletion when retention is no longer justified.[10]

Issue

Quantum computing fundamentally complicates compliance with this statutory requirement by introducing unprecedented long-term confidentiality vulnerabilities. Continued retention of personal information beyond the period of necessity not only heightens exposure to future security compromises but may also become increasingly difficult to characterise as 'reasonable' once the foreseeability of quantum-related threats is properly acknowledged and factored into data governance decisions. Even when held for ostensibly legitimate purposes, including regulatory compliance or backup preservation, data retained over extended periods may become susceptible to future quantum-enabled

[10] Personal Data Protection Act 2010, s. 10.

decryption attacks (Ezeogu, 2025), particularly where encrypted archives are maintained in long-term storage.

Potential Solution

This technological shift substantially increases the importance of implementing strict retention limits and establishing robust deletion practices. Organisations can no longer assume that encryption alone provides enduring protection for data held beyond its immediate operational purpose.

5.2 Notice and Choice Principle

Per Section 7 of the PDPA 2010, the Notice and Choice Principle requires data users to inform individuals about the collection and use of their personal data and to obtain their consent.[11] It ensures transparency and allows individuals to make informed choices regarding their data, including the right to access, correct, or withdraw consent.

Issue

With the advancing capabilities of quantum computing, the notice requirements established under Section 7 demand renewed scrutiny. Continued reliance on privacy notices that presume enduring security based on classical cryptographic assumptions may become misleading or materially incomplete.

Potential Solution

Notices must remain adequate and meaningful in light of evolving technological threats. While data users cannot be expected to predict the precise timeline of quantum capability development, material limitations in data protection measures that substantively affect a data subject's capacity to make informed choices about their personal information may need to be transparently communicated to maintain statutory compliance.

5.3 Disclosure Principle

The disclosure principle articulated in Section 8 restricts the disclosure of personal data to purposes for which consent was obtained at the time of collection, or to purposes directly related thereto, while limiting disclosure to specified categories of third parties.[12]

Issue

Quantum computing introduces substantial complications for compliance with this principle by materially increasing the risk of unauthorised or unintended disclosure events. When encrypted data becomes compromised through quantum-capable decryption techniques, disclosure may occur entirely outside the scope of consented purposes and reach recipients

[11] Personal Data Protection Act 2010, s. 8.

[12] Personal Data Protection Act 2010, s. 8.

beyond those originally contemplated, even absent any deliberate wrongdoing or negligent action by the data user (Baseri et al., 2026). This creates a scenario where technical vulnerability, rather than human failure, drives non-compliance.

Potential Solution

The primary and potent technical response lies in the proactive adoption of Post-quantum Cryptographic (PQC) standards that are resistant to quantum-enabled attacks (Kan and Une, 2021). While quantum decryption capabilities remain largely prospective, the principle of anticipatory compliance requires data users to prepare for foreseeable technological risks (as discussed below). Importantly, the failure to migrate to quantum-resistant encryption, once such standards are reasonably entrenched and available, may itself constitute a breach of data protection obligations.

5.4 Security Principle

Section 9 of the PDPA 2010 establishes the security principle, imposing a continuing statutory obligation on data users to adopt 'practical steps' to safeguard personal data. This obligation is assessed contextually with reference to factors including the nature of the data, sensitivity of information, storage mechanisms, personnel access controls, and data transfer protocols.[13]

Issue

Quantum decryption capabilities directly challenge the adequacy of this obligation in its current implementation. Encryption constitutes a fundamental security measure expressly contemplated under Sections 9(1)(c) and 9(1)(e). However, cryptographic safeguards that prove adequate against classical computational attacks may become fundamentally ineffective when confronted with quantum adversaries employing algorithms such as Shor's algorithm for factoring large integers or Grover's algorithm for searching unstructured databases (Ansari et al., 2025). Consequently, data users who continue to rely exclusively on classical encryption methodologies may fail to satisfy the statutory standard of protection, even where those measures were fully compliant and represented best practices at the time of their initial deployment.

Potential Solution

The PDPA 2010's risk-based statutory language suggests that the foreseeability of quantum threats may necessitate anticipatory adaptation measures, including proactive migration toward post-quantum cryptographic standards and quantum-resilient security architectures. As quantum computing transitions from theoretical possibility to practical reality, the definition of 'reasonable' security measures under Section 9 must correspondingly evolve to account for this foreseeable threat landscape.

[13] Personal Data Protection Act 2010, s. 9.

Section 9(2) extends the security principle beyond the data user's immediate operational systems by imposing an affirmative duty to ensure that any engaged data processor provides 'sufficient guarantees' with respect to technical and organisational security measures.[14] This provision further mandates that reasonable steps be taken to ensure ongoing compliance with those protective measures throughout the processing relationship. This framework reflects an accountability-based model of data protection that emphasises continuous oversight rather than one-time verification.

Quantum computing substantially intensifies this statutory obligation. Data users may no longer defensibly rely on generic security assurances or industry-standard certifications when engaging processors such as cloud service providers, managed IT vendors, or outsourced data handling firms. Instead, 'sufficient guarantees' under Section 9(2)(a) may increasingly require demonstrable quantum-resilient capabilities, including documented readiness for post-quantum cryptography implementation, deployment of adaptive security frameworks capable of responding to evolving threats, and concrete plans for migration to quantum-safe protocols.[15]

Failure to reassess and update processor safeguards in light of foreseeable quantum-related risks could render previously adequate contractual security assurances insufficient, thereby exposing data users to substantial regulatory enforcement action and civil liability under the PDPA 2010. The statutory duty to ensure processor compliance is not discharged through initial due diligence alone but requires ongoing monitoring and adaptation as the threat environment evolves.

Given these multifaceted data protection challenges, regulatory authorities should actively consider developing comprehensive frameworks to support phased migration toward PQC standards that have been validated and standardised by bodies such as the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). The domestic hurdles are mirrored by parallel standardisation efforts led by the European Telecommunications Standards Institute (ETSI) and European Union Agency for Cybersecurity (ENISA), which provide the technical scaffolding for future-proofing legal regimes. The Technical Committee on Quantum Technologies (TC QT) at ETSI is instrumental in advancing technical specifications for quantum communications (European Telecommunications Standards Institute, n.d.). These efforts ensure international coherence and align with broader regulatory movements, such as the proposed European Quantum Act (Institute, n.d.). ENISA has transitioned from theoretical analysis to publishing structured methodologies for evaluating 'quantum-safe solutions'. Their recent focus on post-quantum cryptographic standards provides a critical blueprint for transitioning legacy systems to more resilient, quantum-resistant architectures(European Union Agency for Cybersecurity, n.d.).

[14] Personal Data Protection Act 2010, s. 9(2).

[15] Personal Data Protection Act 2010, s. 9(2).

Additionally, regulators should explore piloting advanced quantum-secure technologies, including Quantum Key Distribution (QKD) systems, which leverage the fundamental principles of quantum mechanics to detect eavesdropping attempts and ensure cryptographic key security. Proactive regulatory guidance in this domain would assist data users in understanding their evolving obligations and provide a structured pathway toward quantum-resilient data protection frameworks.

6. Competition Law and Quantum

Per Section 4 of the Competition Act 2010: 'A horizontal or vertical agreement between enterprises is prohibited insofar as the agreement has the object or effect of significantly preventing, restricting or distorting competition in any market for goods or services'.[16] This provision enumerates various conventional anti-competitive practices, including price manipulation schemes, territorial allocation arrangements, and collusive tendering. However, Section 4(2)(c)(iii) holds particular relevance for nascent technology industries through its proscription of agreements constraining 'technical or technological development', which bears direct relevance to quantum computing markets, where competitive dynamics centre predominantly upon innovation velocity rather than conventional price mechanisms.[17]

Traditional competition law enforcement typically scrutinises pricing conduct, production limitations, or geographic market partitioning. Quantum computing ecosystems, however, function as emerging domains where competitive advantage derives fundamentally from technological progression rates and developmental trajectories (Coccia et al., 2022). Market participants compete across multiple quantum technology layers: Hardware components encompassing qubit systems, cryogenic infrastructure, control mechanisms, and measurement apparatus; software elements including error mitigation protocols, compilation frameworks, algorithmic implementations, and scalable architectural designs. Arrangements restricting advancement within these technological dimensions risk stifling innovation while simultaneously distorting competitive market structures throughout Malaysia.

Practically speaking, quantum computing development ecosystems necessarily involve collaborative mechanisms, strategic alliances, inter-enterprise joint ventures, and reciprocal intellectual property licensing frameworks (Cierra Choucair, 2024). Such cooperative structures carry legitimate justification given quantum research and development's resource intensity and inherently multidisciplinary character. Nevertheless, this collaborative orientation simultaneously creates conditions potentially conducive to anti-competitive coordination practices. Competing quantum technology enterprises might, for instance, establish exclusive or limiting arrangements precluding the pursuit of alternative quantum architectural paradigms or deliberately abstaining from developing rival quantum software

[16] Competition Act 2010, s. 4.

[17] Competition Act 2010, s. 4(2)(c)(iii).

frameworks, thereby cementing prevailing technological trajectories while erecting substantial market entry obstacles confronting nascent or resource-constrained participants.

Evidently, should enterprises be conducting operations within Malaysian jurisdiction and coordinate activities in a manner suppressing technological advancement, such conduct threatens Malaysia's competitive positioning internationally while simultaneously diminishing domestic capability development across quantum computing domains.

Further, the CA 2010 prohibits business entities from 'engaging, whether independently or collectively, in any conduct which amounts to an abuse of a dominant position in any market for goods or services'. The legislative framework clarifies, under Section 10(2), that the listed abusive practices are illustrative rather than exhaustive. In the context of quantum computing, this analysis considers relevant Section 10(2) elements, particularly subsections (a) and (b), to clarify their legal application and identify scenarios in which business conduct within quantum technology sectors may warrant regulatory scrutiny.[18]

6.1 Unfair Commercial Terms and Pricing Exploitation Under Section 10(2)(a)

The abusive exercise of market dominance may include imposing an 'unfair purchase or selling price or other unfair trading condition on any supplier or customer', as specified in Section 10(2)(a) of the legislation. Quantum computing service providers with significant market power (Aboy et al., 2022) could exploit this position through pricing structures or contractual obligations that disadvantage service consumers. For example, if a quantum cloud platform attains the status of indispensable infrastructure, the operator may impose economically unreasonable fees for computational tasks or require extended exclusivity through restrictive contracts. Such pricing strategies, which surpass competitive norms, exploit consumers who have limited alternatives, a situation exacerbated by the nascent market and scarcity of substitutes. Additionally, dominant entities may employ targeted below-cost pricing for specific consumer segments or regions, intentionally creating barriers for new entrants and reinforcing their own market position. When these strategies are intended to exclude competitors or produce anti-competitive effects, the conduct exhibits characteristics of predatory pricing.

6.2 Production Controls and Market Entry Impediments under Section 10(2)(b)

Abusive dominance also encompasses 'limiting or controlling, (i) production; (ii) market outlets or market access; (iii) technical or technological development; or (iv) investment, to the prejudice of [the] consumer', as outlined in Section 10(2)(b).[19] Quantum computing operators with dominant positions may impose artificial restrictions on the distribution of quantum processing equipment or the provision of network-based computational services within Malaysia. Such operators might intentionally limit the availability of quantum

[18] Competition Act 2010, s. 10.

[19] Competition Act 2010, s. 10.

hardware or reduce the penetration of quantum computing services, not due to legitimate engineering or operational considerations, but to sustain high prices, redirect resources to other regions, or favour specific partnerships. These actions can disadvantage local commercial stakeholders.

In Malaysia, dominant market actors may also design, implement, or structure their technological platforms and operational frameworks in ways that increase competitors' entry or expansion costs, even when less restrictive alternatives are available. In the absence of valid business justifications (Ramaiah, 2015), such exclusionary technological choices can result in market closure by limiting cross-platform compatibility, increasing consumer switching costs, and hindering effective competition. Collectively, these strategies slow the pace of innovation and delay the adoption of advanced quantum computing technologies, ultimately harming consumers by restricting technological progress and diminishing competitive benefits.

In sum, quantum computing introduces unique structural vulnerabilities to competition, with dominance likely to emerge early through control of key technologies, platforms, and IP. In navigating the intersection of IP and competition law in quantum computing, regulators must strike a careful balance: Protecting genuine innovation while curbing exclusionary practices that use proprietary quantum technologies to entrench dominance and suppress ecosystem-wide development. The CA 2010 offers a robust statutory basis to address such concerns, particularly through Sections 4 and 10. However, regulatory vigilance must evolve alongside technological developments. Proactive enforcement and sector-specific guidance will be essential to prevent monopolistic structures, ensure open market access, and sustain innovation within Malaysia's emerging quantum ecosystem.

7. Regulatory Analysis and Recommendations: Toward Quantum-Resilient Future

Principle-based regulation denotes a shift away from reliance on 'detailed' and 'prescriptive rules' toward the use of broadly stated principles to prescribe standards and guide regulatory conduct. Such an approach facilitates regulatory openness and flexibility, reducing the risk that technologies become encumbered by a dense 'regulatory thicket', a characteristic of a highly rule-centric approach (Fenwick et al., 2017). By the adoption of a principle-based approach, innovation can proceed without undue compliance burdens while maintaining meaningful oversight. Its durability lies in its capacity to remain effective over time, as the regulatory framework can adjust to ongoing technological developments and shifting market conditions without requiring constant legislative amendments (Black, 2010).

In the context of quantum computing, however, a principle-based regulatory approach may prove inadequate. Its inherent vagueness can undermine navigability, making it more difficult for regulatory entities and stakeholders alike to identify applicable obligations and anticipate compliance expectations. Given the open-textured nature of principles in the field of quantum computing, there is a risk of inconsistent, erroneous, and egregious

interpretation. To mitigate these risks, regulators typically supplement principles with extensive guidance or conduct post-implementation reviews. However, in a field as rapidly evolving as quantum technologies, such guidance can quickly become outdated or even contradictory unless regulators undertake a holistic review prior to issuing further materials. Nevertheless, even this exercise may be practically impossible given the novelty and unpredictability of the technology. Firms may become overly cautious to the extent that they delay deployment for fear of breaching poorly defined regulatory principles. Start-ups and new entrants in the field of quantum technology may face heightened barriers to entry due to a lack of compliance resources of established actors. The very flexibility offered by principle-based regulation may, paradoxically, generate uncertainty and impede technological development in high-velocity domains such as quantum computing. With quantum computing now applied to complex problems across healthcare, finance, logistics, manufacturing, and energy, the legal and ethical implications become more pronounced. Relying solely on a principles-based framework may therefore be inadequate to ensure the proper, fair, and responsible use and deployment of quantum technologies.

Although recent and embryonic advances in quantum computing have attracted considerable attention, the technology is still far from large-scale commercial use (McKinsey and Company, 2025). This has created a gap in regulating a technology that is potentially transformative, but whose developmental path is unpredictable. Should regulators utilise precautionary principles in shaping standards and parameters, or should they adopt wait-and-see measures until quantum computing technologies are more clearly defined? Generally, the precautionary approach authorises regulatory intervention even where evidence of harm is incomplete or uncertain (Todt and Luján, 2014). Under this model, uncertainty itself justifies pre-emptive action. It presumes that where risk cannot be ruled out, potentially harmful activity should be restricted until it can be shown to pose an acceptable or negligible level of risk.

In the context of rapidly advancing quantum technology, there are legitimate concerns about its effects on individual welfare and broader societal conditions. However, precautionary regulation is ill-suited to quantum technology, as the approach risks technology stagnation. Grounded in speculative and hypothetical harms that may never materialise, precautionary regulation risks suppressing beneficial development long before any demonstrable risk emerges. This is similarly a concern when utilising ex-ante, or 'before the fact', approaches to regulate discrete and opaque quantum systems (Scherer, 2016). By exploiting superposition and entanglement, quantum computers can explore vast solution landscapes simultaneously, enabling them to propose outcomes that humans may not have anticipated or may have deemed implausible using classical analytic methods.

In deploying quantum technology and avoiding the pitfalls of the tortoise-and-hare sprint, it is important to establish an intuitive and evolving regulatory framework or buffer regime, ensuring that modifications and changes can occur effectively in response to novel circumstances. Consider, for instance, the development of workable methods to allow qubits to hold information for meaningful and informative calculations. These methods also

provide robust pathways for breaking modern cryptographic systems (Kandula, 2025). In these likely circumstances, it becomes crucial that regulatory frameworks remain flexible enough to counter the risks posed by quantum technology, especially when new cryptographic vulnerabilities emerge, breaking existing encryption protocols, or when cloud-based access to quantum processors raises issues around data rights and potential misuse by threat actors across the globe. Recently, NIST released its quantum-resistant encryption algorithms to defend against quantum-based cyberattacks (Käppler and Schneider, 2022). Such domain-specific standards can be extended to mitigate risks by providing regulatory scaffolding in areas like data privacy and cybersecurity while preventing technological stagnation.

There are clear merits for Malaysia in adopting soft-law regimes, particularly given the uncertainty surrounding the speed, imminence, potential, and extent of quantum breakthroughs. Additionally, adaptive regulation can be complemented by risk-based frameworks. The logic underpinning a risk-based approach is straightforward: The greater the potential harm, the stricter the obligations and the more extensive the regulatory instruments required (Black and Baldwin, 2010). Assessing potential risks requires considering all aspects of sociotechnical systems. By developing a structured risk-classification framework, quantum computing technologies can be categorised according to whether they pose negligible, moderate, or serious potential harm. Such differentiation facilitates proportionate regulatory responses, ensuring that oversight intensifies in line with the level of risk. For instance, a quantum computing system that predicts crop yields clearly poses far less risk than one capable of decrypting sensitive satellite-based intelligence from other jurisdictions or territories.

This brings us back to the realities of the Collingridge dilemma in the domain of quantum computing. Collingridge observed that the social consequences of emerging technologies are often impossible to predict in their early stages, before they are widely deployed and utilised (Cecchi et al., 2024; Collingridge, 1980). However, once a technology becomes deeply embedded in society, introducing effective regulation becomes significantly more difficult and costly (Collingridge, 1980; Kudina and Verbeek, 2019). This presents a core dilemma: Regulators face an uncertainty paradox or the benefit of hindsight regarding how quantum technology will evolve.

8. Conclusion

Compounding the challenges discussed above, quantum computing is likely to accumulate technological momentum, making it increasingly resistant to regulatory intervention over time. As such, adaptive and risk-based regulatory frameworks can provide a measured approach by enabling early intervention before harmful practices become deeply entrenched in systems, while simultaneously preventing technological stagnation.

Acknowledgement

I am deeply grateful to have mentors, teachers, family, and friends who offered unwavering support and encouragement throughout the research and writing process.

Funding Statement

The author received no funding from any party for the research and publication of this article.

Author's Contributions

The author contributed to the final version and approved the submission.

Conflict of Interest Declaration

The author declares that no conflict of interest in this study.

Ethics Approval

Ethical approval was not required for this study as it is based on doctrinal legal research involving the analysis of legislation, case law, and secondary sources, and does not involve human participants, personal data, or sensitive materials.

AI Usage Declaration

The author declares that no AI tools were used to generate the substantive content, analysis, or conclusions of this manuscript. The author has reviewed and takes full responsibility for the content of this work.

References

Aboy, M., Minssen, T., & Kop, M. (2022). Mapping the patent landscape of quantum technologies: Patenting trends, innovation and policy implications. *IIC – International Review of Intellectual Property and Competition Law, 53*(6), 853–882. https://doi.org/10.1007/s40319-022-01209-3

Ansari, N. M., Tariq, T., Iqbal, R., Abbas, A., Abbas, H., & Zohaib, M. M. (2025). Quantum cryptography: Securing data in the post-quantum computing era—A comprehensive exploration of the future of cybersecurity. *Kashf Journal of Multidisciplinary Research, 2*(2), 28–43. https://doi.org/10.71146/kjmr259

Atik, J., & Jeutner, V. (2021). Quantum computing and computational law. *Law, Innovation and Technology, 13*(2), 302–324. https://doi.org/10.1080/17579961.2021.1977216

Balarabe, K. (2025). Quantum computing and the law: Navigating the legal implications of a quantum leap. *European Journal of Risk Regulation, 16*(2), 794–813. https://doi.org/10.1017/err.2025.8

Baruah, R., Portugal, P., Wabnig, J., & Flindt, C. (2025). Fast, accurate, and local temperature control using qubits. *Physical Review B, 111*(12), 125406. https://doi.org/10.1103/PhysRevB.111.125406

Baseri, Y., Chouhan, V., & Ghorbani, A. (2026). Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure. *Computers & Security, 167*, 104917. https://doi.org/10.1016/j.cose.2026.104917

Black, J. (2010). *The rise, fall and fate of principles based regulation*. (Legal Studies Working Paper No. 17/2010). London School of Economics and Political Science, Law School.

Black, J., & Baldwin, R. (2010). Really responsive risk-based regulation. *Law & Policy, 32*(2), 181–213. https://doi.org/10.1111/j.1467-9930.2010.00318.x

Brown, K. R., Kim, J., & Monroe, C. (2016). Co-designing a scalable quantum computer with trapped atomic ions. *npj Quantum Information, 2*, 16034. https://doi.org/10.1038/npjqi.2016.34

Casas, B., Braccia, P., Gouzien, E., Cerezo, M., & Garcia-Martin, D. (2026). *Matchgate synthesis via Clifford matchgates and T gates* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2602.05425

Cecchi, R., Haja, T. M., Calabro, F., Fasterholdt, I., & Rasmussen, B. S. B. (2024). Artificial intelligence in healthcare: Why not apply the medico-legal method starting with the Collingridge dilemma? *International Journal of Legal Medicine, 138*, 1173–1178. https://doi.org/10.1007/s00414-023-03152-5

Chicano, F., Luque, G., Dahi, Z. A., & Gil-Merino, R. (2025). Combinatorial optimization with quantum computers. *Engineering Optimization, 57*(1), 208–233. https://doi.org/10.1080/0305215X.2024.2435538

Chong, F. T., Franklin, D., & Martonosi, M. (2017). Programming languages and compiler design for realistic quantum hardware. *Nature, 549*, 180–187. https://doi.org/10.1038/nature23459

Choucair, C. (2025, January 1). *It takes a village: Top 10 qquantum partnerships of 2024*. The Quantum Insider. https://thequantuminsider.com/2025/01/01/it-takes-a-village-top-10-quantum-partnerships-of-2024/

Choucair, C. (2024, November 13). *Malaysia's first quantum computing centre launched through SDT Inc. and MIMOS partnership*. The Quantum Insider. https://thequantuminsider.com/2024/11/13/malaysias-first-quantum-computing-centre-launched-through-sdt-inc-and-mimos-partnership/

Coccia, M., Roshani, S., & Mosleh, M. (2022). Evolution of quantum computing: Theoretical and innovation management implications for emerging quantum industry. *IEEE Transactions on Engineering Management, 71*, 2270–2280. https://doi.org/10.1109/TEM.2022.3175633

Collingridge, D. (1980). The dilemma of control. In *The social control of technology* (pp. 13–22). Francis Pinter.

Chinnappan, C. C., Krishnan, P. T., Elamaran, E., Arul, R., & Kumar, T. S. (2025). Quantum computing: Foundations, architecture and applications. *Engineering Reports, 7*(8), e70337. https://doi.org/10.1002/eng2.70337

Dasari, Y., & Dondeti, V. (2023). RSA security in cloud computing: A distributed model for integrated GNFS with Black Wiedemann algorithm for integer factorization. *AIP Conference Proceedings, 2938*(1), Article 030008. https://doi.org/10.1063/5.0182676

De Leon, N. P., Itoh, K. M., Kim, D., Mehta, K. K., Northup, T. E., Paik, H., Palmer, B. S., Samarth, N., Sangtawesin, S., & Steuerman, D. W. (2021). Materials challenges and opportunities for quantum computing hardware. *Science, 372*(6539) Article abb2823. https://doi.org/10.1126/science.abb2823

European Union Agency for Cybersecurity. (n.d.). *Cryptography*. https://www.enisa.europa.eu/topics/digital-identity-and-data-protection/cryptography

Ezeogu, A. O. (2025). Post-quantum cryptography for healthcare: Future-proofing population health databases against quantum computing threats. *Research Corridor Journal of Engineering Science, 2*(1), 29–56.

Fenwick, M. D., Kaal, W. A., & Vermeulen, E. P. M. (2017). Regulation tomorrow: What happens when technology is faster than the law? *American University Business Law Review, 6*(3), 561. https://dx.doi.org/10.2139/ssrn.2834531

Fingerhuth, M., Babej, T., & Wittek, P. (2018). Open source software in quantum computing. *PLOS ONE, 13*(12), Article e0208561. https://doi.org/10.1371/journal.pone.0208561

Fu, H., Wang, P., Hu, Z., Li, Y., & Lin, X. (2021). Low-temperature environments for quantum computation and quantum simulation. *Chinese Physics B, 30*(2), Article 020702. https://doi.org/10.48550/arXiv.2010.15626

Gui, L. L. (2006). General quantum interference principle and duality computer. *Communications in Theoretical Physics, 45*(5), 825–844. https://doi.org/10.48550/arXiv.quant-ph/0512120

European Telecommunications Standards Institute. (n.d.). *Technical Committee (TC) Quantum Technologies*. https://www.etsi.org/committee/2600-quantum-technologies

Kan, K., & Une, M. (2021). Recent trends on research and development of quantum computers and standardization of post-quantum cryptography. *Monetary and Economic Studies, 39*, 77–108. https://www.imes.boj.or.jp/research/papers/english/me39-6.pdf

Kandula, S. R. (2025). Breaking traditional encryption: Quantum computing risks to web and mobile applications. *International Journal of Advanced Research in Engineering and Technology, 16*(2), 329–342. https://doi.org/10.34218/IJARET_16_02_020

Kappler, S. A., & Schneider, B. (2022). Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms. *Proceedings of the Society, 84*, 61–71. https://doi.org/10.29007/2tpw

Kop, M., Aboy, M., & Minssen, T. (2022). Intellectual property in quantum computing and market power: A theoretical discussion and empirical analysis. *Journal of Intellectual Property Law and Practice, 17*(8), 613–628. https://doi.org/10.1093/jiplp/jpac060

Kovachy, T., Asenbaum, P., Overstreet, C., Donnelly, C. A., Dickerson, S. M., Sugarbaker, A., Hogan, J. M., & Kasevich, M. A. (2015). Quantum superposition at the half-metre scale. *Nature, 528*, 530–533. https://doi.org/10.1038/nature16155

Kudina, O., & Verbeek, P. (2019). Ethics from within: Google Glass, the Collingridge dilemma, and the mediated value of privacy. *Science, Technology, & Human Values, 44*(2), 291–314. https://doi.org/10.1177/0162243918793711

Kumar, M., & Mondal, B. (2024). Study on implementation of Shor's factorization algorithm on quantum computer. *SN Computer Science, 5*, Article 413. https://doi.org/10.1007/s42979-024-02771-y

Kundu, S., Gupta, T., Sardar, A., Bandyopadhyay, A., Swain, S., & Mallik, S. (2025). A survey on quantum computing: Transforming cryptography, AI/ML, blockchain, and network communication. *Franklin Open, 12*, Article 100371. https://doi.org/10.1016/j.fraope.2025.100371

Li, Z., Peng, J., Mei, Y., Lin, S., Wu, Y., Padon, O., & Jia, Z. (2024). Quarl: A learning-based quantum circuit optimizer. P*roceedings of the ACM on Programming Languages, 8*(OOPSLA1), Article 114. https://doi.org/10.1145/3649831

Liu, Y., John, J., & Wang, Q. (2025). E-loQ: Enhanced locking for quantum circuit IP protection. *2025 IEEE International Symposium on Hardware Oriented Security and Trust*. https://doi.org/10.48550/arXiv.2412.17101

Man'ko, M. A., & Man'ko, V. I. (2023). Probability distributions describing qubit-state superpositions. *Entropy, 25*(10), Article 1366. https://doi.org/10.3390/e25101366

Marella, S. T., & Parisa, H. S. K. (2020). Introduction to quantum computing. In Y. Zhao (Ed.), *Quantum computing and communications*. IntechOpen. https://doi.org/10.5772/intechopen.94103

McKinsey & Company. (2025, March 31). *What is quantum computing?* https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing

Mitarai, K., & Fujii, K. (2021). Constructing a virtual two-qubit gate by sampling single-qubit operations. *New Journal of Physics, 23*, Article 023021. https://doi.org/10.1088/1367-2630/abd7bc

Nagy, M., & Akl, S. G. (2007). Quantum computing: Beyond the limits of conventional computation. *The International Journal of Parallel, Emergent and Distributed Systems, 22*(2), 123–135. https://doi.org/10.1080/13547500600899209

National Quantum Computing Centre. (2023, March). *National quantum strategy*. https://www.nqcc.ac.uk/about-us/national-quantum-strategy/

Newton, N. J. (2012). An infinite-dimensional statistical manifold modelled on Hilbert space. *Journal of Functional Analysis, 263*(6), 1661–1681. https://doi.org/10.1016/j.jfa.2012.06.007

Organisation for Economic Co-operation and Development. (2025). *Mapping the global quantum ecosystem*. https://link.epo.org/web/publications/studies/en-mapping-the-global-quantum-ecosystem.pdf?utm_source=chatgpt.com

Prasad, Y. J. D. S. (2026). Optimizing fault-tolerant quantum circuits through unified T-gate resource reduction. arXiv. https://www.academia.edu/145709104/Optimizing_Fault_Tolerant_Quantum_Circuits_through_Unified_T_Gate_Resource_Reduction

Quantum Computing Report. (2025). *Malaysia establishes first national quantum technology center with Korean company SDT*. https://quantumcomputingreport.com/malaysia-establishes-first-national-quantum-technology-center-with-korean-company-sdt/

Ramaiah, A. K. (2015). Competition law and exemption policy in Malaysia: When, why and why not. *International Journal of Business, Economics and Law, 8*(4), 80–87. https://ijbel.com/wp-content/uploads/2016/01/law-29.pdf

Root, R. H., Jarnagin, J. R., & Provo Ii, M. L. (2025). *Shielding the quantum realm: Technical considerations for maintaining a stable and secure radio frequency environment for quantum research* (Technical Report). U.S. Department of Energy Office of Scientific and Technical Information. https://doi.org/10.2172/2575287

Saklakov, D. (2025). Microgravity and near-absolute zero: A new frontier in quantum computing hardware. arXiv. https://doi.org/10.48550/arXiv.2512.11091

Scherer, M. U. (2016). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology, 29*(2), 353–400. https://dx.doi.org/10.2139/ssrn.2609777

Schmid, L., Locher, D. F., Rispler, M., Blatt, S., Zeiher, J., Muller, M., & Wille, R. (2024). Computational capabilities and compiler development for neutral atom quantum processors—Connecting tool developers and hardware experts. *Quantum Science and Technology, 9*(3), Article 033001. https://doi.org/10.1088/2058-9565/ad33ac

Scholten, T. L., Williams, C. J., Moody, D., Mosca, M., Hurley, W., Zeng, W. J., Troyer, M., & Gambetta, J. M. (2024). *Assessing the benefits and risks of quantum computers*. arXiv. https://doi.org/10.48550/arXiv.2401.16317

Shahshahani, S. (2025). Against the abstract-ideas exclusion. *Berkeley Technology Law Journal, 40*, 447–518. https://doi.org/10.15779/Z38XD0R04T

Shrivastava, P., Soni, K. K., & Rasool, A. (2019). Evolution of quantum computing based on Grover's search algorithm. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICCCNT45670.2019.8944676

Singh, H. (2024). Managing the quantum cybersecurity threat. In M. Hammoudeh, A. T. Alessa, A. M. Sherbeeni, C. M. Firth, & A. S. Alessa (Eds.), *Quantum computing* (pp. 142–158). CRC Press. https://doi.org/10.1201/9781003475286-9

Singh, S., & Sakk, E. (2024). *Implementation and analysis of Shor's algorithm to break RSA cryptosystem security*. TechRxiv. https://doi.org/10.36227/techrxiv.170259160.05374043/v2

Todt, O., & Lujan, J. L. (2014). Analyzing precautionary regulation: Do precaution, science, and innovation go together? *Risk Analysis, 34*(12), 2163–2173. https://doi.org/10.1111/risa.12246

Tripathi, A., Tiwari, G., & Gupta, V. (2025). Comparative analysis of quantum programming environments in India: Insights for usability and adoption in India. *International Journal of All Research Education & Scientific Methods, 13*(2), 501–515. https://www.ijaresm.com/uploaded_files/document_file/Dr._Anuj_Tripathi_ju4L.pdf

Wang, H. F., Wen, J. J., Zhu, A. D., Zhang, S., & Yeon, K.-H. (2013). Deterministic CNOT gate and entanglement swapping for photonic qubits using a quantum-dot spin in a double-sided optical microcavity. *Physics Letters A, 377*(40), 2870–2876. https://doi.org/10.1016/j.physleta.2013.09.005

Wong, H. Y. (2022). *Introduction to quantum computing: From a layperson to a programmer in 30 steps*. Springer. https://doi.org/10.1007/978-3-030-98339-0_17