European Journal of Risk Regulation (2025), 1–20
doi:10.1017/err.2025.8

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap

Kasim Balarabe

Jindal Global Law School, O P Jindal Global University, Sonipat, Haryana, India
Email: kbalarabe@jgu.edu.in

Abstract

The rapid advancement of quantum computing presents unparalleled opportunities and challenges for the legal field. This article investigates the key legal implications of quantum computing, focusing on intellectual property, data security, regulation, and ethical considerations. The unique characteristics of quantum algorithms and hardware pose significant challenges for the existing patent system, necessitating a clear and consistent framework for protecting quantum innovations while fostering collaboration. The threat of quantum computing to current encryption methods highlights the urgent need for forward-looking data protection policies and the adoption of post-quantum cryptography. As quantum technologies continue to evolve, policymakers must work closely with stakeholders to develop adaptive, principles-based regulations that strike a balance between promoting innovation and mitigating risks. Moreover, the societal and ethical impacts of quantum computing cannot be overlooked; prioritising applications that deliver significant social good and establishing robust ethical guidelines will be crucial. Preparing the legal workforce for the quantum era requires a concerted effort to develop quantum literacy and expertise. By adopting a proactive, interdisciplinary approach, the legal community can play a vital role in shaping the quantum future, ensuring that this transformative technology upholds the rule of law, protects individual rights, and promotes the greater good of society.

Keywords: data security; intellectual property; legal implications; Quantum computing

I. Introduction

Quantum computing is a transformative technology that exploits the principles of quantum mechanics to perform certain computations exponentially faster than classical computers.[1] Unlike classical computers that process information using bits that can only be in one of two states (0 or 1), quantum computers harness the properties of quantum bits or qubits, which can exist in multiple states simultaneously through quantum superposition, entanglement and interference.[2] Through leveraging these unique properties of quantum systems, quantum computing can perform computations in fundamentally different ways than classical computers. These quantum phenomena allow quantum computers to search and analyse vast computational spaces simultaneously and find solutions to certain problems much faster than the best-known classical algorithms.[3]

[1] J Preskill, "Quantum Computing in the NISQ Era and Beyond" (2018) 2 Quantum 79.

[2] MA Nielsen and IL Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge, Cambridge University Press 2010) p 13.

[3] AW Harrow and A Montanaro, "Quantum Computational Supremacy" (2017) 549(7671) Nature 203.

For example, Shor's algorithm can factor integers in polynomial time, resulting in far-reaching implications for cryptography.[4] Grover's algorithm offers a quadratic speedup for unstructured search problems, enhancing the efficiency of optimisation and machine learning tasks.[5] In addition, quantum computers could be inherently efficient in simulating complicated quantum systems, such as molecules and materials, which would significantly advance other fields, including drug discovery, material science, and quantum chemistry.[6] As quantum hardware scales up and quantum algorithms mature, quantum computing is poised to tackle some of the most challenging computational problems across various domains. This will likely usher in a new era of scientific discovery and technological innovation. This paradigm shift in computing allows quantum computers to tackle complex problems that classical computers simply cannot handle, including factoring large numbers, simulating quantum systems, and optimising complex functions.[7] However, it is important to note that quantum computers are not a universal replacement for classical computers, and their capabilities are still being actively researched and developed.

Quantum algorithms, which are specialised sets of instructions designed to run on quantum computers, play an indispensable role in harnessing the power of quantum computing. These algorithms capitalise on the unique properties of quantum hardware, such as superposition and quantum entanglement, to perform calculations in fundamentally different ways than classical algorithms.[8] The symbiotic bond between quantum hardware and software is essential for implementing quantum algorithms. Quantum hardware, including superconducting qubits and ion traps, provides the physical platform for performing quantum computation, while quantum programming languages and compilers translate abstract quantum algorithms into a sequence of physical operations that can be executed on the hardware.[9]

As quantum hardware continues to enhance in qubit count, connectivity and error rates, more intricate quantum algorithms can be put into action and run on these systems. The evolution of quantum software and programming frameworks, for instance, Qiskit, OpenQASM and Q#, facilitates the creation and optimisation of quantum algorithms for specific hardware architectures.[10] The dynamic interplay between quantum algorithms, software and hardware is pivotal for harnessing the full potential of quantum computing. As research progresses in all three areas, we can expect to see more powerful and efficient quantum computing systems capable of tackling increasingly complex problems across various domains.

Progress in delivering quantum hardware and software has been accelerating, with the likes of Google, IBM and Microsoft racing alongside startups and research bodies to build quantum devices that are scalable and fault-tolerant.[11] Thus, as quantum computing advances and becomes commercially viable, its applications across diverse fields, from

[4] PW Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer" (1997) 26(5) SIAM Journal on Computing 1484.

[5] LK Grover, "A Fast Quantum Mechanical Algorithm for Database Search" (1996) 28th Annual ACM Symposium on the Theory of Computing 212.

[6] Y Cao and Others, "Quantum Chemistry in the Age of Quantum Computing" (2019) 119(19) Chemical Reviews 10856.

[7] A Montanaro, "Quantum Algorithms: An Overview" (2016) 2(1) NPJ Quantum Information 15023.

[8] Nielsen and Chuang, supra, n 2, 20–5.

[9] Cao and others, supra, n 6.

[10] See G Aleksandrowicz and Others, "Qiskit: An Open-source Framework for Quantum Computing" (2019) <https://doi.org/10.5281/zenodo.2562111> (last accessed 31 December 2024).

[11] See S Rosenbush, "The Age of Quantum Software Has Already Started" *The Wall Street Journal* (New York, 19 December 2024) <https://www.wsj.com/articles/the-age-of-quantum-software-has-already-started-854eccfa> (last accessed 28 December 2024).

cryptography, drug discovery, materials science, and optimisation to machine learning, are predicted to grow.[12] However, this disruptive potential also raises significant legal challenges that must be addressed proactively.

One of the most pressing concerns facing modern society is the impact that emerging quantum computing capabilities could have on cryptography and digital security as we know it. Many of the cryptographic methods underpinning much of today's encrypted communications and transactions, such as RSA and elliptic curve cryptography, rely on mathematical problems like prime factoring and discrete logarithms that are considered intractable for classical computers.[13] However, Peter Shor's landmark quantum algorithm from 1994 demonstrates how a sufficiently powerful quantum system could potentially solve these problems with ease, jeopardising confidential data that relies on these conventional encryption techniques for protection.[14] This necessitates the development and deployment of quantum-resistant or post-quantum cryptography to protect sensitive data from potential quantum attacks.[15]

Another major legal issue relates to the intellectual property (IP) environment for quantum technologies. Quantum algorithms and hardware come with many unique features that strain the existing patent system, which was tailored to classical technologies. The evaluation of quantum inventions in terms of novelty, non-obviousness and enablement requires a clear and consistent framework that aligns with the quantum paradigm.[16] At the same time, the pace of innovation in the field could incentivise many to file patent applications, which might lead to overlapping and contradictory claims that could hinder innovation and collaboration.

The regulatory framework for quantum technologies is in its infancy, and jurisdictions are addressing this issue in a variety of ways based on national interests or capabilities. Some regions, such as the United States and China, have already initiated targeted initiatives and strategies to support quantum research and development, and formal regulatory frameworks that address the specific risks and challenges posed by quantum technologies are yet to be developed.[17] Law and policymakers must collaborate closely with stakeholders from industry, academia and civil society to develop adaptive principles-based regulations that strike a balance between promoting innovation and mitigating potential harms. A typical example here could be that policymakers should work with quantum technology companies and research institutions to establish clear guidelines and best practices for the secure development and deployment of quantum computing systems. This could include setting standards for post-quantum cryptography, quantum key distribution, and quantum-safe communication protocols to ensure the integrity and confidentiality of sensitive data. Again, a proactive and anticipatory approach to governance, the type that takes into consideration the potential long-term impacts of quantum technologies and, therefore, seeks to steer their development in socially desirable directions, is important. Responsible innovation frameworks, which

[12] Cao and others, supra, n 6.

[13] DJ Bernstein and T Lange, "Post-Quantum Cryptography" (2017) 549(7671) Nature 188.

[14] PW Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring" (1994) Proceedings 35th Annual Symposium on Foundations of Computer Science 124.

[15] National Institute of Standards and Technology, "Post-Quantum Cryptography" (*NIST Computer Security Resource Center*, 2017) <https://csrc.nist.gov/projects/post-quantum-cryptography> (last accessed 28 December 2024).

[16] M Kop, M Aboy and T Minssen, "Intellectual Property in Quantum Computing and Market Power: A Theoretical Discussion and Empirical Analysis" (2022) 17(8) Journal of Intellectual Property Law & Practice 613.

[17] Veritx, "The Race for Quantum Supremacy: A Comparative Analysis of Quantum Computing Development in the US and China" (*Veritx*, 5 June 2024) <https://www.veritx.com/the-race-for-quantum-supremacy-a-comparative-analysis-of-quantum-computing-development-in-the-us-and-china> (last accessed 28 December 2024).

emphasise the importance of addressing ethical and societal concerns throughout the research and development process, can also provide valuable guidance in this regard.

In addition to the above-mentioned challenges, the ethical implications of quantum computing cannot be overlooked. As the systems become more powerful, their applications may have some profound societal impacts, such as exacerbating inequalities, enabling mass surveillance, or automating decision-making processes.[18] In this context, prioritising the development of quantum applications that deliver significant social benefits and establishing robust ethical guidelines for the responsible use of quantum technologies, it is opined here, will be crucial to ensure that their benefits are distributed equitably and their potential risks are mitigated. The ethical considerations surrounding quantum computing are closely intertwined with its legal implications. As quantum technologies become more powerful and pervasive, they raise fundamental questions about fairness, accountability, transparency and privacy. These ethical concerns, in turn, shape the legal landscape, informing the development of regulations, guidelines, and standards that seek to promote the responsible development and deployment of quantum computing. By exploring the ethical dimensions of quantum technologies alongside their legal implications, this article aims to provide a more comprehensive and nuanced understanding of the challenges and opportunities presented by this transformative field.

Given the pace of advancements in quantum computing and its far-reaching implications, legal professionals must actively engage with this emerging technology. The aim of this article is to provide a modest analysis of the key legal challenges and opportunities presented by quantum computing. Essentially, it focuses on four critical areas: intellectual property, data security, regulation and ethical considerations. The article adopts an interdisciplinary approach by drawing insights from law, policy, technology and ethics. By doing this, the article seeks to contribute to the growing discourse on the legal dimensions of quantum computing. It also proposes recommendations for navigating this complex landscape.

The article is structured as follows: Section 2 provides an overview of the technical foundations of quantum computing by explaining its basic principles, comparing it with classical computing, as well as highlighting its potential advantages. Section 3 examines the intellectual property challenges associated with patenting quantum algorithms and technologies and discusses the implications for IP law and policy. Section 4 analyses the threat of quantum computing to current encryption methods and explores legal protections for data security in the quantum era. Section 5 reviews the current state of quantum technology regulation across different jurisdictions and offers recommendations for future regulatory frameworks. Section 6 delves into the societal and ethical impacts of quantum computing and discusses strategies for balancing its benefits and risks. Section 7 reflects on the long-term implications of quantum computing for the legal field and emphasises the need for the legal community to prepare for the quantum era. Section 8 provides conclusions.

II. Technical foundations

In order to effectively navigate the evolving legal landscape of quantum computing, legal actors require a firm understanding of the fundamental principles that guide quantum computing. In this part, I provide a brief outline of the core quantum concepts suited for a legal audience, the main differences between quantum and classical computing, and the possible features of quantum systems that offer competitive advantages over their classical counterparts.

[18] PE Vermaas, "The Societal Impact of the Emerging Quantum Technologies: A Renewed Urgency to Make Quantum Theory Understandable" (2017) 19(4) Ethics and Information Technology 241.

1. Basic principles of quantum computing

The quantum computer stems from the quantum bit (known as the qubit), which is the fundamental unit of information within a quantum computer.[19] The qubit has similarities with the bit, which is the foundational unit of state in a classical computer, yet it is much different. Unlike classical bits, which can only exist in one of two states (0 or 1), qubits can simultaneously exist in a superposition of multiple states.[20] This property allows quantum computers to perform certain computations exponentially faster than classical computers by exploiting the principles of quantum mechanics.

Another important concept of quantum computing is quantum entanglement or simply entanglement. Entanglement between two or more qubits involves correlated states of two particles that remain interdependent, even when their quantum states are separated by an arbitrarily large distance.[21] Entanglement facilitates computing by allowing quantum computers to process information in ways that are fundamentally distinct from classical computers. It also results in new algorithms and paradigms of computation that simply would not exist on classical computers.[22]

Quantum computers use quantum interference too – that is, they "interfere" with the quantum state in a way that amplifies the desired outcome and suppresses the unwanted one.[23] Quantum interference between multiple interdependent quantum states makes quantum computers able to process information following rules that differ from classical computers, leading to the development of new types of algorithms and computation mechanisms. Additionally, quantum computing is based on quantum interference, which allows quantum states to undergo constructive or destructive interference. By adjusting quantum states' phases, quantum algorithms amplify the desired outcomes and weaken the undesired ones, providing a massive speedup for particular computational tasks.[24]

2. Comparison with classical computing

Classical computers have been the dominant form of computing for decades. They work by acting upon bits of binary data, which can only be in the state of 0 or 1 at once. This calculation-performing method is processed by applying subsequent logical operations to the bits. This operation is carried out over a fixed number of steps, known as an algorithm. Quantum computers achieve their calculative power using the principles of quantum mechanics. The superposition of a qubit allows quantum computers to perform calculations on an exponential number at once, a property known as quantum parallelism.[25] This allows quantum computers to perform certain calculations much faster, mainly those related to searching and factoring large numbers.[26]

Another key difference between classical and quantum computing lies in the way information is processed. Classical computers rely on deterministic algorithms, which always produce the same output for a given input. Quantum computers, on the other hand, can employ probabilistic algorithms, which may produce different outputs with certain

[19] Nielsen and Chuang, supra n 2, 13.

[20] Ibid.

[21] See R Horodecki and Others, "Quantum Entanglement" (2009) 81(2) Reviews of Modern Physics 865.

[22] Preskill, supra, n 1.

[23] R Cleve and Others, "Quantum Algorithms Revisited" (1997) 454 Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences 1.

[24] Shor, supra n 4, p 1495.

[25] D Deutsch and R Jozsa, "Rapid Solution of Problems by Quantum Computation" (1992) 439(1907) Proceedings of the Royal Society of London Series A: Mathematical and Physical Sciences 553.

[26] Montanaro, supra n 7.

probabilities.[27] This probabilistic nature of quantum computing can be harnessed to solve problems that are intractable for classical computers, such as simulating complex quantum systems or optimising complex functions.

3. Potential advantages of quantum computing

Among other things, quantum computing possesses several potential advantages over classical computing, which make it highly attractive to certain domains where classical algorithms increasingly struggle to handle larger and more complex problems. Perhaps the most notorious of these is the domain of cryptography. Quantum computers are believed to be capable of breaking many of the existing public-key encryption schemes, including those based on RSA and elliptic curve cryptography.[28] This has significant implications for the security of digital communications and transactions, necessitating the development of post-quantum cryptographic algorithms that can withstand attacks by quantum computers.

Another domain where quantum computing might be beneficial is optimisation. This branch of computer science aims to discover the best solution out of many plausible solutions. Quantum approximating algorithms like the Quantum Approximate Optimization Algorithm and the quantum adiabatic algorithm are believed to hold potential for outcompeting classical optimisation methods in fields such as logistics, finance, or resource allocation.[29]

Another promising area is the simulation of complex quantum systems, such as molecules and materials.[30] Since such systems behave in a distinctly quantum way, using quantum computer technology could help to accurately simulate, for instance, chemical reactions, discover new materials with ideal properties and create drugs and catalysts more efficiently. This will impact various sectors, from pharmaceuticals and materials science to energy and the environment.

Given the rapid growth of the quantum technology business, it is critical that legal experts are abreast of the technology's underlying principles and associated risks and opportunities. By becoming familiar with the quantum computing principles and implications of quantum vs. traditional computing, legal professionals may be better prepared to address quantum's expanding involvement in various social and economic activities.

III. Intellectual property

The rapid development of quantum computing has created a new intellectual property (IP) frontier. The acquisition and commercialisation of quantum technologies have highlighted the general difficulty of patenting quantum algorithms and hardware. In this part, I investigate the unique challenges in patenting quantum algorithms and technologies and also discuss the implications for IP law and policy.

1. Challenges in patenting quantum algorithms and technologies

Unlike patent claims to classical computing inventions, patent claims to quantum algorithms and technologies present certain challenges. The main challenge is related to

[27] See Y Huang and S Pang, "Optimization of a Probabilistic Quantum Search Algorithm with a Priori Information" (2023) 108(2) Physical Review A 022417.

[28] Bernstein and Lange, supra n 13, 188.

[29] See N Moll and others, "Quantum Optimization Using Variational Algorithms on Near-term Quantum Devices" (2018) 3(3) Quantum Science and Technology 030503.

[30] Cao and others, supra n 6.

the distinctive difficulty of defining and claiming quantum inventions in a way that meets the minimum requirements of novelty, non-obviousness and enablement.[31]

Quantum algorithms are a form of computation that employs quantum mechanics for their design and implementation. It is complicated to describe the result of the execution of quantum algorithms, and they are based on the creation and management of complex quantum states. There is no accepted language and notation to record quantum algorithms. Consequently, the language used to patent quantum algorithms may be vague and non-uniform, and therefore, the novelty and non-obviousness of the formulations to an examiner may be tough to decide.[32]

Furthermore, quantum computing is still in its early stages, and most of the underlying principles and techniques are extensions of the well-known laws of quantum mechanics. This leads to another pressing issue of the patentability of quantum algorithms and technologies – specifically, whether they are eligible for patent protection, as they may be characterised as 'laws of nature' or 'abstract ideas'.[33]

Another problem with patenting quantum technologies is the issue of demonstrating useful applications and commercial viability.[34] Most quantum algorithms and other quantum computing technologies are still in the theoretical stage or proven only in the laboratory based on a small scale, making it difficult to provide evidence for a credible and real-world useful application to patent offices.

2. *Implications for intellectual property law and policy*

Overall, the challenges and uncertainties associated with patenting quantum algorithms and technologies have broad implications for IP law and policy. The rapid growth and maturation of the quantum computing industry will force policymakers and legal experts to consider how existing IP frameworks should be adjusted to take into account the unique characteristics of quantum inventions.

One of the major concerns will be the trade-off between encouraging the creation of new knowledge through IP protection and encouraging its diffusion. Indeed, while patents may offer a strong incentive for companies and researchers to invest in the development of quantum technologies by granting them a temporary monopoly over their commercialisation,[35] extensive and restrictive patents can also impede further innovation by blockading the fields from new entrants and preventing researchers from building on one another's work.[36]

To address these concerns, policymakers may consider the need for targeted reform of patent laws and examination processes to align them with the unique challenges posed by quantum inventions. Possible reforms might involve creating a standard quantum algorithm and hardware description language, developing guidelines for examining patent

[31] Intepat, "Navigating Intellectual Property in The Era of Quantum Computing" (*Intepat*, 2 May 2024) <https://www.intepat.com/blog/navigating-intellectual-property-in-the-era-of-quantum-computing/> (last accessed 21 May 2024).

[32] See MK Henry, "Alice in Quantum Land: Is Your Quantum Computing Invention Patent-Eligible?" (*Henry Patent Law Firm*, 5 July 2023) <https://henry.law/blog/alice-in-quantum-land-is-your-quantum-computing-invention-patent-eligible/> (last accessed 21 May 2024).

[33] Congressional Research Service, "Patent-Eligible Subject Matter Reform: An Overview" (*United States Congress*, 3 January 2024) <https://crsreports.congress.gov/product/pdf/IF/IF12563/1#:~:text=URL%3A%20https%3A%2F%2Fcrsreports.congress.gov%2Fproduct%2Fpdf%2FIF%2FIF12563%2F1%0AVisible%3A%200%25%20> (last accessed 21 May 2024).

[34] Preskill, supra, n 1, 1.

[35] W Fisher, "Theories of Intellectual Property" in SR Munzer (ed), *New Essays in the Legal and Political Theory of Property* (Cambridge, Cambridge University Press) 168.

[36] See MA Heller and RS Eisenberg, "Can Patents Deter Innovation? The Anticommons in Biomedical Research" (1998) 280(5364) Science 698. See also Kop, Aboy and Minssen, supra, n 16, 625–7.

eligibility of quantum inventions and establishing dedicated patent examination units with the necessary expertise.[37]

Another relevant consideration is the effect quantum computing patents can have on the access and affordability of quantum technologies. Given the increasing importance of quantum computing in various applications ranging from drug discovery and material science to cryptography and finance, ensuring their widespread use and affordability will be vital to promoting innovation and social welfare.[38] Policymakers may need to explore additional IP models, such as patent pools, cross-licensing deals and open-source initiatives, to enable quantum computing knowledge and technologies to be shared with as many researchers and companies as possible.[39] This can help alleviate the patent buckle risks and licensing barriers while ensuring enough incentive for invention and commercialisation.

Finally, the quantum computing industry is highly global in nature, posing challenges to the development of coherent and coordinated IP policies. Due to the growing importance of quantum technologies for national security and economic success, different countries will attempt to protect their burgeoning quantum industries through trade secret laws, export restrictions, and other mechanisms.[40] This problem risks undermining international collaboration and knowledge-sharing at the core of the quantum computing industry, but it could be used to facilitate progress split through the restrictions of trade secrets. Therefore, policymakers and jurists must develop a common framework for quantum IP law whose ambitions are proportional to its constraints. Policymakers can achieve this through the creation of international norms and dispute resolutions regarding quantum IP, adapting to the developing technology, and evolving disputes surrounding it.

IV. Data security

The emergence of quantum computing is a major technological breakthrough, but it also poses a significant threat to the security of digital technologies. The issue of the growing computing power of quantum computers becoming an imminent threat to our current encryption systems has many facets and creates several complex problems. This section describes the potential impact of quantum computing on data security; it also proposes a list of proper regulatory and legal measures for protecting data in the quantum era.

[37] See Kop, Aboy and Minssen, supra, n 16, 628. See also F Qiu, "Patent Landscape for Quantum Computing: A Survey of Patenting Activities for Different Physical Realization Methods" (*IP Watch Dog*, 13 February 2024) <https://ipwatchdog.com/2024/02/13/patent-landscape-quantum-computing-survey-patenting-activities-different-physical-realization-methods/id=173303/#> (last accessed 21 May 2024).

[38] Vermaas, supra, n 18, 244.

[39] See for example B Verbeure, "Patent Pools" in G van Overwalle (ed), *Gene Patents and Collaborative Licensing Models: Patent Pools, Clearinghouses, Open Source Models and Liability Regimes* (Cambridge Intellectual Property and Information Law, Cambridge University Press 2009) 3, 5; E van Zimmeren, "Clearinghouses" in G van Overwalle (ed), *Gene Patents and Collaborative Licensing Models: Patent Pools, Clearinghouses, Open Source Models and Liability Regimes* (Cambridge Intellectual Property and Information Law, Cambridge University Press 2009) 63, 69.

[40] See FBI, "Protecting Quantum Science and Technology" (*US Federal Bureau of Investigation*, 12 April 2024) <https://www.fbi.gov/news/stories/protecting-quantum-science-and-technology> (last accessed 21 May 2021); WA Reinsch, T Denamiel and M Schleich, "Optimizing U.S. Export Controls for Critical and Emerging Technologies: Working with Partners" (February 2024) Center for Strategic & International Studies <https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-02/240214_Reinsch_Export_Controls.pdf?VersionId=T3Gx0p4LNWRyYrNwWqhr.xM4WHRreDuY> (last accessed 20 May 2024); and M Swayne, "France Advances Quantum Technology Export Controls Under New EU Regulation Framework" (*The Quantum Insider*, 26 February 2024) <https://thequantuminsider.com/2024/02/26/france-advances-quantum-technology-export-controls-under-new-eu-regulation-framework/> (last accessed 18 May 2024).

1. Quantum computing's threat to current encryption methods

The security of modern digital communications and transactions depends on public-key cryptography, which uses mathematical algorithms to encode and decode sensitive information.[41] The most widely used public-key cryptographic algorithms (based on the RSA number-theory algorithm, elliptic curve cryptography or ECC, and others working in a similar way) are considered secure because there is no known algorithm that allows for efficient solutions to the underlying mathematical problem: the difficulty of factoring large numbers, or the inability to compute their so-called discrete logarithms.[42] These problems are deemed intractable for a classical computer, meaning it would still take a prohibitively long time to factor any large number or compute its discrete logarithm using the most advanced supercomputers available even today.[43]

However, quantum computing changes the situation and threatens the security of most modern encryption methods. For example, in 1994, Peter Shor formulated the quantum algorithm that allows for solving integer factorisation and discrete logarithm problems on a quantum computer efficiently.[44] The quantum mechanics phenomena of superposition and entanglement exploited during the vast quantum superposition and entanglement processes on quantum computers make it feasible to calculate something that is impossible to compute on classical computers.[45]

We do not currently have large-scale, fault-tolerant quantum computers capable of running Shor's algorithm, but experts predict we may get to that point in a decade or two.[46] If such quantum computers were developed, their impact on the security of our digital systems would be devastating. They could leverage Shor's algorithm to break the encryption that protects data transferred or stored in digital systems, from financial transactions to medical records to government secrets.[47] However, the danger of quantum computing is not limited to the immediate threat of a data breach. In fact, the forward secrecy of encrypted messages can also be compromised, meaning that once data is encrypted and saved, it can be later decrypted using the power of a quantum computer.[48] This fact poses a problem for data that should be kept secure in the long term, as data that is safe from attacks when encrypted today maybe later decrypted in the quantum era.

Research and industry are currently working to develop post-quantum cryptography (PQC).[49] PQC is resistant to quantum attacks while retaining the desirable properties of existing cryptographic systems. The most prominent PQC systems include lattice-based cryptography and hash-based signatures, both of which rely on problems that are hard for

[41] W Stallings, *Cryptography and Network Security: Principles and Practice* (7th Ed edn, Pearson Education Limited 2017) pp 291–2; J Buchmann, K Lauter and M Mosca, "Postquantum Cryptography – State of the Art" (2017) 15(4) IEEE Security & Privacy 12; M Mosca and J Mulholland, "A Methodology for Quantum Risk Assessment" (2017) <https://globalriskinstitute.org/publication/a-methodology-for-quantum-risk-assessment/> (last accessed 17 May 2024).

[42] RL Rivest, A Shamir and L Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems" (1978) 21(2) Commun ACM 120.

[43] F Arute and Others, "Quantum Supremacy Using a Programmable Superconducting Processor" (2019) 574(7779) Nature 505.

[44] PW Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer (1999) 41(2) SIAM Review 303.

[45] Nielsen and Chuang, supra, n 2, 6–7.

[46] M Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" (2018) 16(5) IEEE Security & Privacy 38.

[47] See National Academies of Sciences Engineering and Medicine, *Quantum Computing: Progress and Prospects* (Washington, DC, The National Academies Press 2018) Chapter 4.

[48] Buchmann, Lauter and Mosca, supra, n 51, 12–13.

[49] See Bernstein and Lange, supra, n 13.

classical and quantum computers to solve.[50] Switching to post-quantum cryptography is complex and would require several years of work to replace the current cryptographic systems.[51]

2. *Legal protections for data security in the quantum era*

With the increasing threat of quantum computing to data security, it is vital that legal frameworks and regulations are updated and adapted to safeguard sensitive information in the quantum era. While current laws, such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act, set out certain basic requirements for appropriate and secure processing and storage of personal data,[52] these laws do not sufficiently address the challenges specific to the threat of quantum computing. In order to adequately protect data as the threat of quantum computing closes, policymakers and regulators must closely cooperate with experts in the field and industry experts to craft appropriate standards, guidelines and other measures. These can include requirements for the use of post-quantum cryptographic measures within a certain industry, guidelines on liability and reporting of quantum-related security breaches, and possibly some incentive structures to promote the use of quantum-resistant security measures.[53]

A key concern is that we might need forward-looking data protection policies that take account of the long-term security threats posed by quantum computing: organisations might have to do a quantum-readiness health check and have a plan to move away from quantum-vulnerable cryptography to post-quantum alternatives.[54] Data protection policies might need to be adapted to minimise the volumes of data stored that a future quantum attack might compromise.

Another key aspect of legal protections for data security in the quantum era is in the area of international cooperation and the development of standards and norms for quantum-resistant data security. Over time, as quantum computing capabilities mature, countries will likely have to work together to develop a coherent international, global approach to quantum-resistant cryptography and data security. This might include coordination and harmonisation of national laws and regulatory measures, sharing best practices and technical knowledge, and international norm-setting for quantum-related security incidents.

V. Regulatory landscape

The rapid development of quantum technology has provided unprecedented opportunities for innovation to the global economy but also has brought an array of new risks. With quantum computing, quantum communication, and quantum sensing technologies

[50] A Gorjan and Others, *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process* (NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD 2019).

[51] M Mosca and J Mulholland, "A Methodology for Quantum Risk Assessment" (2017) <https://globalriskinstitute.org/publication/a-methodology-for-quantum-risk-assessment/> (last accessed 17 May 2024).

[52] S Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model" (2018) 10(2) Law, Innovation and Technology 266, 268.

[53] See W Barker, W Polk and M Souppaya, "Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms" (28 April 2021) National Institute of Standards and Technology <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf> (last accessed 17 May 2024).

[54] E Chiu, "Preparing Enterprises for the Quantum Computing Cybersecurity Threats" (2019) Cloud Security Alliance <https://naavi.org/uploads_wp/2020/quantum_computing_threats.pdf> (last accessed 22 May 2024).

continuing to mature, it is important to understand the current quantum technology regulatory landscape, analyse and compare different regulatory practices across major jurisdictions, and suggest the direction for future regulations that will enable innovation and mitigate resulting risks.

1. Current state of quantum technology regulation

At the moment, the regulation of quantum technologies is in its infancy. However, upon realising the revolutionary potential of quantum technologies, numerous governments and intergovernmental organisations appreciated their potential dangers, particularly in the realm of security and privacy. Notwithstanding, formal regulatory regimes that respond to the specific challenges raised by quantum technologies are yet to be developed.

Certain aspects of quantum technologies may be regulated by existing legislation, particularly in the fields of cybersecurity, data protection, and intellectual property rights. For example, the procedures for quantum-generated and quantum-processed data may fall into the legal requirements of the European Union's General Data Protection Regulation and California Consumer Privacy Act, as well as other relevant laws on privacy and data processing in other jurisdictions.[55] Furthermore, patent laws and intellectual property rights protect inventories in quantum technologies, including quantum algorithms and quantum hardware components.[56] However, the current regulatory framework is likely to be insufficient to address the specific challenges of quantum technologies. These include quantum computers' ability to compromise existing encryption standards and the need for quantum-proof security measures to secure quantum-sensitive information. In addition, the global and interdisciplinary nature of quantum research and development presents additional challenges for regulators, as it requires coordination and cooperation across borders and among various stakeholders, including governments, industry, academia, and civil society.[57] Despite the nascent stage of quantum technology regulation, various international organisations (such as the World Economic Forum and OECD) and governments (such as the United States, United Kingdom, Germany and Japan) have initiated efforts to address the governance challenges posed by these emerging technologies.

2. Comparative analysis of regulatory approaches across jurisdictions

To date, regulatory approaches to quantum technologies have been diverse across jurisdictions, reflecting differences in national priorities, levels of technological capability and policy frameworks. Some nations have played leading roles in developing targeted policies and initiatives to underpin the responsible development and governance of quantum technologies, while others have been more hesitant or adaptive in their approaches.

In the United States, the National Quantum Initiative Act, which was signed into law in 2018, created a nationally coordinated programme to accelerate quantum research and development. This law emphasised public–private partnerships and the development of a qualified quantum workforce.[58] It also required the development of a national strategic

[55] See S Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model" (2018) 10(2) Law, Innovation and Technology 266.

[56] See P Singh, "Role of Intellectual Property Rights in the Era of Quantum Technology" (*IIPRD*, 23 November 2022) <https://www.iiprd.com/role-of-intellectual-property-rights-in-the-era-of-quantum-technology/> (last accessed 22 May 2024).

[57] See National Quantum Coordination Office, "National Quantum Initiative: The Federal Source and Gateway to Quantum R&D Across the US Government" (*National Quantum Coordination Office*) <https://www.quantum.gov/> (last accessed 22 May 2024).

[58] National Quantum Initiative Act, H.R.6227, 115th Cong (2018).

plan to direct the federal government's quantum technology investments, including consideration of ethical, legal, and societal implications.[59]

On the European level, the European Union has also recognised the strategic importance of quantum technologies and launched several initiatives to support their development and regulation. The €1 billion EU Quantum Flagship – a research and innovation initiative launched in 2018 to consolidate and expand European scientific leadership and excellence in this field – also explicitly addresses quantum technologies' societal and ethical implications.[60] The European Commission has also called for a coordinated approach to quantum regulation and the development of the European Quantum Policy, which would ensure a coherent framework for the development, deployment, and governance of quantum technologies within the European Union.[61] However, the European Commission has indicated that new legislative proposals specific to quantum technologies are not expected before the end of the current mandate.[62]

Compared to the United States, China's pursuit of quantum technology is more state-led, with substantial injections of government funds and a coordinated effort among the public and private sectors. The Chinese government has recognised quantum technology as a national priority and has invested heavily in research and development, with a focus on making real and substantial breakthroughs by 2030. These efforts have culminated in a National Quantum Program and investments totalling $15.3 billion as of 2022, more than the European Union and the United States put together.[63] The government has also implemented educational measures, with the most notable being the Education Modernisation 2035 Plan to focus more on the quantum sector.[64] Furthermore, the country has put forward a loose regulatory framework for quantum technology. The government's priority is to make as many quantum technological advancements as possible rapidly and then implement regulation measures for its security.

Other countries, such as Canada, Australia, and Japan, have also launched national initiatives and strategies to support the development of quantum technologies, with varying degrees of emphasis on regulatory considerations.[65]

[59] Ibid.

[60] European Commission, "Quantum Technologies Flagship" (*European Commission*, 19 December 2023) <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship> (last accessed 22 May 2024).

[61] European Commission, "A European Strategy for Data" (*European Union* 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066> (last accessed 21 May 2024).

[62] J Keane, "Is Quantum Computing the Next Technology on the EU's Regulation Agenda?" (*EuroNews*, 30 January 2024) <https://www.euronews.com/next/2024/01/30/is-quantum-computing-the-next-technology-on-the-eus-regulation-agenda> (last accessed 22 May 2024).

[63] B Hart and Others, "Is China a Leader in Quantum Technologies?" (*China Power*, 14 August 2023) <https://chinapower.csis.org/china-quantum-technology/> accessed 18 May 2024; EB Kania, "China's Quantum Future: Xi's Quest to Build a High-Tech Superpower" *Foreign Affairs* <https://www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future> (last accessed 16 May 2024).

[64] JP, "Chinese Quantum Companies and National Strategy 2023" (*The Quantum Insider*, 13 April 2023) <https://thequantuminsider.com/2023/04/13/chinese-quantum-companies-and-national-strategy-2023/> (last accessed 16 May 2024).

[65] Government of Canada, "Engagement paper: Developing a National Quantum Strategy" (*Government of Canada*, 16 July 2021) <https://ised-isde.canada.ca/site/national-quantum-strategy/en/engagement-paper-developing-national-quantum-strategy> (last accessed 22 May 2024); G Williams and M Bick, "Growing Australia's Quantum Technology Industry" (*CSIRO*, 12 October 2022) <https://www.csiro.au/en/work-with-us/services/consultancy-strategic-advice-services/csiro-futures/future-industries/quantum> (last accessed 18 May 2024); Y Yamamoto, M Sasaki and H Takesue, "Quantum Information Science and Technology in Japan" (2019) 4(2) Quantum Science and Technology 020502.

3. Governance frameworks and the international year of quantum

The United Nations General Assembly declaring 2025 to be the International Year of Quantum Science and Technology (IYoQST) is a manifestation of an increasing acknowledgement of the transformative power of quantum technologies and their governance requirements in an era of growing hype around a quantum revolution.[66] This resolution, adopted on 7 June 2024, sets the stage for a global, multi-stakeholder effort to harness the power of quantum science and technology for sustainable development while addressing the challenges and risks associated with these emerging technologies. The IYoQST resolution emphasises the vital role of quantum science and technology in driving economic advancement and addressing pressing global challenges, such as food security, health, sustainable cities, clean water and energy, and climate action.[67] However, the resolution also acknowledges the need to collectively address the challenges posed by quantum technologies by highlighting the importance of international cooperation, public awareness, and education in this particular field.[68]

Promoting international, multilateral, and interdisciplinary scientific cooperation among research institutions, researchers, and innovators in quantum science and technology is among the key aims of the IYoQST.[69] Such a collaborative effort is necessary for developing governance frameworks that match the pace of quantum technology and meet societal values and priorities.[70] The resolution also highlights the need for providing broad access to science, technology, engineering and mathematics (STEM) education and research for all, in particular the youth, girls and women, particularly in developing countries.[71] This focus on the inclusive and diverse quantum workforce is critical so that the benefits of quantum technologies are equitable and that governance frameworks embody a diverse set of perspectives and interests.[72]

To operationalise the IYoQST goals, the resolution calls on the United Nations Educational, Scientific and Cultural Organization (UNESCO) to be the leading agency and contact point for the IYoQST.[73] This designation reflects the important role that international organisations play in fostering multi-stakeholder cooperation and creating global norms and standards for the governing of quantum technologies.[74]

The IYoQST resolution lays the groundwork for developing adaptive, anticipatory and responsive governance frameworks for quantum technologies. These frameworks should be grounded in the principles of responsible research and innovation (RRI), which emphasise the importance of anticipating and mitigating potential risks and negative consequences while ensuring that the development and deployment of quantum technologies align with societal values and priorities.[75] To effectively implement RRI principles in the context of quantum technologies, governance frameworks should

[66] United Nations General Assembly, *International Year of Quantum Science and Technology, 2025* (Resolution 78/287, 7 June 2024) UN Doc A/RES/78/287.

[67] Ibid., preamble.

[68] Ibid., preamble and operative para 3.

[69] Ibid., operative para 3.

[70] J Stilgoe, R Owen and P Macnaghten, "Developing a Framework for Responsible Innovation" (2013) 42(9) Research Policy 1568.

[71] United Nations General Assembly, supra, n 67, preamble.

[72] U Gasser, R Budish and S West, "Multistakeholder as Governance Groups: Observations from Case Studies" (2015) Berkman Center Research Publication No 2015-1

[73] United Nations General Assembly, supra, n 76, operative para 2.

[74] G Marchant and W Wallach, "Governing the Governance of Emerging Technologies" in GE Marchant, KW Abbott and B Allenby (eds), *Innovative Governance Models for Emerging Technologies* (Cheltenham and Northarmton, Edward Elgar 2013) p 141.

[75] European Commission, Directorate-General for Communications Networks and Content Technology, *Ethics Guidelines for Trustworthy AI* (Brussels, Publications Office 2019).

incorporate mechanisms for technology assessment (TA) and public engagement.[76] TA involves systematically evaluating the potential impacts and risks of emerging technologies, while public engagement ensures that the perspectives and concerns of diverse stakeholders are taken into account in the governance process.[77]

Finally, the International Year of Quantum Science and Technology is an important opportunity for our global community to advance towards coherent and substantive governance of quantum technology. The international community can ensure quantum technologies reach their full transformative promise while limiting their risks by encouraging international cooperation, inclusive education and workforce development, and the pursuit of responsible research and innovation principles. In order to advance the responsible governance of quantum technology, policymakers and other stakeholders must continue their engagement in foresight exercises and scenario planning, anticipating possible future impacts of quantum technologies and considering how best to mitigate them. This could involve establishing dedicated quantum technology assessment bodies or integrating quantum considerations into existing technology assessment frameworks.

4. Recommendations for future regulatory frameworks

As the frontiers of quantum technologies continue to be pushed and new applications continue to unfold, it will be critical to build future regulatory frameworks that are adaptive, collaborative, and forward-looking to address the peculiar challenges and opportunities posed by these technologies. The following recommendations, accordingly, can help drive these future frameworks to fruition:

1. Develop quantum-specific regulations: Governments should cooperate with industry, academia, and civil society stakeholders to promulgate regulations specifically designed to tackle the attributes and challenges of quantum technologies, such as quantum security, quantum data protection, and quantum IP regulations.
2. Foster international cooperation: In light of the fact that many of the advances in quantum are global in scope, the development of a cohesive approach to regulation, one that promotes innovation while mitigating risk, will require international cooperation and coordination. Dialogue between governments at the bilateral and multilateral levels regarding best practices, common standards and cross-border challenges associated with the use of quantum technologies should be actively cultivated.
3. Encourage multi-stakeholder engagement: Quantum technology's crucial role in a wide range of sectors means that robust and effective regulation will require the engagement and input of a large number of stakeholders. These stakeholders include government agencies, the private sector (which could encompass manufacturing, technology companies, finance and other commercial sectors), academic institutions, civil society and expert constituencies. Accordingly, policymakers should enact institutional mechanisms that encourage multi-stakeholder engagement and dialogue on quantum technology regulation to ensure that ongoing deliberation on regulatory design is informed by a rich array of perspectives and knowledge.
4. Emphasise adaptability: As quantum technologies rapidly develop, regulators must develop regulatory frameworks adapted to those technologies by keeping a keen eye on technological development and adapting regulations accordingly.

[76] A Grunwald, *Technology Assessment in Practice and Theory* (Abingdon and New York, Routledge 2019).

[77] G Rowe and LJ Frewer, "A Typology of Public Engagement Mechanisms" (2005) 30(2) Science, Technology, & Human Values 251.

Decisionmakers should consider adopting principles-based approaches to regulation that are flexible and allow room to accommodate new developments and applications of quantum technologies in the future.

5. Consider trade-offs around innovation and risk mitigation: Future quantum regulations will need to balance innovation goals, such as encouraging development in quantum technologies and mitigating risk and unforeseen consequences. Such mitigation strategies might be suitably aligned by utilising risk-based approaches to regulation: the use of risk frameworks to develop regulatory standards for quantum technologies based on the expected or actual quantum-related outcomes or consequences.
6. Invest in quantum literacy and quantum workforce development: Governments could invest toward increasing the quantum literacy of policymakers, regulators and the public more broadly. For example, intergovernmental organisations and/or governments could support academic programmes, workforce development initiatives and public outreach programs focused on quantum safety and security.

Following these recommendations and coordinating globally and across sectors, policymakers can shape future regulations to optimally address the transformative potential of quantum technologies and to nurture their responsible development and use for the benefit of society.

VI. Ethical considerations

The progression of quantum computing, accompanied by the emergence of its broad applications, raises a problem of their social and ethical implications. Indeed, with the high potential for addressing various complex problems and enhancing innovations in multiple spheres, quantum computing brings about numerous challenges and risks that should be appropriately addressed. This part will address the ethical implications of quantum computing. It will centre upon social repercussions and the necessity for ethically weighing the opportunities and threats of quantum technology.

1. Societal and ethical impacts of quantum computing

Quantum computing has the power to transform many sectors, from healthcare and finance to transportation and energy. However, the same abilities that make quantum computing so powerful also come with their own set of ethical questions and concerns. Perhaps one of the most serious issues concerning quantum computing's impact is the possibility of disrupting cryptography and data security. Quantum computers may be capable of cracking many of the cryptographic algorithms that now safeguard our digital messages and transactions, as previously noted. This may have a significant impact on individual privacy, national security, and the financial markets. Post-quantum cryptography is critical to limiting these hazards, but it calls into question the accessibility and distribution of quantum-resistant security measures.

Another aspect in which quantum computing may have profound implications is artificial intelligence (AI) and machine learning. Using quantum algorithms, AI systems may be exponentially faster and more accurate than traditional systems, allowing them to handle enormous data volumes and link disparate datasets to identify sophisticated patterns and discoveries.[78] These systems are expected to revolutionise areas such as drug discovery, material science and climate modelling but will also introduce new concerns

[78] See J Biamonte and others, "Quantum Machine Learning" (2017) 549(7671) Nature 195.

about the transparency, accountability, and fairness of quantum-powered AI systems.[79] Ethical rules must be built and enforced as these systems gain autonomy and power to ensure their responsible development and deployment.

Additionally, quantum computing could be used to further entrench social and economic disparities that already prevail in modern societies. Just like much other emerging technology, quantum computing might only be available to a limited number of people, corporate entities, or countries in the world. Such a development would leave a considerable population disadvantaged and create a "quantum gap" separating those with quantum computing abilities from those without. It will, therefore, be important to create an environment where everyone can partake in quantum education, research, and infrastructure to avoid a situation where quantum advantages concentrate in the hands of a few.

Furthermore, the development and implementation of quantum computing have fundamental implications for the roles and obligations of research, development, and policymakers. As quantum technologies become more powerful and their impacts on society more severe, it will be essential to consider the positive and negative effects of these technologies on the population. These may include challenging issues related to using quantum computing for military purposes, surveillance or manipulation, and the need to balance scientific progress with public safety and well-being.[80]

2. *Balancing the benefits and risks of quantum technology*

Given the immense potential benefits and risks of quantum technology, it is essential to start developing frameworks and approaches to regulate the competing considerations of quantum computing. This process will require continuous collaboration and dialogue between scientists, policymakers, ethicists, and society in general – to secure the optimal values behind the development and deployment of quantum technologies. In particular, one such balancing act is concentrating the efforts and making the quantum applications that promise the highest positive social impact. For example, quantum computing might help to develop and discover medicines and treatments for various diseases faster and with less expense; it can help optimise renewable energy systems or put more effort into trying to minimise and stop the development of climate change. In all such cases and many others, concentrating efforts on high-impact and positive applications is one effective approach to ensure quantum computing's socially optimal application.

At the same time, in addition to technical standards, it is also critical to set forth strong ethical guidelines and principles for quantum technologies. While existing ethical frameworks, such as the Belmont Report[81] or Asilomar AI Principles,[82] may be adapted to the context of quantum computing, new ones tailored to the specific challenges and opportunities of quantum technologies should also be developed. Issues to be considered in those guidelines should include transparency, accountability, fairness, and privacy. Such a system should provide clear and guiding rules for researchers, developers, and users of quantum technologies.[83]

[79] See V Dunjko and HJ Briegel, "Machine Learning & Artificial Intelligence in the Quantum Domain: A Review of Recent Progress" (2018) 81(7) Reports on Progress in Physics 074001.

[80] See M Möller and C Vuik, "On the Impact of Quantum Computing Technology on Future Developments in High-Performance Scientific Computing" (2017) 19(4) Ethics and Information Technology 253.

[81] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, "The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research" (*US Department of Health and Human Services* 1979) <https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html> (last accessed 22 May 2024).

[82] Future of Life Institute, "Asilomar AI Principles" (*Future of Life Institute* 2017) <https://futureoflife.org/open-letter/ai-principles/> (last accessed 22 May 2024).

[83] See I Rahwan and Others, "Machine Behaviour" (2019) 568(7753) Nature 477.

Proactive risk assessment and management are also relevant for striking a balance between the benefits and risks of quantum technology. This measure can be implemented through systematic horizon scanning to detect novel threats and vulnerabilities of quantum-based technologies, accompanied by the development of contingency plans and countermeasures.[84] In addition, the industry can invest in related research and development work to produce "quantum-safe" technologies and infrastructures.[85] This may be achieved by developing and deploying post-quantum cryptographic and quantum resistance hardware to generate a quantum-proof encryption scheme.

Lastly, building public trust and familiarity with advanced quantum technologies will be necessary to ensure these tools are developed and used responsibly. As with any other unfamiliar technology, researchers and professionals in quantum computing will need to take steps to explain the benefits and risks of their work to nonspecialist audiences, whether through public outreach, policymaker engagement or other efforts. We should also strive to include a diverse array of stakeholders in the governance and management of quantum technologies to boost the public's trust in it. Through these measures, the entire quantum computing field may be designed and implemented to follow societal norms and requirements.

VII. Future outlook

As quantum computing advances and its applications become more widespread, it is essential to consider the long-term implications of this transformative technology in the legal field. This part addresses the possible consequences of quantum computing on legal practice, the development of quantum-based legal tech solutions, and the importance of preparing the legal workforce for the quantum era.

1. Long-term implications of quantum computing on the legal field

Quantum computing has the potential to transform the legal field in the future; quantum computing would lead to a paradigm shift in how legal research is conducted and how legal disputes are resolved. The most important impact of quantum computing currently and in the future on the legal field is the possibility of speeding up and improving legal research and analysis. Quantum algorithms could be applied to rapidly search and analyse large amounts of legal data, such as case law, statutes and regulations, and regulatory filings, aiding attorneys in finding relevant precedents and arguments swiftly.[86] This would not only save legal professionals and their clients time and money but also provide more accurate findings.

Furthermore, quantum computing may open up prospects for the emergence of much more advanced tools for legal analytics. Such tools might help identify hidden complex patterns and interconnections in legal data that a human analyst might have difficulty recognising. Consequently, it may boost a lawyer's capacity to foresee the merits of a lawsuit or the outcome of a case and develop a better legal position. Additionally, quantum computing might also have distant implications for the domain by accelerating the settlement of disputes. Since quantum algorithms enable the resolution of hard and complicated problems, they may be employed to optimise the most successful and least

[84] See for example, M Altman, A Wood and E Vayena, "A Harm-Reduction Framework for Algorithmic Fairness" (2018) 16(03) IEEE Security & Privacy 34, 35–7.

[85] See Rahwan and Others, supra, n 83, 484.

[86] See A Pentland, "A Perspective on Legal Algorithms" (*MIT Law*, 7 December 2019) <https://law.mit.edu/pub/aperspectiveonlegalalgorithms/release/3> (last accessed 22 May 2024).

expensive strategy for a mutual settlement. This might be used in the course of a complex judicial settlement or to simulate the outcome of a judicial settlement.

Moreover, with the help of quantum computing, one might be able to create more sophisticated alternative dispute resolution systems like quantum-enhanced mediation or arbitration. With unlimited data processing and the possibility to simulate various complicated situations, they might allow one to settle legal disputes in a more efficient and fair way than it is possible to do via traditional litigation, which is also, *inter alia*, a more time- and money-consuming way of resolving conflicts.

On the other hand, there are substantial long-term consequences of quantum computing that may negatively affect the legal sector. For one, employing quantum algorithms in legal research and legal background documentation may cause issues of transparency and accountability (control over legal decisions), especially if the algorithms used are not easily understood and could conceal bias. The potential application of quantum computing to litigation could also pose serious concerns by calling the fairness and legitimacy of such an outcome into question, depending on the extent to which the parties to an action have equal access to quantum computing resources and expertise. Addressing these concerns will require continued engagement and dialogue between legal professionals, technologists, ethicists and policymakers to prioritise the ramifications of quantum computing for legal practice and take the appropriate steps accordingly.

2. *Potential changes in legal practice and the development of quantum-based legal tech solutions*

Given the role that quantum computing will inevitably have in the field of data-driven legal work, quantum computing can be expected to herald major transformations in what we today refer to as legal tech and contribute to the emergence of innovations such as quantum-borne legal analytics and prediction. The tools could harness the resources of quantum computing to comb through mountains of legal data and produce highly accurate projections on the results of future cases or on the probabilities of particular legal events. Such a service would allow lawyers to consider the chances of success of a case before taking it on, make informed choices about the investment of resources to bring to a case and give legal advisers the data to identify the most viable way to mount a challenge or appeal.

Another change in legal practice might be the emergence of quantum contract analysis and management software. Such tools might involve quantum algorithms helping to review large and complex contracts quickly and discover risks, contradictions, and an opportunity for a better deal. As a result, lawyers can draft better, faster and more efficient contracts and manage and monitor contract performance more effectively.

Likewise, quantum computing could facilitate the advancement of novel legal tech solutions applicable to e-discovery and document review. Quantum e-discovery software systems would allow identifying and pulling only relevant documents and data for litigation quickly. Similarly, such tools would save time and money compared to traditional e-discovery tools or software systems. In addition, advancements in quantum-based legal tech might also give rise to new legal service delivery methods. These might include quantum-enhanced legal process outsourcing and quantum-based legal consulting services, which would utilise quantum computing to offer more efficient and less costly legal services, mostly in the areas of contract drafting and administration, as well as compliance and risk management.

On the other hand, the emergence of quantum-based legal tech solutions creates considerable risks and challenges. Namely, the complexity and high costs associated with the development and implementation of quantum computing systems can require

significant investments and expert expertise from larger law firms and legal entities, further aggravating the existing inequalities in the legal industry.

Furthermore, the implementation of quantum-based legal tech tools may raise concerns about the protection of the security and privacy of sensitive legal data, especially considering that quantum computers can decrypt traditional encryption methods. Addressing these challenges will require ongoing investment in quantum-safe security measures, as well as the development of clear legal and ethical guidelines for the use of quantum computing in legal practice.

3. Preparing the legal workforce for the quantum era

As quantum computing becomes more prevalent in the legal field, it is critical to prepare the legal workforce for the threat it may pose while also preparing them to seize the opportunity it presents. This will require a concerted effort to educate and train legal professionals in the fundamentals of quantum computing and its potential applications in the legal domain. Law schools and similar legal training programmes will have to integrate quantum computing knowledge into the existing curricula. Such integration implies a general understanding of the technology and its possible applications in legal practice. The development of relevant courses and study materials with an emphasis on the relationship between quantum computing and law is expected.

Additionally, beyond formal education and training, legal professionals will need to undertake continuous professional development and learning to keep pace with recent developments in quantum computing and its use in the legal domain. This might include conferences, workshops, or seminars on quantum computing and law, as well as online learning communities and resources. Legal organisations and law firms will also have to spend in cultivating the quantum computing knowledge and abilities of their staff. This might entail recruiting quantum computing experts or partnering with quantum computing providers to create bespoke legal technology solutions and services.

Furthermore, preparing the legal workforce for the quantum era will involve dealing with issues of diversity, equity, and inclusion in quantum computing. Indeed, the quantum computing workforce is primarily male, and the field has few players from different racial, ethnic, and socioeconomic status backgrounds. To ensure that the benefits and opportunities presented by quantum computing elicit the range of legal players' needs and aspirations, there is a need for a highly diversified quantum computing workforce.

VIII. Conclusion

Quantum computing is rapidly evolving, and the legal community is facing unprecedented opportunities and challenges with its emergence. Given its rapid development, the legal community must lay the groundwork for addressing the legal implications and building a coherent framework to manage the developments of this quantum era.

This article analysed quantum computing's primary legal ramifications, including IP, data security, and ethical concerns. Quantum capabilities have the potential to challenge our traditional patent system since quantum algorithms and hardware possess an unprecedented scope and potential for discovery. Quantum computing will render current encryption methods obsolete, and attention should be paid to establishing data protection policies and post-quantum cryptography as soon as possible.

Regulation of quantum technology is in its nascent phase, and different jurisdictions have different regulative approaches to quantum technologies. Policymakers must work closely with industry, academia, and civil society to establish adaptive, principle-based legal frameworks that strike a balance between innovation pressure and risk mitigation.

Given the global implications of quantum research, collaboration among nations and stakeholders is essential. Moreover, the societal and ethical implications of quantum computing must not be overlooked.

Given the increasing power of quantum computing, it is essential to prioritise initiatives that advance a large social good and develop a robust set of principles and ethical guidelines to govern the development and deployment of quantum computers. Proactive risk assessment and management, along with efforts to foster public trust and understanding, will be key to ensuring that the benefits of quantum computing are distributed equitably and potential harms are mitigated.

The quantum era will be upon us soon, and preparing the legal workforce for this quantum era will require a concerted effort to educate and train legal professionals in the rudiments of quantum computing and its probable applications. Law schools and other legal organisations have to invest in developing quantum literacy and capability while settling the issues of diversity, equity, and incorporation in the quantum workforce. The legal implications of quantum computing are vast and far-reaching, presenting both challenges and opportunities for the legal community. By adopting a proactive, interdisciplinary, and collaborative approach, legal professionals can play a vital role in shaping the quantum future and ensuring that this transformative technology is developed and deployed in a manner that upholds the rule of law, protects individual rights, and promotes the greater good of society.

Competing interests. There are no competing interests to declare.

Funding statement. This article was not funded in any way by a person or organisation with any financial or other interest in its content. The author certifies that he has no affiliations with or involvement in any organisation or entity with any financial or non-financial interest in the subject matter or materials discussed in this manuscript. This research received no specific grant from funding agencies in the public, commercial or not-for-profit sectors.

Cite this article: K Balarabe, "Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2025.8