Quantum Technological Era: Legal Shifts and Challenges

-Nishita Sharma*

Abstract

The year 2025, declared the International Year of Quantum Science and Technology, by the United Nations General Assembly, marks a century since German theoretical physicist, Werner Heisenberg first introduced the foundational theory of quantum mechanics. This symbolic milestone coincides with unprecedented global advancements in quantum technologies, ranging from quantum computing to quantum communication, heralding what is often referred to as the 'second quantum revolution". As tech giants and nation-states alike race to secure dominance in this transformative field based on their priorities, massive investments and national strategies are being rolled out to position themselves as quantum superpowers.

Amidst this surge of technological ambition, the legal and regulatory challenges posed by quantum technologies have yet to be fully conceptualised, let alone addressed. Existing legal frameworks, particularly in areas such as data protection, intellectual property and cybersecurity, are largely unequipped to handle the complex implications of quantum capabilities. The disruptive potential of quantum computing to undermine current encryption standards, for instance, calls for urgent re-evaluation of global data security norms.

This paper explored the foundational principles of quantum mechanics that underpin emerging technologies, maps out major governmental and corporate initiatives driving the quantum agenda, and critically assesses the regulatory gaps that exist in anticipation of this shift. It also evaluates India's position within the global quantum landscape, examining recent national missions, institutional capacities, and policy responses. By adopting an interdisciplinary lens, this paper aims to contribute to the growing discourse on the legal preparedness needed in the face of quantum disruption.

I. Introduction

The rapid advancement in development of quantum computing, represents unparalleled challenges and huge scopes of advanced technologies. As we might already know, quantum physics is one of the most interesting branches of physics, and also one of the most less-understood one. There are numerous unique characteristics of quantum algorithms and hardware, and owing to this there are very different set of problems arising.

* 4th-year student at NALSAR, University of Law.

Quantum technologies represent a paradigm shift in computing, cryptography, and sensing, challenging existing legal frameworks designed for classical systems[1]. These technologies leverage quantum mechanical phenomena like superposition and entanglement to perform calculations and transmit information in fundamentally different ways than conventional systems. Due to this innovation, there are different needs to establish new frameworks or modify the current ones, focusing on intellectual property, data security, regulations and also ethical considerations.

The legal system faces several challenges in addressing quantum technologies. First, quantum computing threatens current encryption standards, potentially rendering sensitive data vulnerable and undermining privacy laws and cybersecurity regulations. Second, quantum sensing technologies raise novel privacy concerns by potentially detecting information through barriers previously considered impenetrable. International governance presents another challenge, as quantum technologies could disrupt power balances in cybersecurity and intelligence gathering. Export controls and technology transfer regulations require reconsideration in light of these unlimited quantum capabilities. Legal frameworks need adaptation in several key areas. Cryptographic regulations must evolve to establish quantum-resistant standards and transition protocols.

Data protection laws require updating, in order to effectively address quantum-specific vulnerabilities, since there are already multiple plans and frameworks across different jurisdictions contributing to development of the technologies.

In terms of ethical considerations, there are different dimensions that will have to be looked at. As the systems become more powerful, they will pervade important walks of lives, and it would also have profound societal impacts[2], such as exacerbating inequalities, enabling mass surveillance or making the decision-making process automated, as we saw with the rise of AI. Hence, the emphasis should also be on implementing robust ethical guidelines for responsible use of such technologies.

National security frameworks need provisions for quantum communication channels and computing resources. International agreements on quantum technology development and deployment are

---

[1] John Preskill 'Qauntum Computing in the NISQ era and beyond' (2018) <https://doi.org/10.22331/q-2018-08-06-79> Quantum 2, 79, accessed 12 March 2025.

[2] P. E. Vermaas, 'The societal impact of the emerging quantum technologies: a renewed urgency to make quantum theory understandable' (2017) Ethics and Information Technolgy <https://link.springer.com/article/10.1007/s10676-017-9429-1>.

necessary to prevent fragmented regulations and security vulnerabilities. The legal system must adopt a proactive and flexible approach, incorporating technical expertise in quantum physics while maintaining foundational legal principles of privacy, security, and fairness.

II. Foundational Theory of Quantum Computing

The evolution of quantum technology can be traced back to the early 20th century, with the rising study of quantum mechanics. However, more practical applications emerged in the late 20th and early 21st centuries. Interestingly, in 2023 the Nobel Prize in Physics was awarded to 3 Quantum physicists.

In 1981, the prominent physicist, Richard Feynman proposed the idea of quantum computers. This served as the bed rock for the 1994 quantum algorithm designed by Peter Shor[3], it demonstrated the potential of quantum computing to break the widely used schemes in encryption.

By 2020, several tech giants like IBM, Google and Intel had developed Quantum computers capable of performing tasks on a much-advanced level than the classical computers. IBM's quantum processor achieved quantum volume milestones[4].

Quantum computing operates on fundamentally different principles than classical computing. It leverages the unique properties of quantum mechanics, specifically, the interactions of subatomic particles such as protons, neutrons, and electrons, to achieve exponentially greater processing power.

Traditional computers rely on binary "bits," which exist in one of two states, 0 or 1, and perform logical operations such as "and," "not," and "or" to process data. They employ a series of circuits, called 'gates', and perform all the logical operations, based on the state of those switches. In contrast, quantum computers substitute the binary 'bits' with "qubits". Qubits operate through the phenomenon of Quantum Superposition, and can exist as 0, 1, or both simultaneously.

Mathematically, superposition equation is a combination of '0' and '1' and is written linearly as:

---

[3] Peter W. Shor, 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer', (1996) <https://arxiv.org/pdf/quant-ph/9508027> accessed 12 March 2025.

[4] Ankit Singh, "The Impact of Quantum Technology on Data Security" (29 May 2024) <https://www.azoquantum.com/Article.aspx?ArticleID=524> accessed 20 March ch 2025.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Here, $|\psi\rangle$ is the state of the qubit, and $|0\rangle$ and $|1\rangle$ are the basis states and α and β, are complex numbers called 'probability amplitudes'. These amplitudes determine the probability of measuring the qubit in either state when a measurement is made[5]. This ability enables quantum systems to perform multiple calculations at once, significantly enhancing computational efficiency.

Another, reason behind these technologies being extremely rapid, is the phenomenon of 'Quantum Entanglement.' Quantum entanglement is the state where multiple objects- let's say electrons and photons, share a single quantum state[6]. The qubits, can exhibit "entanglement," where the state of one qubit is intrinsically connected to another, regardless of distance. This, in strict quantum physics terms was termed as "spooky action at a distance", by Einstein. The entangled entities, cannot be described as independent anymore.

In quantum computing, this phenomenon of entanglement, allows quantum parallelism. It is the ability of the computer to perform multiple calculations simultaneously. Essentially, it means that many qubits would be entangled in a single operation, and if a measurement is made on one of them and it is $|0\rangle$, the state of the other qubit will immediately collapse to $|0\rangle$ as well[7].

As more qubits become entangled, computational capacity grows exponentially. For instance, in 2019, a 72-qubit quantum computer executed a complex calculation in just 200 seconds, a task that would have taken the most advanced supercomputer an estimated 10,000 years to complete[8].

In 2020, as per a report by McKinsey, by 2030 there would be 2000-5000 quantum computers that would be operational[9].

---

[5] Microsoft, 'Explore Quantum Superposition' < https://quantum.microsoft.com/en-us/insights/education/concepts/superposition> accessed 12 March 2025.

[6] Dan Garisto, ' What is Quantum Entanglement' (8 June 2022) <https://spectrum.ieee.org/what-is-quantum-entanglement> accessed 12 March 2025.

[7] Microsoft, 'Explore Quantum Entanglement' <https://quantum.microsoft.com/en-us/insights/education/concepts/entanglement> accessed 10 March 2025.

[8] Berkeley Nucleonics Corp, "Quantum Computing v Classical Computing" (23 August 2024) <https://www.berkeleynucleonics.com/Augustust-23-2024-quantum-computing-vs-classical-computing> accessed 10 March 2025.

[9] McKinsey Quarterly, "A game plan for Quantum Computing" (6 February 2020) <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/a-game-plan-for-quantum-computing> accessed 13 March 2025.

III. How Do They Differ Significantly From Classical Computers?

Classical computers have been the dominant form of computing for decades. They work by employing binary bits which are in the states of either 0 or 1. This limit them to perform N number of calculations, when N number of bits are employed. However, with Quantum computers they can do 2^N calculations in the same time. If classical computer can do 5 calculations, then a quantum computer can do 32 calculations in the same time.

Quantum computing relies on quantum bits (called qubits), instead of the traditional binary bits. Quantum computing relies on quantum entanglement, essentially what it means is that multiple qubits are sustained in 'quantum-coherent' state, whereby qubits are entangled. In 2024, it was ascertained that fifty qubits was the approximate number where quantum computing becomes capable of calculations very swiftly[10].

Additionally, both types of computers employ algorithms to perform calculations. An input goes in and then the algorithm processes it and puts out an output. Quantum computations[11] take into account multiple options simultaneously and the execution of algorithms take just one step, that too in a very miniscule amount of time. In contrast, classical computers, algorithms take a lot of parallel computations which is very time consuming. Additionally, classical computers also rely on a deterministic algorithm, this means that the output for an input will always remain same, however, quantum computers employ probabilistic algorithms, meaning they can produce a range of outputs, all probabilistic. This entails solving problems that are intractable for the classical computers[12].

IV. Where Can Quantum Computing Be Used

As already described above, the quantum computers excel at handling highly complex operations. They have several potential advantages over classical computing, making them particularly effective for tasks such as

---

[10] Quantropi, ' Quantum Versus Classical Computing and the Quantum Threat' <https://www.quantropi.com/quantum-versus-classical-computing-and-the-quantum-threat/#:~:text=Quantum%20Versus%20Classical%20Computing,-In%20general%2C%20classical&text=In%20classical%20computers%2C%20an%20algorithm,options%20in%20a%20single%20step> accessed 30 March 2025.

[11] Yudong Cao, 'Quantum Chemistry in the age of quantum computing' (2019) Chem.Rev. <https://doi.org/10.1021/acs.chemrev.8b00803> accessed 20 March 2025.

[12] Y Huang and S Pang, "Optimization of a Probabilistic Quantum Search Algorithm with a Priori Information" (2023) 108(2) Physical Review <https://journals.aps.org/pra/abstract/10.1103/PhysRevA.108.022417> accessed 20 March 2025.

simulating particle interactions, solving optimization problems with multiple variables, significantly enhancing AI training processes, and rapidly factoring prime numbers, which an essential aspect of modern encryption systems.

The most notorious of these domains is the use of cryptography. In 1994, mathematician Peter Shor, described quantum computers to pose a significant threat to the traditional security systems[13]. He also demonstrated a theoretical quantum computer's ability to effortlessly decipher the encryption algorithm, public key encryption (PKE).

Quantum computers are believed to be capable of breaking many existing encryption schemes. In theory, it is more secure than any of the previous types of cryptographic algorithms and is also unhack-able. Since, it is impossible to predict the exact quantum state of the qubits, they can exist in several positions at any given time, hacking becomes almost impossible without altering the algorithm altogether.

Another area is simulation of complex quantum systems such as molecules, this would allow computers to accurately simulate chemical reactions. It would also consequentially allow for discovering of new materials. These advanced capabilities position quantum computing as a game-changer across various industries, including pharmaceuticals for drug discovery.

V. Current Developments

Scholars term this era as "Second Quantum Revolution" after the first revolution in the early twentieth century. Governments worldwide are making substantial investments in quantum computing research and development, recognizing its transformative potential. The European Union's Digital Decade Strategy aimed for Europe to have its first supercomputer with Quantum Acceleration in 2025, and to have it at the cutting edge of Quantum capabilities by 2030[14].

The European Union has spearheaded several initiatives in this direction, including the Quantum Technologies Flagship, which was launched in

[13] Josh Schneider & Ian Smalley, "What is Quantum Cryptography" (1 December 2023) <https://www.ibm.com/think/topics/quantum-cryptography> accessed 10 March 2025.
[14] European Commission, "Europe's Digital Decemberade : Digital Targets for 2030" <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-Decemberade-digital-targets-2030_en>

2018. It is a decade-long, €1 billion research and innovation program[15]. In October 2022, the European High Performance Computing Joint Undertaking, (EuroHPC JU), announced six places to have first European Quantum Computers. Alongside these, there is also the European Quantum Communication Infrastructure (EuroQCI), which aims to establish a secure quantum communication network across all 27 EU Member States.[16].

Apart from Europe, China's 14th five-year plan (2021-2025)[17] also provided valuable insights into the country's stance on quantum technologies. According to that, China has become a pioneer in building Quantum communication infrastructure, and that is also its strategic priority in terms of strengthening its national defence and proliferation of economic growth.

In 2018, the US released its National Quantum Strategy and entailed an approach at federal level to improve research and development in Quantum Technology for the same reasons as China. The US also has the National Quantum Initiative Act, which was signed into law in 2018, it established a framework to accelerate quantum research and development. In the United States, the National Institute of Standards and Technology (NIST) has initiated a process to develop and standardize encryption protocols capable of withstanding quantum computing threats, which is about developing new algorithms that are resistant to hacking.

VI. 2025: The year of Quantum Science

The year 2025 marks the centenary of Heisenberg's developments of matrix mechanics, which was the first solidification of the ideas of quantum mechanics into a coherent physical theory. And the United

[15] European Parliament, "Quantum : What is it and where does EU stand", (10 April 2024) <https://epthinktank.eu/2024/04/10/quantum-what-is-it-and-where-does-the-eu-stand/> accessed 12 March 2025.

[16] Defence Industry and Space, "Quantum Technologies" <https://defence-industry-space.ec.europa.eu/eu-space/research-development-and-inNovemberation/quantum-technologies_en#:~:text=The%20Quantum%20initiative%20%E2%80%9CEuroQCI%20%E2%80%9D%20intends,critical%20infrastructures%20across%20the%20Union> accessed 10 March 2025.

[17] The Government of Fujian Province, "Outline of the Five-Year Plan (2021-2025) for Social Development and Visions 2035 of the People's Republic of China (9 August 2021) <https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm#C4> accessed 13 March 2025.

Nations General Assembly also declared 2025 to be the International Year of Quantum Science and Technology (IYoQST), on June 7th, 2024[18].

This worldwide initiative recognizes and celebrates the contributions of quantum science to technological progress since the first formalization of theory by Heisenberg. Quantum theory has revolutionised modern electronics, and is also an important pillar of global telecommunications.

It is also to raise global awareness about the importance of quantum technologies for sustainable development in the 21st century. One of the other important aims is also to ensure that all nations have access to quantum education and opportunities in developing those as well. It also stresses on providing youth, girls and women particularly in developing countries with opportunities of learning about science and technology. The focus on inclusivity and support, is critical, it acknowledges the importance of quantum technologies, and also emphasizes on equitable and diverse perspectives in governance frameworks[19].

This is also an acknowledgment of increasing transformative power of quantum technologies and their governance requirements. Quantum science and technology is poised to help address the current most pressing challenges, including but not limited to rapidly develop renewable energy, human health in terms of finding more drugs, climate action, clean water and energy, food security. UN stressed on its importance in supporting UN's Sustainable Development Goals[20].

The IYoQST resolution laid the groundwork for developing a governance framework that is inclusive, adaptive, anticipatory, responsive, and harbours diverse perspectives therein. We are in 2025, which is the International Year of Quantum Science and Technology, is an important opportunity for our global community to reap benefits of it and advance towards a more coherent and substantive governance. The emphasis should be on, letting the quantum technologies reach their full transformative promise while limiting the risks and harms posed by this.

This could be done in a lot of ways, particularly ensuring that all of the developments are grounded in Responsible Research and Innovation (RRI). RRI focuses on the importance of anticipating and mitigating the potential risks poses by technologies, while still ensuring that the

---

[18] UNESCO, "International Year of Quantum Science and Technology"< https://www.unesco.org/en/years/quantum-science-technology> accessed 3 March 2025.
[19] U Gasser, R Budish and S West, "Multistakeholder as Governance Groups: Observations from Case Studies" (2015) Berkman Center Research Publication.
[20] IUPAC, "The International Year of Quantum Science and Technology" (3 October 2024) <https://iupac.org/the-international-year-of-quantum-science-and-technology-2025/> accessed 2 March 2025.

development and deployment of such technologies is not thwarted[21]. Another possible way is to involve establishment of dedicated quantum technology assessment bodies, and integrating scientific minds and quantum considerations into the existing technological regulation frameworks. Legal professionals must also develop expertise in quantum communication systems, particularly Quantum Key Distribution (QKD), which offers unprecedented opportunities for secure data transmission (Scarani et al., 2009).

As these technologies gain traction, lawyers must be prepared to advise clients on the legal implications of quantum-based security solutions and their role in enhancing data protection. This requires continuous engagement with industry advancements, collaboration with quantum technology specialists, and active participation in relevant legal and technological forums.

VII. Effect on The Current Encryption Methods

The advent of quantum technologies poses a significant challenge to existing cybersecurity frameworks. As quantum computing has the potential to break widely used encryption methods, rendering traditional data protection mechanisms ineffective, the threat to cybersecurity is imminent[22].

Although, most of it is limited to theoretical reality, this concern prompted the National Institute of Standards and Technology (NIST), to call for development of 'quantum-safe' encryption algorithms. Interestingly, in 2015 the National Security Agency advised the US agencies and businesses to prepare in time, for the 'not-too-distant' future of quantum technologies wreaking havoc on all existing digital realms[23]. It is pertinent to note that, at the time, the time frame for this was approximately 10 years, and now we are in the timeline of this advisory.

The security of the current modern digital communications and transactions, is heavily reliant on the public-key cryptography. It uses

---

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

[22] James Dargan, "Quantum Cybersecurity Explained : Comprehensive Guide" (13 March 2024) <https://thequantuminsider.com/2024/03/13/quantum-cybersecurity-explained-comprehensive-guide/> accessed 10 March 2025.

[23] Dan Goodin, "NSA preps quantum-resistant algorithms to head off crypto-apocalypse", (21 August 2015) <https://arstechnica.com/information-technology/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/> accessed 15 March 2025.

mathematical algorithms to encode and decode sensitive information, the most widely used such algorithm is ECC (elliptic curve cryptography). Similar algorithms have been considered secure due to the sheer impossibility of the ability to find efficient solutions to the underlying mathematical problem, because of factoring of large numbers. It is deemed impossible for the classical computers, however, as already mentioned above, the situation significantly changes when quantum computing is considered due to their ability to do such computations easily and efficiently.

The ability of quantum computers to employ phenomena of superposition and entanglement, make it feasible for them to calculate something that is considered relatively impossible for the classical computers. Importantly, we currently lack large scale, quantum computers capable of running the Shor's algorithm, however, given the pace of advancement in the area, it is just a matter of a few years till it is a reality, as per experts.

This would have a devastating effect on the digital systems, this algorithm could be leveraged to break the existing encryption protected data, transferred or stored in digital systems, including financial records and government secrets. One may be inclined to think that this threat is not imminent, then why should we pay attention to it. However, the danger of quantum computing is not limited to imminent data breaches, rather, data can be encrypted and saved right now, and can be later decrypted using such quantum computing technologies. Among cybersecurity experts this is the rise of "harvest now, decrypt later" attacks, where malicious actors intercept and store encrypted data today, anticipating the future availability of quantum computers capable of breaking asymmetric encryption. Without pre-emptive quantum-resistant safeguards, businesses could face substantial legal and financial liabilities years down the line.

This has also led to evolution of a field called "post-quantum cryptography"[24] (PQC), which is also called quantum-resistant encryption. PQC is supposed to be resistant to quantum attacks while still retaining the desirable properties of the existing cryptographic systems.

VIII. Data Security and Regulatory Frameworks

The emergence of quantum technologies marks a significant shift in the technological landscape, with profound implications for various sectors,

[24] National Institute of Standards and Technology, 'Post Quantum Cryptography' <https://csrc.nist.gov/projects/post-quantum-cryptography> accessed 12 February 2025.

including law. **In 2013, the infamous Yahoo Data Breach[25], where three billion accounts were hacked, then the Aadhaar case in 2018[26] and the Alibaba data breach in 2019[27],** all of these, detail the turmoil that can occur in the digital world. In the growing quantum world, it is imperative to say that they have the potential to compromise the preexisting encryption methods attributed to their advanced computational abilities.

As quantum computing, quantum communication, and related innovations progress at an unprecedented pace, they present novel legal challenges that necessitate the evolution of regulatory and intellectual property frameworks. The intersection of quantum technologies and the law has given rise to an emerging field known as quantum law, which seeks to address these complex issues. Given their potential to disrupt industries ranging from cybersecurity to artificial intelligence, quantum technologies demand careful legal scrutiny to ensure robust governance and protection of rights.

IX. The Regulatory Demand to Shift

This shift from classical to quantum technology era, raises urgent concerns about privacy and security, particularly in light of established regulatory frameworks such as the United States' Electronic Communications Privacy Act (ECPA) and the European Union's General Data Protection Regulation (GDPR), which may prove inadequate in addressing quantum-related threats (Smith, 2020).

While these current laws, set out certain basic requirements for appropriate and secure processing, as well as storage of personal data, still these fall short of addressing the problems posed by use of quantum technologies. Policymakers and legal experts must now grapple with the necessity of updating these regulations to account for the unprecedented risks posed by quantum advancements[28].

---

[25] Nicole Perlroth, 'All 3 Billion Yahoo Accounts Were Affected by 2013 Attack', *The New York Times* (3 October 2017).

[26] Mardav Jain, 'The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment'(University of Washington News, 9 May 2019) <https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/> accessed 13 February 2025.

[27] Dashveenjit Kaur, 'Is Alibaba responsible for the largest data heist in China' (*Tech Wire Asia,* 18 July 2022) <https://techwireasia.com/2022/07/is-alibaba-responsible-for-the-largest-data-heist-in-china/> accessed 10 February 2025.

[28] Mauritz Kop, 'Towards Responsible Quantum Technology' (21 March 2023) Harvard Berkman Klein Center for Internet and Society Research <https://cyber.harvard.edu/publication/2023/towards-responsible-quantum-technology> accessed 30 March 2025.

Furthermore, the intellectual property landscape faces new complexities, as quantum innovations give rise to novel challenges in patenting, licensing, trade secrets, and other forms of IP protection, necessitating a re-evaluation of existing legal doctrines to accommodate this rapidly evolving field.

X. The Current Regulatory Frameworks

The rapid evolution of quantum technologies demands a proactive legal approach to address emerging challenges effectively. The disruptive potential of quantum computing presents significant legal challenges that must be addressed proactively. One of the most urgent concerns is the profound impact quantum advancements could have on cryptography and digital security.

Many of today's encryption protocols, including RSA and elliptic curve cryptography, are based on mathematical problems—such as prime factorization and discrete logarithms—that classical computers struggle to solve. However, Peter Shor's groundbreaking quantum algorithm (1994) demonstrates that a sufficiently powerful quantum computer could efficiently solve these problems, rendering conventional encryption methods obsolete and compromising the confidentiality of encrypted data.

This looming threat underscores the necessity of developing and implementing quantum-resistant or post-quantum cryptographic solutions. Governments, businesses, and legal institutions must prepare for a post-quantum security landscape by fostering research, updating regulatory frameworks, and ensuring the seamless transition to encryption standards resilient to quantum attacks.

As with any groundbreaking technology, quantum computing is likely to fuel a surge in legal disputes. Its capacity to significantly enhance artificial intelligence and machine learning could amplify existing concerns over algorithmic bias and flawed decision-making, leading to litigation over unfair or harmful outcomes.

As already developed throughout the paper, the major source of contention will be quantum computing's ability to crack current encryption methods, potentially exposing sensitive personal, financial, and commercial data to cybercriminals. This risk could trigger waves of negligence-based class actions from affected consumers, commercial disputes between businesses, and even shareholder litigation over the financial impact of a data breach. Regulators worldwide are already exploring ways to "quantum-proof" cybersecurity, and companies that fail

to take proactive steps may find themselves facing legal action from various stakeholders[29].

From a legal standpoint, current privacy and cybersecurity frameworks are built around the principle of "reasonable security," meaning businesses must implement protective measures that align with the prevailing threat landscape. However, as quantum computing advances toward mainstream adoption, the legal interpretation of what constitutes "reasonable" security may evolve.

The current data protection laws like GDPR and California Consumer Privacy Act[30], would have the locus for regulation of certain aspects of quantum technologies, like cybersecurity and data protection, but they would need significant tailoring bespoke for quantum technologies. For instance, the GDPR mandates that data controllers implement "state-of-the-art" security measures, but such protections may become obsolete if quantum computing renders traditional encryption ineffective. If quantum computers render public encryption keys obsolete, the consequences could be catastrophic for digital ecosystems.

The synergy between quantum hardware and software is critical for implementing these algorithms. Quantum hardware, including superconducting qubits and ion traps, forms the foundation of quantum computation, while quantum programming languages and compilers translate abstract quantum algorithms into executable instructions. Frameworks like Qiskit, OpenQASM, and Q# facilitate the development and optimization of quantum algorithms for specific hardware architectures. This dynamic interaction between quantum hardware, software, and algorithms is fundamental to realizing the full potential of quantum computing.

Thus, Quantum technologies are expected to be safeguarded through a combination of intellectual property (IP) protections, given their complex structure and multidisciplinary nature. A quantum computer comprises various components, including qubits, quantum gates, multipliers, chips, processors, and cooling systems, alongside the software that enables their functionality. Thus, even patent laws and intellectual property rights have a major role to play in the regulation of quantum technologies.

Patent law, which protects novel, useful, and non-obvious human inventions, is particularly relevant for securing advancements in quantum hardware. Meanwhile, copyright—requiring originality, creativity, and

[29] : K Balarabe, “Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap” EJRR <https://doi.org/10.1017/err.2025.8> accessed 15 March 2025.
[30] California Consumer Privacy Act (CCPA) <https://oag.ca.gov/privacy/ccpa> accessed 15 March 2025.

human authorship—is better suited for software-related aspects of quantum computing. Quantum algorithms, often open source in nature, can be eligible for copyright protection once converted into source code. Additionally, patents may apply to certain algorithmic applications that produce a technical effect on quantum hardware. Since quantum computing outputs typically involve human intervention at some stage, they may also be considered intellectual property, akin to traditional software-generated content.

National security concerns surrounding quantum computing could lead to stricter regulations, with some quantum technologies potentially being classified as state secrets. Furthermore, ongoing debates in academic and policy circles question whether traditional IP protections, such as copyright extending for the life of the author plus 70 years, are being considered too rigid for such a rapidly evolving field.

While the stage of development for quantum technologies is still nascent, various international organizations like the World Economic Forum and OECD, and some governments like the US, the UK, Germany, and Japan, have already initiated efforts to address the possible governance challenges posed by these rapidly emerging technologies. The European Commission has introduced proposals aimed at adapting IP frameworks to better accommodate advances in data science and artificial intelligence, signalling potential shifts in how quantum innovations will be protected in the future.

XI. Comparative Analysis: Different Frameworks

To date, different jurisdictions have their own approaches towards developing regulatory mechanisms for quantum technologies. It depends on national priorities, standards, and levels of technological capabilities and existing policy frameworks.

In the US, the National Quantum Initiative Act, was signed into law in 2018. It established a nationally coordinated programme to accelerate quantum research and development, and also allowed for effective public-private partnerships which would contribute to qualified quantum workforce[31]. It also sought to direct the federal governments in their investments in quantum technologies, including consideration of dimensions like legal, ethical and wider societal.

Europe has been a pioneer in this area, it recognized the inevitable strategic importance of quantum technologies, thereby launching several

[31] National Quantum Initiative Act [2018] H.R.6227.

initiatives to support developments as well as regulations to assure minimal damage. European Commission called for a coordinated approach to quantum regulation, and asked for development of European Quantum Policy. This was to ensure that there remains a coherent framework for the development and governance of such emerging quantum technologies, within the European Union. Further, the €1 EU Quantum Flagship, which was launched in 2018 aimed to consolidate and expand the European leadership in this field. This initiative also explicitly addressed quantum technologies, and their societal and ethical implications.

China is also a big contender in quantum era. Its pursuit of quantum technology has been more state led, with a lot of government funds and dialogue facilitations between the public and private sectors. As mentioned previously, the regulations on quantum technologies are based on numerous factors, and, for China it is about situating the country at the forefront of quantum developments. There, quantum technology is a national priority and huge investments are made in research and development. China aims to make substantial and real breakthroughs by as close as 2030. Till 2022, the total investments in quantum technologies in China was $15.3 billion that culminated in a National Quantum Program, this is more than the US and EU cumulatively. China's Educational Modernisation 2035 Plan also emphasizes on quantum technology in the education sector. It also has a somewhat less robust regulatory framework for quantum technologies, which more or less focuses on making as many technological advancements in the quantum sector as rapidly as possible, and putting in place security measures for it.

India is also taking steps towards it. In April 2023, India launched the National Quantum Mission which is to be implemented till 2031 by the Department of Science and Technology. It had four areas: Quantum Computing, Quantum Communication, Quantum Sensing and Metrology and lastly, Quantum Materials and Devices.

Similarly, other countries such as Canada[32]., Japan[33] and Australia[34] have also launched numerous national initiatives to strategize and develop quantum technologies, with varying degrees of emphasis on its regulation, based on what they deem important

XII. Ethical Dimensions

It is also pertinent to identify the potential ethical problems that would emerge with quantum technologies. Since, it is set to completely revolutionize the technological arena, it would inevitably have a lot of ethical implications. By focusing on the ethical dimensions, we can not only allow exploitation of social values of technologies but also, find solutions for risk management from all perspectives.

One argument that keeps being iterated is that, quantum technologies is a nascent technology, its development has largely limited itself to theoretical dimensions, and it is often influenced by a strong rhetoric of revolutionising the future of technologies. However, quantum technologies can be used as an umbrella term for all such range of technologies that are emerging, which are very different from each other but have very strong impacts in all dimensions.

Interestingly, while there are so many discussions and discourse around quantum regulations and strategies, there is no focus on specific ethical problems. In the UK and EU, midterm report on quantum strategy, the terms like 'ethics", and 'morals' did not appear. Some important facets of this discussion are also that there would be a huge imbalance between populations with advanced quantum technologies and the ones without it. As already explained, there would be a new definition of privacy in quantum age, given encryption would be changed drastically.

Additionally, in 2022, the US National Security Memorandum published a report that stated that in order to cope with the risk poses by quantum cryptography, it must promote collaborations with overseas allies, in education and professional aspects. This international engagement would

---

[32] Government of Canada, "Canada's National Quantum Strategy" (Government of Canada, 2 February 2020) <https://ised-isde.canada.ca/site/national-quantum-strategy/sites/default/files/attachments/2022/NQS-SQN-eng.pdf > accessed 22 March 2025.

[33] The Government of Japan, Touching the cutting edge of quantum technology in the homeland of the superconducting qubit (31 May 2022) <https://www.japan.go.jp/kizuna/2022/05/cutting_edge_of_quantum_technology.html > accessed 20 March 2025.

[34] Australian Government, "National Quantum Strategy" (2 May 2023) <https://www.industry.gov.au/sites/default/files/2023-05/national-quantum-strategy.pdf> accessed 20 March 2025.

prove to be essential in identifying various risks and inculcating diverse perspectives on quantum security and protection[35].

One of the key points in discussions about ethical implications of quantum technologies, revolve around social issues concerning equity, diversity and inclusion specifically for marginalized groups in academic literature, policy and debates on quantum technologies. It has been a normal way of looking at technological advancements purely from a legal perspective, and rarely an eye is turned towards the 'social' of it.

One way around it is to inculcate RRI as already described above. RRI helps facilitate public dialogues, envisages involvement of parliaments, allows from inputs from all relevant stakeholder, and given the stochastic nature of the quantum computational system, it is important to have a transparent process. Given that quantum computing inculcates quantum physics which is notoriously misunderstood and less-understood, the need for transparency in communication, explanation and interpretation of quantum algorithms becomes pertinent[36].

Quantum cryptography is the most notorious area of all of it, and cryptography is also an indispensable means to protect information in a computer system. Peter Shor in 1994 already showed that quantum computer can easily solve several of the computational problems. This essentially meant that anyone with a real-world quantum computer would be capable of easily breaking the cryptographic codes, thus compromising the encrypted communications.

At the conjuncture of this problem is the ethical dimension of security v privacy. One way to potentially deal with it is to cultivate post-quantum algorithms like lattice systems, coding-based systems etc. This would raise questions of governmental paternalism, and diminishing rights of privacy and autonomy.

The interplay between ethics and law is crucial in shaping regulations that govern quantum technologies. Legal frameworks must incorporate ethical principles to ensure accountability, prevent misuse, and promote transparency in quantum-powered systems. The ever-impending question of privacy and autonomy will always loom over us, and the key is to find a

---

[35] Scott Buchholz & Beena Ammanath, 'Quantum computing May create ethical risks for businesses' (*Deloitte Insights,*12 May 2022) <https://www2.deloitte.com/us/en/insights/topics/cyber-risk/quantum-computing-ethics-risks.html> accessed 18 March 2025.

[36] Luca M. Possati, 'Ethics of Quantum Computing' [2023], Vol. 36 Philosophy and Technology <https://link.springer.com/article/10.1007/s13347-023-00651-6> accessed 19 March 2025.

good balance between them in an ever-changing and rapidly advancing technological ground.

XIII. Where does India Stand on All of this

On 19th April, 2023, India approved the National Quantum Mission (NQM), which envisioned propelling India into the international forefront of quantum technology research and development. It has a budgetary allocation of Rs. 6,000 crores for the period of 2023-2031. With this, India aims to harness the power of quantum technology to drive innovation in the field and also to position itself as a global leader in this cutting-edge field.

Many countries are already working on this in a more proactive way, making significant contributions to the field, like the US, EU, and China. Since, quantum technology will percolate the most important walks of life like healthcare, clean energy, climate change, data and cyber security, India has a chance to play a key role in the regulatory framework.

As a part of this mission, a total of four Thematic Hubs has been chosen (T-hubs)[37], these bring together 14 Technical groups across 17 states and 2 Union territories. The focus will be on technology innovation, skill development, industry partnerships, fostering a global collaborative space to ensure a national impact. An important feature of these T-hubs is that, they will work on a Hub-Spoke-Spike Model which will foster a cluster-based network. It will focus on a collaborative ecosystem involving 152 researchers from 43 different institutions across the country[38].

Further, India's journey towards becoming a global leader in quantum technology also involves strategic investments. One such initiative to bridge the gap between research and industry is Quantum Computing Applications Lab, which is led by the Ministry of Electronics and Information technology. This lab supports India's aspirations to create a thriving quantum research hub.

Another important step is equipping India's academic institutions to evolve research in quantum technologies. This flows from "Jai Anusandhan" vision of the government, wherein they work closely with the

---

[37] These are: 1. Quantum Computing, 2. Quantum Communication, 3. Quantum Sensing and Metrology and 4. Quantum Materials and Devices.

[38] Ministry of Science and Technology *National Quantum Mission: India's Quantum Leap* (17 March 2025) <https://pib.gov.in/PressNoteDetails.aspx?NoteId=153963&ModuleId=3&reg=3&lang=1> accessed 18 March 2025.

Department of Telecommunications and Department of Science and Technology[39].

Thus, in a nutshell, India's advancements in quantum computing represent a coordinated effort between various stakeholders, including the government, academic scholars, private sectors and evolving startup ecosystem. This has also been a insight of Niti Aayog, which was published in the March 2025 edition of Future Front[40].

XIV. Regulatory Challenges in India

While, India has taken steps towards quantum advancement, it lacks a specific quantum technology regulatory framework. As explained throughout the paper, there is a big threat on current encryption standards, and there is a need to establish a quantum-safe encryption standard.

Given that the other jurisdictions are already ahead of India in this, we can take inspiration from them. In the US, the quantum ecosystem thrives on strong government funding and a dynamic private sector. This is something, the Indian government has already started with the National Quantum Mission. In Europe, there is more emphasis on regional collaboration and strategic autonomy. And in most other jurisdictions the emphasis is also on fostering international dialogues and collaborations.

India must prepare for disruptive breakthroughs, as there are new platforms like silicon spin or topological qubits that have the potential to shorten the quantum timeline, hence, we need to be prepared in advance.

The emphasis should be to foster cooperation between various stakeholders like industry, academia, civil society etc. International cooperation, produce innovation but mitigate risks. Emphasize adaptability.

XV. Conclusion

As we stand at the threshold of a new era in science and technology, the quantum revolution presents both an extraordinary opportunity and a formidable challenge. The year 2025, marking a century since the birth of

---

[39] Cierra Choucair, 'Qauntum Computing in India : Ecosystem Growth & Key Initiatives in 2024' (*Quantum Insider,* 27 November, 2024) <https://thequantuminsider.com/2024/11/27/quantum-computing-advancements-in-india/> accessed 20 March ch 2025.

[40] NITI Aayog, *Quantum Computing : National Security Implications & Strategic Preparedness,* Issue 2, (March . 2025).

quantum mechanics, has not only been symbolically recognized by the United Nations, but has also emerged as a watershed moment in global technological development.

Quantum technologies, be it computing, cryptography, sensing or communication, have the potential to reshape the digital landscape in profound and irreversible ways. And so, the critical need to reassess and reimagine existing legal and regulatory frameworks. Quantum computing's capacity to break current cryptographic systems threatens the foundational security structures that underpin global digital infrastructure. The legal community must, therefore, move beyond reactive governance and adopt a proactive, anticipatory approach to regulation. This involves creation of flexible, principles-based frameworks that can adopt to the rapid pace of quantum advancements while ensuring accountability, security and ethical integrity.

India's recent push toward quantum leadership through the National Quantum Mission and various public-private collaborations is a promising step in the right direction, yet, for India to emerge as a serious global player, it must also invest in developing legal, ethical and policy ecosystems.

This paper has explored foundations of quantum technology, highlighted major global initiatives, exposed shortcomings in regulations and assessed India's emerging role in this landscape. Ultimately, it has asserted that innovation is not an enemy of the legal, rather the goal is to keep pace with technological change, to shape it responsibly. As we stand at the threshold of a quantum revolution, it is only apt to recall Niels Bohr's timeless words:

"Anyone who is not shocked by quantum theory has not understood it."