QUANTUM TECHNOLOGICAL ERA: LEGAL SHIFTS AND CHALLENGES

Nishita Sharma, NALSAR, University of Law

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 the 'second quantum revolution". As tech giants and nation-states 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 data protection, intellectual property and cybersecurity, are largely unequipped to handle the complex implications of quantum capabilities. For instance, the disruptive potential of quantum computing to undermine current encryption standards 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 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.

Introduction:

The rapid advancement in the development of quantum computing represents unparalleled challenges and an immense scope of advanced technologies. As we might already know, quantum physics is one of the most interesting and least understood branches of physics. There are numerous unique characteristics of quantum algorithms and hardware, so very different sets of problems arise.

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 is a need to establish or modify new frameworks, focusing on intellectual property, data security, regulations, and 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: 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 to effectively address quantum-specific vulnerabilities, since multiple plans and frameworks exist across different jurisdictions, contributing to the development of the technologies.

Regarding ethical considerations, different dimensions will have to be examined. As the systems become more powerful, they will pervade essential walks of life and have profound

[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.

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, we should emphasise implementing robust ethical guidelines for the 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 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.

Foundational Theory of Quantum Computing:

The evolution of quantum technology can be traced back to the early 20th century, with the rise of the 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, which served as the bedrock for the 1994 quantum algorithm designed by Peter Shor[3], which 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 much more advanced than classical computers. IBM's quantum processor achieved quantum volume milestones[4].

Quantum computing operates on fundamentally different principles from classical computing. It leverages the unique properties of quantum mechanics, specifically, the interactions of

[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>.

[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.

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

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

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 simultaneously, significantly enhancing computational efficiency.

Another reason why these technologies are extremely rapid is the phenomenon of 'Quantum Entanglement'. Quantum entanglement is where multiple objects- like 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. In strict quantum physics terms, this was termed "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. The computer can perform multiple calculations simultaneously. Essentially, it means that many

[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.

qubits would be entangled in a single operation, and if a measurement is made on one of them and it is |0⟩, the state of the other qubit will immediately collapse to |0⟩ 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].

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 limits them from performing N calculations when N bits are utilised. However, with Quantum computers, they can do 2^N calculations in the same time. If a classical computer can do five calculations, then a quantum computer can do 32 calculations simultaneously.

Quantum computing relies on quantum bits (called qubits) instead of the traditional binary bits. Quantum computing relies on quantum entanglement; essentially, multiple qubits are sustained in a 'quantum-coherent' state, whereby qubits are entangled. In 2024, they ascertained that fifty qubits were 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

[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.

[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.

goes in, and then the algorithm processes it and puts out an output. Quantum computations[11] consider multiple options simultaneously, and the execution of algorithms takes just one step, which is also a very minuscule amount of time. In contrast, classical computers and algorithms require a lot of parallel computations, which is very time-consuming. Additionally, classical computers rely on a deterministic algorithm, which means that the output for an input will always remain the 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 classical computers[12].

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 simulating particle interactions, solving optimisation problems with multiple variables, significantly enhancing AI training processes, and rapidly factoring prime numbers, 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 as a significant threat to 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. Theoretically, it is more secure than any of the previous types of cryptographic algorithms and unhackable. Since it is impossible to predict the exact quantum state of the qubits, they can exist in several positions at any given time, making hacking almost impossible without altering the algorithm altogether.

Another area is the simulation of complex quantum systems, such as molecules, which would allow computers to simulate chemical reactions accurately. It would also consequently allow

[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.
[13] Josh Schneider & Ian Smalley, "What is Quantum Cryptography" (1 December 2023) <https://www.ibm.com/think/topics/quantum-cryptography> accessed 10 March 2025.

for the discovery of new materials. These advanced capabilities position quantum computing as a game-changer across various industries, including pharmaceuticals for drug discovery.

Current Developments:

Scholars term this era the "Second Quantum Revolution" after the first revolution in the early twentieth century. Governments worldwide are investing substantially in quantum computing research and development, recognising 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 launched in 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 sites to host the first European Quantum Computers. 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, which is also its strategic priority in strengthening its national defence and promoting economic growth.

In 2018, the US released its National Quantum Strategy, which entailed an approach at the 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

[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>

[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.

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 standardise encryption protocols capable of withstanding quantum computing threats, which involves creating new algorithms resistant to hacking.

2025: The year of Quantum Science:

The year 2025 marks the centenary of Heisenberg's development of matrix mechanics, which was the first solidification of the ideas of quantum mechanics into a coherent physical theory. And the United 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 recognises and celebrates the contributions of quantum science to technological progress since Heisenberg's first formalisation of the theory. Quantum theory has revolutionised modern electronics and is an essential pillar of global telecommunications.

It also raises global awareness about the importance of quantum technologies for sustainable development in the 21st century. One of the other essential aims is to ensure that all nations have access to quantum education and opportunities to develop it. It also stresses 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, as it acknowledges quantum technologies' importance and emphasises equitable and diverse perspectives in governance frameworks[19].

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

[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.

The IYoQST resolution established groundwork for developing a governance framework encompassing inclusive, adaptive, anticipatory, and responsive elements while harbouring diverse perspectives. As we navigate 2025, designated as the International Year of Quantum Science and Technology, our global community has a significant opportunity to reap the benefits of quantum technologies and advance toward more coherent and substantive governance.

Policymakers and stakeholders should emphasise allowing quantum technologies to reach their full transformative promise while limiting the risks and harms these technologies pose. This balanced approach enables society to harness quantum innovations while protecting against negative consequences.

Developers and researchers can accomplish this through various approaches, particularly by grounding all developments in Responsible Research and Innovation (RRI) principles. RRI emphasises the importance of anticipating and mitigating technologies' potential risks. At the same time, RRI ensures that such risk mitigation efforts do not thwart the development and deployment of these technologies. This framework allows innovators to pursue technological advancement while maintaining appropriate safeguards and ethical considerations[21]. Another possible way is to establish dedicated quantum technology assessment bodies and integrate 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.

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

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

methods, rendering traditional data protection mechanisms ineffective, the cybersecurity threat 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 the 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.

Modern digital communications and transactions rely heavily on public-key cryptography for their security. This system uses mathematical algorithms to encode and decode sensitive information, with ECC (elliptic curve cryptography) as the most widely used algorithm.

Security experts have considered these algorithms secure because classical computers cannot efficiently solve the underlying mathematical problems that involve factoring large numbers. Classical computers find it virtually impossible to perform these calculations within reasonable timeframes. However, quantum computing significantly changes this situation. Quantum computers can perform such computations easily and efficiently, fundamentally altering the security landscape on which current cryptographic systems depend.

Quantum computers leverage the phenomena of superposition and entanglement, which enable them to calculate solutions that classical computers consider relatively impossible to solve. Large-scale quantum computers capable of running Shor's algorithm do not exist. Still, experts predict that, given the pace of advancement in this field, such systems will become a reality within just a few years.

This development would devastate digital systems worldwide. Malicious actors could leverage this algorithm to break encryption that protects data transferred or stored in digital systems, including financial records and government secrets. While some may dismiss this threat as

[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.

non-imminent and question why we should pay attention to it now, the danger extends beyond immediate data breaches.

Adversaries can encrypt and save data, then decrypt it later using quantum computing technologies. This "harvest now, decrypt later" approach means sensitive information collected today remains vulnerable to future quantum attacks. 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 later.

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

Data Security and Regulatory Frameworks:

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

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

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.

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 specific basic requirements for appropriate and secure processing and storage of personal data, they still fall short of addressing the problems posed by the use of quantum technologies. Policymakers and legal experts must now update these regulations to account for the unprecedented risks posed by quantum advancements[28].

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 re-evaluation of existing legal doctrines to accommodate this rapidly evolving field.

The Current Regulatory Frameworks:

Legal systems must adopt a proactive approach to address the challenges that the rapid evolution of quantum technologies creates. Quantum computing's disruptive potential presents significant legal challenges that lawmakers and regulators must address before these technologies mature fully.

The profound impact that quantum advancements could have on cryptography and digital security represents one of the most urgent concerns. Many current encryption protocols,

[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.

including RSA and elliptic curve cryptography, base their security on mathematical problems such as prime factorisation and discrete logarithms that classical computers struggle to solve.

However, Peter Shor's groundbreaking quantum algorithm, developed in 1994, demonstrates that a sufficiently powerful quantum computer could efficiently solve these problems. This capability would render conventional encryption methods obsolete and compromise the confidentiality of encrypted data that organisations and individuals rely upon for security.

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 concerns over algorithmic bias and flawed decision-making, leading to litigation over unfair or harmful outcomes.

As already developed throughout the paper, the primary 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 "reasonable" security may evolve.

[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.

The current data protection laws, like GDPR and the California Consumer Privacy Act[30], would provide the locus for the regulation of certain aspects of quantum technologies, like cybersecurity and data protection. Still, 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.

Quantum hardware and software create a critical synergy that enables the implementation of quantum algorithms. Superconducting qubits and ion traps provide the foundation for quantum computation, while quantum programming languages and compilers translate abstract quantum algorithms into executable instructions that hardware can process. Frameworks such as Qiskit, OpenQASM, and Q# facilitate developers' efforts to create and optimise quantum algorithms for specific hardware architectures. This dynamic interaction between quantum hardware, software, and algorithms enables researchers and practitioners to realise the full potential of quantum computing systems.

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, as well as the software enabling their functionality. Thus, even patent laws and intellectual property rights have a significant role in regulating quantum technologies.

Patent law, which protects novel, practical, and non-obvious human inventions, is particularly relevant for securing advancements in quantum hardware. Meanwhile, copyright—requiring originality, creativity, and human authorship—is better suited for software-related aspects of quantum computing. Quantum algorithms, often open source, 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.

[30] California Consumer Privacy Act (CCPA) <https://oag.ca.gov/privacy/ccpa> accessed 15 March 2025.

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 author's life plus 70 years, are considered too rigid for such a rapidly evolving field.

Although quantum technologies remain in their nascent stages of development, various international organisations and governments have already begun addressing potential governance challenges. The World Economic Forum and OECD have initiated efforts alongside governments, including the United States, the United Kingdom, Germany, and Japan, to tackle issues that these rapidly emerging technologies may pose.

The European Commission has introduced proposals that adapt intellectual property frameworks to better accommodate data science and artificial intelligence advances. These proposals signal potential shifts in how authorities will protect quantum innovations in the future.

Comparative Analysis: Different Frameworks

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

In 2018 the United States government signed the National Quantum Initiative Act into law. This legislation established a nationally coordinated program accelerating quantum research and development nationwide. Also, it allowed for effective public-private partnerships, which would contribute to a 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 has early recognised the inevitable strategic importance of quantum technologies, thereby launching several initiatives to support developments and regulations to ensure minimal damage. The European Commission called for a coordinated approach to quantum regulation and asked to develop European Quantum

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

Policy. The European Union implemented these measures to maintain a coherent framework for developing and governing emerging quantum technologies. Officials designed this approach to ensure consistent standards and practices across member states.

In 2018, the EU launched the €1 billion Quantum Flagship initiative to consolidate and expand European leadership in quantum technology. This flagship program actively addressed quantum technologies while explicitly examining their societal and ethical implications for European society.

China is also a big contender in the quantum era. The Chinese government has actively led the pursuit of quantum technology development. Officials have allocated substantial government funds and facilitated dialogue between public and private sector participants in this field. Multiple factors influence China's regulations on quantum technologies. China bases these regulations on its strategic objective to position the country at the forefront of quantum developments and maintain its competitive edge in this emerging field. There, quantum technology is a national priority, and huge investments are being made in research and development. China aims to make substantial and real breakthroughs by 2030. Until 2022, the total investments in quantum technologies in China were $15.3 billion, culminating in a National Quantum Program; this is more than the US and EU combined. China's Educational Modernisation 2035 Plan also emphasises quantum technology in education. 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 security measures in place.

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 Sensing and Metrology, Quantum Communication, and lastly, Quantum Materials and Devices.

Similarly, several other countries such as Canada[32], Japan[33] and Australia[34] have also launched

[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)

numerous initiatives to strategise and develop quantum technologies, with varying degrees of emphasis on their regulation, based on what vision they hold for their country in this quantum era.

Ethical Dimensions:

Identifying the potential ethical problems that would emerge with quantum technologies is also pertinent. Since it is set to revolutionise the technological arena completely, it would inevitably have a lot of ethical implications. By focusing on the moral 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 are nascent technologies, their development has largely limited itself to theoretical dimensions, and they are often influenced by a strong rhetoric of revolutionising the future of technologies. However, quantum technologies can be used as an umbrella term for a range of emerging technologies, which are very different from each other but have powerful impacts in all dimensions.

Interestingly, while there are many discussions and discourses around quantum regulations and strategies, there is no focus on specific ethical problems. In the UK and EU midterm reports on quantum strategy, terms like 'ethics' and 'morals' did not appear. An essential facet of this discussion is that there would be a massive imbalance between populations with advanced quantum technologies and those without them. As already explained, there would be a new definition of privacy in the quantum age, given that encryption would change drastically.

Additionally, in 2022, the US National Security Memorandum published a report stating that to cope with the risk posed by quantum cryptography, it must promote collaborations with overseas allies, in education and professional aspects. This international engagement would be essential in identifying risks and inculcating diverse perspectives on quantum security and protection[35].

<https://www.industry.gov.au/sites/default/files/2023-05/national-quantum-strategy.pdf> accessed 20 March 2025.

[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.

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

One way around it is to inculcate RRI as already described above. RRI helps facilitate public dialogues, envisages involvement of parliaments, and allows for input from all relevant stakeholders. Given the stochastic nature of the quantum computational system, it is crucial 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, showed that a quantum computer can easily solve several computational problems. This essentially meant that anyone with a real-world quantum computer could easily break the cryptographic codes, thus compromising the encrypted communications.

At the confluence of this problem is the ethical dimension of security versus 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 about governmental paternalism and diminishing privacy and autonomy rights.

Ethics and law are 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 good balance between them in an ever-changing and rapidly advancing technological landscape.

[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.

Where does India stand on all of this?

On April 19th, 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 2023-2031. With this, India aims to harness the power of quantum technology to drive innovation and position itself as a cutting-edge global leader.

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

As a part of this mission, four Thematic Hubs have been chosen (T-hubs)[37], which bring together 14 Technical groups across 17 states and 2 Union territories. The focus will be on technology innovation, skill development, industry partnerships, and fostering a global collaborative space to ensure a national impact. An essential feature of these T-hubs is that they will work on a Hub-Spoke-Spike Model, which will encourage a cluster-based network. It will focus on a collaborative ecosystem involving 152 researchers from 43 different institutions nationwide[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 the Quantum Computing Applications Lab, which the Ministry of Electronics and Information Technology leads. This lab supports India's aspirations to create a thriving quantum research hub.

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

[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.

work closely with the Department of Telecommunications and the 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, the private sector and the evolving startup ecosystem. This has also been an insight of Niti Aayog, which was published in the March 2025 edition of Future Front[40].

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 significant threat to 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. The quantum ecosystem thrives on strong government funding and a dynamic private sector in the US. This is something that 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 new platforms like silicon spin or topological qubits have the potential to shorten the quantum timeline; hence, we need to be prepared in advance.

The emphasis should be on fostering cooperation between various stakeholders, like industry, academia, civil society, etc. International cooperation produces innovation but mitigates risks and emphasises adaptability.

[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).

Conclusion:

As we stand at the threshold of a new era in science and technology, the quantum revolution presents an extraordinary opportunity and a formidable challenge. The year 2025, marking a century since the birth of quantum mechanics, has been symbolically recognised by the United Nations and 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. Therefore, there is a 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 the creation of flexible, principles-based frameworks that can adapt 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. However, for India to emerge as a serious global player, it must also invest in developing legal, ethical and policy ecosystems.

This paper has explored the 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 law but aims to keep pace with technological change and 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 not shocked by quantum theory has not understood it".