Master of Science in Law, Digital Innovation and Sustainability

Department of Law

Course of Data Protection Law

RESPONSIBLE QUANTUM TECHNOLOGIES:

A REGULATORY ROADMAP

Prof. Filiberto E. Brozzetti

SUPERVISOR

Prof. Giuseppe D'Acquisto

CO-SUPERVISOR

Margarita Borodavina

630543

CANDIDATE

Academic Year 2022/2023

I. Introduction

Quantum technologies stand as an extraordinary and unparalleled innovation that has captured the attention of the world. Its potential to revolutionize industries and solve complex problems with unprecedented speed has sparked a race among leading nations to achieve quantum supremacy. However, as this technology advances, it brings forth a host of legal, ethical, and security concerns that require careful consideration. In this article, we delve into the distinctive realm of quantum computing, scrutinizing legal, social, political and ethical isuues it entails today.

It can be tempting to begin discussions of qubits vs bits, the mysterious collapse of the wave function, or the infamous Schrödinger's Cat paradox when exploring the world of quantum computers. Undoubtedly, thorough regulation requires a thorough understanding of the properties of quantum computers. However, to grasp the broader legal ramifications, it is sufficient to understand such fundamental quantum features as principles of superposition, entanglement, and interference that set them apart from classical comuters. Quantum superposition is a fundamental principle of quantum mechanics. In classical mechanics, things like position or momentum are always well-defined. We may not know what they are at any given time, but that is an issue of our understanding and not the physical system. In quantum mechanics, a particle can be in a superposition of different states. However, a measurement always finds it in one state, but before and after the measurement, it interacts in ways that can only be explained by having a superposition of different states. Entanglement, another pivotal concept, emerges when quantum particles become intimately linked in a way that the state of one particle instantly influences the state of another, even when they are separated by vast distances. This phenomenon, often described as "spooky action at a distance"[1] by Einstein, has profound implications for quantum information, communication, and cryptography.Furthermore, quantum interference, a consequence of the wave-like nature of quantum particles, occurs when probabilities of different outcomes interact and combine. This results in intricate patterns of behavior that classical systems cannot replicate. Quantum algorithms harness interference to achieve computational tasks more efficiently than classical computers in some cases.[2] QT has potentiality to change political agendas, economic sectors and social institutions due to their computational power. They can greatly increase speed of

[1] Hossenfelder, S. (2021). "Einstein's Spooky Action at a Distance." Link
[2] Heisenberg, Werner. "The Physical Principles of the Quantum Theory." Dover Publications, 1949. Link

operations and perform tasks that are impossible for conventional computers, resulting in breakthroughs in a spectrum of domains, including but not limited to cryptographic systems, pharmaceutical research, materials engineering, and meteorological forecasting. Industries benefit from quantum optimizations, including energy grids, supply chain logistics, and financial modeling, enhancing efficiency and precision. Moreover, quantum sensors improve aircraft navigation, climate modeling, environmental monitoring, and space exploration. Quantum machine learning empowers artificial intelligence applications, while quantum communication networks bolster cybersecurity. Quantum technologies are a crucial area of research with broad ramifications for the globe since they have the potential to alter industries, increase efficiency, and handle difficult global concerns.

The research question which is adressed in this study is "How can existing regulatory frameworks be adapted to address the unique characteristics and capabilities of quantum technologies?" It stands as a pivotal inquiry in the rapidly evolving realm of emerging technologies regulation. Quantum inventions, with its unprecedented computational powers and transformative potential, challenges conventional regulatory paradigms. This question underscores the nesseccity of exploring new regulatory approaches and harmonizing established regulations with the fast developing innovations. As quantum technology permeates various sectors, including finance, healthcare, public administration and many others, understanding how to adapt regulatory frameworks becomes essential to ensure responsible and secure integration. This research question serves as a crucial entry point for exploring the dynamic landscape of quantum computing governance, shedding light on strategies to harness its immense potential while effectively addressing the novel challenges it presents.

This thesis makes a significant contribution to advancing the objectives of regulating quantum technologies by offering a comprehensive and innovative approach. It addresses the goals set by European authorities to create innovative and flexible legal frameworks, undergo the transition to post-quantum security measures, and review fundamental principles of regulation in the quantum technology domain. The Quantum Flagship initiative[3] was introduced by the European Commission in 2018 as an important and extensive research project. Its effort intends to strengthen European leadership and expertise in quantum

[3] "Quantum Technologies Flagship." *Digital Strategy - European Commission*. Link

technology research while providing substantial funding for the development of a competitive quantum technology economy in Europe. Additionally, the promotion of quantum technology and infrastructure development were set as central goals of the 2030 Path to the Digital Decade policy program.[4] Quantum technologies are progressing towards greater technological maturity and broader adoption. Thus, one of the strategies identified by the Quantum Flagship in its Strategic Research Agenda to accelerate development and adoption is the promotion of well-coordinated and specialized regulation efforts. European regulation in this context are evolving through the efforts of organizations like CEN & CENELEC, ENISA and ETSI. For the Quantum Technologies domain regulation is not only about requirements setting a basis for certification, but can also address quality benchmarks, cybersecurity an compliance with european legislature. By advocating innovative approach in this regard, the thesis aims to facilitate the accelerated development and widespread adoption of quantum technologies. Through its insights, this thesis contributes to shaping the regulatory landscape for quantum technologies, promoting their secure and effective integration into various industries, and ultimately contributing to the realization of their full potential.

This thesis examines the legal aspects associated with quantum technologies, highlighting their intricate and rapidly changing nature. We delve into several key legal issues, including intellectual property rights, data protection, and the emerging field of quantum law.

Furthermore, this research provides an overview of the present status of the standardization efforts in Post-Quantum Cryptography (PQC). We explore the digital transformation occurring in society during the quantum era and emphasize the necessity of PQC to address the security challenges posed by these advancements. It presents an evaluation of the various proposals within the key categories of PQC algorithms. Additionally, it suggests the strategy for enforsing a secure quantum future by introducing a roadmap for the integration and adoption of PQC measures.

This research proposes a framework for Responsible Quantum Technologies (RQT) which includes legal, ethical, social, and political concerns in quantum research and development. The proposed regulatory framework aims to become a starting point for further development, at this early stage while quantum technologies are still adaptive and developing. It needs to be

[4] "Quantum Technologies - RP2023." Rolling Plan ICT Standardisation - *Joinup - European Commission.* Link

considered as a specific methodological framework designed for the characteristics of quantum technology. The primary aim is to create a regulatory sandboxes for QT that encompasses a meticulous review of legal principles while also instilling measures to effectively ensure the necessary level of cybersecurity. This initiative seeks to engage a diverse spectrum of stakeholders, ranging from scientists and researchers to industry leaders and policymakers, fostering a collaborative environment for the development and implementation of QT regulations. It is important to establish a base for responsible QT, to ensure that the evolution of QT remains ethically sound, humancentric, and aligned with global norms.

II. Literature Review and Methodology

The methodology employed for crafting the article is grounded in a multifaceted approach that combines extensive literature review, expert interviews, and comparative analysis. To begin with, an exhaustive review of existing literature on quantum technologies and their regulation was conducted. A thorough examination of academic papers, legal documents, government reports, and industry publications has been done to identify key trends, challenges, and best practices in the field. The domain of quantum technologies has advanced significantly since its inception at the beginning of the 20th century. First scientists such as Albert Einstein, Niels Bohr and Erwin Schrödinger set the basis for quantum mechanics, which has since paved the way for quantum technologies. Understanding the practical apllication of quantum technologies helps to contextualise the current regulatory landscape. Thus, quantum technologies are comprehensively examined in this article, encompassing an exploration of the key facets that underpin a responsible approach to their utilization. In order to analyze the application and regulation of technologies, a thorough understanding of the technical aspects is imperative. Numerous scientists have delved into the study of quantum phisics. Among these researchers, the following names stand out: Antipenko L., Arshinov V., Bargatin I., Bell D., Bennett C., Bohr N., de Broglie L., Born M., Dirac P., Heisenberg W., Pauli W., Schrödinger E., Feynman R., Planck M. Belenchia, A.; Browne, D., Carlesso, M.;Valiev K., Gilbert J., Gorchevich A., Grib A., Dirac P.A.M., Doronin I., Kadomtsev B., Kilin S., Kitaev A., Korolkov A., Krasavin V., von Neumann I., Pilan A., Popov M.A., Stix G., Syaesk I., Horgan D., Chavchanidze V, .Zhang, Q. Their collective contributions have significantly advanced our understanding of quantum information theory.

Furthermore, a comprehensive examination of the technical aspects of quantum cryptography was conducted by studying the works of various experts, including Olejnik, L., Riemann, R., Mansoor Farooq, Rafi khan, Mubashir Hassan Khan, Chunfeng Zhang, Gang SuGuoyi, Huang Wang J., Csenkey K., Bindel N., Paul B., Trivedi G., Li Z., Pan F., Wang X., Massmann R., Grantham N., Mailewa A. In addition, representatives from public agencies have been actively involved in the development of strategies and recommendations for the implementation of PQC, including Beullens W., D'Anvers J.-P., Hülsing A., Lange T., Panny L., de Saint Guilhem C., Smart N., Basu K., Soni D., Nabeel M., Karri R. Researchers have explored the development of post-quantum cryptographic algorithms to safeguard sensitive information. The regulatory challenge here lies in implementing these new cryptographic standards across industries and ensuring compliance.

In the endeavor to craft a foundation for future legal frameworks, it became imperative to delve into the realm of legal research, specifically focusing on articles examing potential regulations that could be applicable to quantum technologies. As of today, quantum technologies are at the forefront of the global legal community's attention. Numerous studies have been published by representatives of the legal studies. Notably, researchers are actively developing the concept of quantum computational law (Atik, J.; Ritter, J.) and the ethics of quantum technologies (Jeutner, V.). There are also scholars investigating pressing issues of applicable property and non-property rights (Deltorn, J., Franck M. Lemley, Mark A., Drexl, J., Gervai, D., Derclaye, E., Goldstein, Paul, and Bernt Hugenholtz, Menell, Peter S., Mark A. Lemley, Robert P. Merges, Huang, Y., Lake, R., Simbierowicz, S.) and establishing the foundations of legal regulation for these technologies, particularly addressing the nuances of their regulation in the contemporary context (Kop, M.; Holodnaya, E.; Dobrobaba, M.; Naumov, V.).

Additionally, interviews were conducted with experts in quantum technology, law, and policy to gain valuable insights and perspectives. These interviews provided firsthand knowledge and allowed for a deeper understanding of the nuances surrounding quantum technology regulation. Proposals made in this thesis provide empirical insights into the implementation and impact of regulatory frameworks in the field of quantum technologies. They were based on in-depth analysis of existing quantum technology regulations and policies from various jurisdictions worldwide. Last but not least, we suggest experimental regulatory models to simulate the application of proposed regulatory frameworks and assess their impact on

quantum technology development and commercialization. This experimental phase provides valuable insights into the practical implications of regulatory decisions. Through a combination of these research methods, our methodology ensures a robust and data-driven exploration of the Quantum Technologies Regulatory Roadmap, offering practical recommendations for policymakers and stakeholders in the field.

By integrating these research methods, this thesis ensures a comprehensive and well-informed exploration of the quantum technologies regulatory landscape. The deep analysis of litrature undertaken throughout this study has proven instrumental in shaping a holistic perspective of the research field. By diligently examining a wide range of relevant factors and sources, a deeper understanding of the subject matter was gained, allowing to form a more comprehensive and well-informed view. This holistic view serves as a solid foundation for further research and the development of effective strategies and frameworks in the field of quantum technologies regulatory roadmap.

III. Overview of Quantum Technology Regulatory Dynamics

The legal framework governing the development, deployment, and use of quantum technologies is a critical aspect of the rapidly evolving quantum technology landscape. With its extraordinary potential to revolutionize fields as diverse as computing, cryptography, communications, and sensing, quantum technology has sparked a global race to harness its power. However, this transformative power poses a range of complex regulatory issues, from security concerns to intellectual property rights, ethical considerations, and international cooperation. This chapter delves into the complicated field of regulatory policies regarding quantum technology and observes the existing legal practices.

European Union

Within the European Union's dynamic landscape of quantum technology development, the Quantum Flagship stands as an initiative, taking flight in 2018 with a clear mission: to propel Europe into a position of global leadership in the realm of quantum technology. As an integral component of the Horizon 2020 program[5], it commands a budget exceeding one

[5] "Horizon 2020 - Funding Programmes and Open Calls." *European Commission - Research and Innovation,* Link

billion euros.[6] The Quantum Flagship's vision is broad and all-encompassing, with a specific emphasis on quantum computing, communication, simulation, and sensing. It serves as an incubator for a multitude of research endeavors, accommodating a spectrum of research levels, from the fundamental to the practical. It seeks to cultivate a vibrant and sustainable quantum technology ecosystem within Europe. This holistic approach includes the establishment of cutting-edge research centers, the cultivation of a highly skilled workforce in the field of quantum, and the creation of supportive policies that will pave the way for quantum technology's seamless integration into society.

Additionally, the pursuit of quantum technologies and the establishment of robust infrastructures stand as pivotal objectives within the 2030 Path to the Digital Decade policy program.[7] The European Commission has placed a specific and ambitious goal on the horizon: by 2025, the European Union aims to have its inaugural quantum-accelerated computer in operation, marking the commencement of a journey towards quantum capabilities that will position Europe at the forefront by 2030. To ensure the realization of this objective, the Commission has proposed the initiation of collaborative, multi-country projects in partnership with Member States. These projects will operate under the umbrella of the newly created European Digital Infrastructure Consortium (EDICs) designed to facilitate the harmonious development of digital initiatives across borders.

Standardization plays a pivotal role in fostering the expansion of emerging technologies and the establishment of streamlined and robust supply chains. Therefore, as underscored in the assessment conducted by the CEN-CENELEC focus group on Quantum Technology,[8] with quantum technologies maturing, it is now opportune to initiate contemplation regarding additional requirements for standardization.

In June 2019, a significant milestone was reached as Member States collectively signed the European Quantum Communication Infrastructure Declaration[9] which will enforce a secure quantum communication infrastructure spanning the whole EU, including its overseas

---

[6] "Quantum Technologies Flagship." *Digital Strategy - European Commission*. Link
[7] "Proposal for a Decision establishing the 2030 Policy Programme - Path to the Digital Decade." *Shaping Europe's digital future - European Commission*. Link
[8] "Standardization Roadmap on Quantum Technologies." *CEN-CENELEC Focus Group on Quantum Technologies*, 2023, Link
[9] "The European Quantum Communication Infrastructure Initiative." *Shaping Europe's digital future - European Commission*. Link

territories. Moreover, The European Parliament and Council, with Regulation (EU) 2021/821 enacted on 20 May 2021, introduced partial export regulations for quantum technology.[10]

This legislative moves signifies Europe's proactive stance in navigating the complexities of this burgeoning field.

USA

As the utilization of quantum computing technology experiences a surge in prominence, both the United States government and relevant authorities have initiated the foundational steps necessary for crafting a legal framework to govern this transformative technology. In response to mounting concerns regarding accountability within the quantum computing realm, the United States has introduced novel legislation aimed at providing support and protection to individuals who may potentially become victims of cybersecurity breaches stemming from the application of quantum computing.

To date, a total of forty-five U.S. states and Puerto Rico have set forth more than 250 resolutions and bills addressing the intricate landscape of cybersecurity risks. These proposed laws encompass a range of proactive measures, including the establishment of task forces dedicated to advising and researching cybersecurity challenges. Furthermore, they entail directives mandating government agencies to undertake cybersecurity training, implement formal security policies, adhere to established standards and practices, and strategize and test their response mechanisms for potential security incidents. These concerted efforts underscore the commitment to safeguarding the digital landscape amidst the quantum computing revolution.[11]

In response to the absence of a federal standard governing the reporting of cybersecurity breaches, a group of Senators has collaborated on a bill designed to compel both public and private institutions to promptly notify the government within a 24-hour window following a breach.[12] This initiative aims to enhance transparency and accountability in the cybersecurity landscape.

---

[10] "Regulation (EU) 2021/694 of the European Parliament and of the Council establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240." *Official Journal of the European Union.* Link
[11] "Cybersecurity Legislation in 2021." *National Conference of State Legislatures (NCSL)*. Link
[12] "Executive Order on Improving the Nation's Cybersecurity." *The White House*. Link

The United States government has also expressed a deep-seated concern regarding the need to formulate encryption methods that are resilient in the face of quantum computing advancements. In pursuit of this objective, the National Security Agency and the National Institute of Standards and Technology (NIST) have been called upon to address these intricate challenges.

Furthermore, at the federal level, a framework has been established to foster and advance quantum computing technology, known as the National Quantum Initiative Act (NQIA). These pivotal measures and developments represent significant steps forward, but it is imperative to recognize that further actions must be undertaken to safeguard the rights of creators and users in this evolving landscape.

China

China has demonstrated a robust commitment to regulating the realm of quantum computing, underpinned by substantial investments in its development. The government has strategically crafted policies that not only promote the advancement of quantum technology but also incentivize research and development investments. Tax incentives have been extended to companies with a quantum-focused agenda, fostering a conducive environment for quantum innovation to thrive.

In parallel, China has established a multitude of dedicated quantum research institutes, underscoring its dedication to pushing the boundaries of quantum knowledge. Moreover, the nation has embarked on ambitious quantum communication and cryptography projects, further solidifying its standing in the quantum domain. In a bid to ensure technical rigor and reliability, China has also instituted precise technical standards, notably in the domains of quantum key distribution and communication.

On the front of cybersecurity, the Chinese government has placed a premium on secure quantum communication networks. This commitment is evident through initiatives aimed at the development of cryptographic algorithms and the establishment of secure quantum key distribution systems. These measures are pivotal in safeguarding critical digital infrastructure.

Crucially, China's overarching national strategies, such as the "Made in China 2025"[13] plan and the current 14th five-year plan for social-economic development (2021–2025), have

[13] "Made in China 2025: Plan to Dominate Manufacturing." *FDIChina.* Link

underscored the importance of achieving "large breakthroughs" in the realm of quantum technologies. These strategic roadmaps solidify China's resolve to remain at the forefront of the quantum revolution and assert its leadership in this transformative field.

Russian Federation

The advancement of quantum technologies holds a prominent position in Russia's quest for scientific and technological progress, aligning with the overarching goals outlined in the Strategy of National Security of the Russian Federation.[14] One of the key vehicles driving this progress is the "Digital Economy" federal target program, which places a strategic emphasis on fostering a diverse range of technologies. This program includes the "Quantum Technologies" Roadmap which casts a focused spotlight on quantum computation, quantum sensors and metrology, as well as quantum cryptography. The Roadmap serves as a comprehensive blueprint, delineating the essential milestones and steps required to propel these quantum technologies forward within Russia. It is a well-structured strategy encompassing research initiatives, infrastructure projects, and organizational activities, all designed to fortify sub-technologies crucial to national security and digital sovereignty. This roadmap extends to the formulation of standards for quantum communications and the Internet of Things.[15]

In tandem with these strategic endeavors, Russia is actively engaged in the development of national standards for products rooted in quantum technologies. National standards GOST R 58568-2019[16] and GOST R 57257-2016/ISO/TS 80004-12:2019[17] have already been approved, providing crucial regulatory frameworks for quantum technology-based products.

Other countries worldwide are also actively pursuing quantum technology initiatives to drive scientific progress and secure their positions in the ever-evolving landscape of quantum advancements.

---

[14] "National Security Strategy of the Russian Federation dated July 02, 2021." Ministry of Foreign Affairs of the Russian Federation, Link

[15] "Quantum technologies Roadmap for developing the "end-to-end" digital technology." *Ministry of Digital Development, Communications and Mass Media of the Russian Federation* Link

[16] "GOST R 58568-2019 Optics and photonics. Photonics. Terms and definitions." *Federal Agency for Technical Regulation and Metrology* Link

[17] "GOST R 57257-2016 Nanotechnologies. Part 12. Quantum phenomena. Terms and definitions." *Federal Agency for Technical Regulation and Metrology* Link

In the United Kingdom, the National Quantum Technologies Programme (NQTP) was established in 2014 with a clear mission: to position the nation as a global leader in quantum technology development and commercialization. A pivotal moment arrived in 2020 when the NQTP published its "Strategic Intent," outlining a visionary path for the country's economic growth, heavily reliant on the integration of quantum technologies.

Canada, on the other hand, has allocated a substantial $360 million for the development of its National Quantum Strategy. This strategic investment is geared towards bolstering the thriving quantum industry within Canada and ensuring the cultivation of a skilled workforce, ultimately reinforcing the nation's global prominence in the quantum technology sphere.[18]

Meanwhile, the Commonwealth of Australia is determined to harness the economic potential of quantum technologies. To achieve this, Australia has established a Quantum Commercialization Center, a critical initiative aimed at fostering the commercialization of quantum research and the growth of quantum-focused businesses.[19]

In the Republic of Singapore, the focus lies on establishing a National Quantum-Safe Network (NQSN).[20] This network will actively test commercial quantum technologies in both public agencies and private enterprises, conduct thorough safety assessments, and offer guidelines to facilitate the seamless integration of these technologies. The government has earmarked 8.5 million Singapore dollars over three years to support this endeavor.

South Korea is also making substantial strides in quantum technology development. In 2019, the nation approved a comprehensive Quantum Computing Development Plan, spanning five years, to advance fundamental quantum technologies, including quantum hardware and prospective innovations in quantum algorithms and software. The ultimate aim of this plan is to design a stable 5-qubit quantum computer. South Korea has further fortified its commitment to quantum technology by adopting a comprehensive 5-year plan dedicated to continued quantum technology development.[21]

These global initiatives collectively underline a shared commitment to unlocking the potential of quantum technologies. Each nation is strategically positioning itself to not only

---

[18] "Canada's National Quantum Strategy." *Government of Canada.* Link
[19] "Australian National Quantum Strategy." *Australian Government, Department of Industry, Science and Resources.* Link
[20] "National Quantum-Safe Network." *Centre for Quantum Technologies (CQT).* Link
[21] "Strategic Planning on the Quantum Science and Technology R&D." Quantum in Korea. *Link*

lead in scientific advancements but also to promote regulatory initiatives in this transformative field.

IV. The Need for Regulation

Quantum Computing in the Modern Era: A Look at Recent Progress and Complexities

In light of impending technological advancements, we find ourselves at a pivotal moment with the opportunity to proactively regulate before these changes fully unfold. However, it's concerning to observe a lack of significant steps among regulators and policymakers in response to this looming transformation. Historically, the legal sphere has often adopted a reactive stance, waiting for developments to occur before instituting regulations post facto. But the quick spread of QT into various areas of life emphasizes how urgent it is to take a more proactive approach. Although QT is still in its infancy, it already has the power to change a wide range of industries. Recent advances in quantum computing include the following:

1. Quantum hardware: Advancements in quantum hardware, including the development of more stable and scalable quantum systems. Progress in quantum algorithms and software, making it possible to perform increasingly complex quantum computations.[22]
2. Quantum cryptography: In the future, quantum technology may provide fundamentally secure encryption techniques that will help safeguard sensitive data from risks posed by quantum computers.[23]
3. AI and Machine learning: The ability to solve complex problems that are beyond the capabilities of conventional computers may result from this integration, which may also improve model training and increase processing efficiency.[24]
4. Quantum simulation: Although tough for classical computers, quantum computers can simulate quantum systems. Materials science, drug discovery, and the comprehension of basic physical events can all benefit from this.

---

[22] Montanaro, A. "Quantum Algorithms: An Overview." Npj Quantum Information, vol. 2, no. 1, 2016. Link
[23] Olejnik, L., & Riemann, R. "Quantum Computing and Cryptography." (2020). Link
[24] Matteo M. Wauters, Emanuele Panizon, Glen B. Mbeng, and Giuseppe E. Santoro. "Reinforcement-learning-assisted quantum optimization." (2020). Link

5. Quantum Internet: The creation of a quantum internet would make it possible to communicate securely and instantaneously over great distances, opening the door for cutting-edge uses in distributed quantum computing and other fields.
6. Energy: The design and management of renewable energy systems can be optimized using quantum computing, which might help reduce energy waste and boost effectiveness.[25]
7. Data processing optimization and modeling: Data processing and modeling[26] could benefit greatly from quantum computing in a number of ways.

These are just a few of the areas where quantum technologies have the potential to bring about significant advancements. However, they also bring a number of ethical, political, and social issues that pose difficulties that must be resolved. Here are some of the aspects regarding quantum technologies:

1. Security and Cryptography: A serious threat to data security and privacy is the ability of quantum computers to break many of the encryption protocols currently in use.
2. Privacy and Quantum Surveillance: Quantum sensors and communication technologies may increase surveillance capabilities, and raise concerns about privacy and excessive government interference. Ethical issues are related to the appropriateness of using quantum technologies for surveillance and the need for strong legal safeguards.
3. Data Security and Trust: Quantum technologies have the potential to create new security challenges. The problem is the inability to trust quantum systems due to lack of transparency, the difficulty in ensuring their reliability, and addressing concerns about potential vulnerabilities.
4. Intellectual Property Rights: The development of quantum technologies may lead to the emergence of complex legal disputes concerning IP rights. The actual problem is to ensure fair access to intellectual property and to prevent monopolism.
5. Liability and responsibility: As quantum computing becomes more widespread, questions may arise about who is responsible in the event of errors or failures. There may also be questions about the use of quantum computing for decision-making, for example

[25] "Quantum Computing: Progress and Prospects." *National Academies of Sciences, Engineering, and Medicine.* (2019). Link
[26] Feynman, R. P. "Simulating physics with computers." *International Journal of Theoretical Physics*, vol. 21, 1982, pp. 467-488.

in employment, finance or criminal justice, and the possibility of algorithmic bias and discrimination.

6. Dual-Use Applications: Quantum technologies can have both civilian and military applications. Legal frameworks need to be developed to use these technologies for the benefit of society and to minimize potential harm. The development of quantum technologies for military purposes, such as quantum cryptography and quantum radar, raises concerns about the potential for an arms race and destabilizing effects on global security.
7. International Collaboration: The development and regulation of quantum technologies requires international cooperation. It is necessary to create conditions for cooperation, equitable distribution of this resource and prevention of competitive arms race.
8. Environmental Impact: Quantum computers require specialized cooling systems that can be energy intensive. Concerns arise over the environmental impact of quantum technologies and the need for energy efficient solutions.
9. Access and Distribution: If quantum technologies are not distributed equitably, there is a possibility that they will exacerbate existing inequalities. Preventing the digital divide and ensuring equal access to the benefits of quantum breakthroughs are ethical requirements.

Quantum technologies are bringing positive transformative changes to all the fields of our lives. At the same time, they pose ethical, legal, political, and social challenges that require careful consideration and proactive measures to ensure that they are developed and used in ways that benefit society while minimizing harm. Legal frameworks, regulations, and international cooperation will play critical roles in addressing these concerns.

Digital Transformation in the Quantum Age through the Social Prism

This dynamic interaction between law and technology is often portrayed as a dialectical system, yet it tends to overlook the crucial role played by society. It's imperative to recognize that it's not just laws and society that are undergoing transformation; society's approach to and acceptance of technological changes are also evolving. This societal shift is occurring at a pace even swifter than legislative developments, making it a critical factor in shaping our technological future. The paternalistic approach that policymakers have historically taken toward consumers and users of technologies is now being overcome by those consumers.

Users are increasingly taking proactive measures to mitigate risks. In essence, users are becoming autonomous regulators. In a quest for a deeper understanding of the technological impact on law and society, we had the distinct privilege of conducting an interview with Professor Derrick de Kerckhove. As the distinguished Director of the McLuhan Program in Culture & Technology, Professor de Kerckhove brings to the table a wealth of knowledge and extensive experience in the field. During our conversation, he expounded upon his theory of operating systems, shedding light on how innovations have the capacity to infiltrate and transform the very foundations of society. While much scholarly attention is directed toward the legislative aspect of regulating technologies, Professor de Kerckhove emphasized the often-underestimated role of technologies as a regulatory force. He posited that, even in the absence of explicit laws, technologies themselves act as a regulator, shaping our interactions and choices within the digital landscape. This notion prompts a broader understanding that human and institutional behavior is never truly unregulated. In the absence of legal regulations, alternative regulators naturally fill this gap.

Professor De Kerckhove discusses that even if there is a general economic and legal tendency to use technology to objectify human experiences, there is a dialectical space between data and practices. Similar to how the law artificially creates rights by dividing human actions, technology turns a public asset into a limited resource. Indeed, technology is pivotal in creating resources: as Hess and Ostrom explain, "this ability of technology to capture the previously uncapturable creates a fundamental change in the nature of the resource, with the resource being converted from a nonrivalrous, nonexclusive public good into a common-pool resource that needs to be managed, monitored, and protected, to ensure sustainability and preservation."[27] Considering the impact of technologies on the social structure, and its' instruments of governance Professor provides a quote of de Angelis: "...the origin of commons rights is in commoning, we are in the presence of a social system generated by its own operations, codes and values."[28] This statement highlights a fundamental concept in the context of commons and commoning. It asserts that it is the practice of 'commoning', the collective and participatory management or use of these resources, that gives rise to the rights associated with commons (shared resources or spaces). That is, the existence of the commons itself is preceded by the process of commoning, in which people collectively engage with and

[27] Hess, C., & Ostrom, E. (Eds.). Understanding knowledge as a commons: From theory to practice. MIT Press, 2007. Link
[28] De Angelis, M. Omnia Sunt Communia. On the Commons and the Transformation to Postcapitalism. (2017). Link

manage a resource. In other words, the idea and concept of the commons arises from the act of people coming together and collectively managing or using a resource (commoning). This undermines the traditional understanding of commons as pre-existing and commoning as a way of managing them. Rather, it is argued that commons are a product of the ongoing social process of commoning, where social groups actively form and determine their distributed resources through their actions, rules, and values. Professor De Kerckhove argues that by analogy with the concept of commoning technologies create and seize a resource where before there was none.

Besides resources, technologies form our way of communication and modes of interaction. In turn, society's evolving needs and values drive the development of new communication technologies. This dynamic interplay between communication, society, and technologies has led to transformative shifts in our social structures, behaviors, and norms. Language is the principal social instrument of human communication. However, in the era of digital transformation, we are witnessing a profound evolution of language dynamics. The advent of language AI models, driven by advanced machine learning and natural language processing, is revolutionizing the way we communicate, share information, and conduct business. These AI models, such as GPT, have the capacity to generate human-like text and comprehend context, making them powerful tools for content creation, translation, and even conversation. While this technology presents immense opportunities for efficiency and accessibility, it also raises critical questions about the responsibility for the outcomes of algorithms. As AI models increasingly take on roles in content generation and decision-making, the ethical and legal implications of this transition come to the forefront. Issues of accountability, transparency, and bias become central concerns. Even more serious issues raise the integration of language AI models with quantum technologies. What’s the future of the concept of responsibility at a time when the production of language is moving away from the responsibility of the person to the responsibility of the machine? In an era where machines are progressively assuming decision-making roles, the concept of responsibility undergoes a profound transformation. As owners and representatives of our words and choices, we are accustomed to bearing the ethical and cognitive weight of our actions. Professor De Kerckhove stated, "In fact, one of the most profound impacts of the digital ecology (as well as, I suspect, the emerging quantum ecology, though we don't yet know in what form), is and will be in law." The digital transformation has indeed brought about significant changes in the way individual accountability and responsibility are perceived and implemented. In recent years, the legal

field has witnessed a remarkable shift driven by rapid technological advancements with AI integration in law. In the near future, we can expect the same introduction of quantum technologies into this field. These innovations are not just changing the way legal professionals work, they are empowering lawyers with new decision-making tools. The encroaching influence of machines and AI systems raises complex questions regarding where the boundaries of responsibility lie. As these systems make decisions on our behalf, we grapple with a profound ethical and cognitive challenge — how do we assign and manage responsibility in a world where machines have a hand in shaping our choices? This shift forces us to grapple with not only the ethical implications of delegating responsibility to machines but also the cognitive challenge of determining accountability in an age where human and artificial intelligence intersect. The quantum ecology will require people to make sense of the fact that the human factor is just one component of the whole system, certainly not the master.[29]

Another question of interest posed by Professor De Kerckhove is: "Could we say, that interfacing devices have not only technical but also social by default and materialize a certain worldview/world-feel/world-performance?" It seems logical statement, that technology serves not only as a digital tool but also as an effective communicative, economic amd political instrument, changing the way of social interaction and public administration. Computers process information in a similar way all around the world, it can lead to people from different places having similar ways of thinking, that is to epistemological convergence of global social consciousness and global networkedness. At the same time, if we consider it objectively, we can conclude that there are significant differences between digital communities, and these differences are based on the types of platforms and algorithms that are popular in these communities. Additionally, we see various approaches to the governance of these technologies and data flows. Indeed, there are distinct approaches to data governance that can be broadly categorized as Asian and Western, each influenced by the cultural, legal, and economic contexts of their respective regions. We refer to the General Data Protection Regulation (GDPR) as representative of the Western approach and the Social Credit System (SCS) as representative of the Asian approach to data governance. GDPR is based on principles of personal consent, awareness, and resistance to behavior modification driven by commercial interests. It reflects Western Europe's individualistic statecraft rooted in

[29] Calzati, S. "Shaping a Data Commoning Polity: Prospects and Challenges of a European Digital Sovereignty." Link

Enlightenment philosophy, aiming to redefine the individual's relationship with the digital realm to safeguard personal autonomy and agency. Fundamentally, GDPR is seeking to define the relationship between the individual and the digital in a way that protects personal autonomy and agency. SCS acknowledges the potential for behavior modification but uses it as a tool to foster "social harmony."[30] It achieves this by monitoring and evaluating citizens' actions through individual credit ratings, which are linked to social rewards and penalties. This approach diverges from GDPR in several significant aspects concerning the concept of the individual. The economic ambition of the CPC's social credit system is clear – it is to be the powerhouse for growth.[31] China needs to shift its economy from export-oriented to one centered on consumption and quality, focusing on sustainability and sensible economic strategies. SCS is designed to facilitate an economy driven by extensive data collection, machine learning algorithms, and real-time cybernetic feedback and adjustment. In this context, big data and its analytics serve as primary tools for economic progress. While GDPR aims to harmonize data laws within the EU for a more efficient single market. However, concerns exist about its impact on innovation in big data and AI.[32] Some experts suggest it could drive tech firms to invest in countries like the US with less regulation. Thus, we observe a reciprocal relationship between technology and society, where advancements in technology shape and influence societal norms, behaviors, and structures, while concurrently, societal needs and values drive the development and adoption of new technologies. Understanding these mutual effects is essential for navigating the evolving landscape of the digital age and ensuring that technological innovations align with societal well-being and ethical considerations. "Understanding how digital transformation has shaped the current landscape can serve as a foundation for making informed predictions about the potential impacts of quantum technologies," said Professor De Kerckhove, "since currently most platforms and algorithms are developed and implemented by big international tech companies, the issue at stake becomes one of transnational techno-cultural fields, rather than "traditional" geopolitical ones (at least in the Westphalian sense of the term)." Certainly digital trasformation has laid the ground for quantum technologies to harness the datafield, it will always be a matter of data, and, without doubts, we can identify entanglement and uncertainty as two key principles of quantum ecology's OS.

---

[30] Aho, B., & Duffield, R. "Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China." Economy and Society, 49, 1-26. Link

[31] Nederveen Pieterse, J. "China's contingencies and globalization." Third World Quarterly, 36(11), 1985–2001.

[32] Ness, S. & Chase, P. "How GDPR could affect the transatlantic relationship." Link

Thus, our interview with Professor de Kerckhove offered profound insights into the intricate dynamics of technology, regulation, and their profound impact on the fabric of our society. Overall, the absence of regulation for quantum computing could result in significant negative consequences for individuals, organizations, and society as a whole. These discusiion highlights the importance of establishing regulations to govern the development and deployment of quantum computing. By doing so, we can ensure that this technology is used responsibly and for the benefit of all, while mitigating potential negative consequences.

V. Legal aspects related to quantum technologieS

Quantum Technologies and Data Protection: GDPR Implementation Challenges

Data processing, communication, and encryption are just a few of the areas of our life that quantum technologies have the potential to transform. As these technologies advance, it is more important to address any potential effects they may have on data privacy and protection. The main questions arise about compliance with the General Data Protection Regulation (GDPR)[33] of the European Union. The process of collecting, processing, storing, and transmitting quantum information differs from the classical one, as specific rules that govern the quantum world.

One of the concerns is related to data privacy and security. Article 5(1)(f)[34] of the GDPR states that personal data must be processed «...in a manner that ensures appropriate security of personal data… using appropriate technical or organizational measures…». Further, for example, according to Article 44[35] transferring personal data outside the EU to countries that don't offer an adequate level of data protection is restricted by the GDPR. Organizations have to take into account the effects of cross-border data transfers and guarantee GDPR compliance by putting in place the necessary protections. The significant processing capability of quantum computers might endanger traditional encryption techniques. In order to secure customer data from increasing risks organizations must use quantum-resistant encryption methods. It is known that quantum cryptography is at an early stage of

[33] "General Data Protection Regulation (GDPR)." *Horizon 2020 Framework Programme of the European Union.* Link
[34] Id.
[35] Id

development and today it is impossible to provide the necessary level of secure processing of personal data.

The GDPR grants data subjects various rights, including the right to access, rectify, and erase their personal data.[36] Additionally, regulation ensures the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and the right to get a copy of the personal data undergoing processing under Article 15.[37] However, dealing with quantum information, it is not extremely challenging to meet these requirements, as information according to the non-cloning theory (which states that it is impossible to create an exact copy of an arbitrary quantum state) can only be teleported, which means the controller will no longer have access to the data.

Furthermore, even if both, the controller and the data subject, have an access to quantum information processing systems, it is still remain impossible to transfer an accurate copy of personal data due to the no-communication theorem, that it is impossible to transfer quantum information from one quantum system to another in a way that does not violate the principles of quantum mechanics. This is due to the fact that any measurement of quantum information leads to its change, as was noted above. The use of quantum teleportation for data transmission can also cause problems with the confidentiality of data and, accordingly, violate the provisions of the GDPR, since the process is based on the transmission of quantum states that can only be reproduced if matching parameters exist on two remote quantum systems.

We should also consider the no-deleting theorem - a no-go theorem that states that, given two copies of some arbitrary quantum state, it is impossible to delete one of the copies. It is a time-reversed dual to the no-cloning theorem, which states that arbitrary states cannot be copied. This means that quantum information cannot be completely erased and will be stored in a certain form even after it has been used or transmitted. It violates Article 17[38] which states the right to be forgotten and Article 5(1)(e)[39] which permits the storage of personal data no longer than is necessary for the purposes for which the personal data are processed.

[36] Id.
[37] Id.
[38] Id.
[39] Id.

Another important provision of the GDPR that can be violated due to the quantum processing of information is data transparency. Article 5(1)(a) and Article 12[40] of the GDPR sets out the requirement that personal data must be processed in a transparent manner. Recital 58 clarifies that the principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible, and easy to understand, and that clear and plain language be used also in order to give a consent for processing. The fundamental standards for the effectiveness of a lawful legal consent are provided for in Article 7 and further clarified in Recital 32 of the GDPR.[41] Before processing a personal data, organizations are required by GDPR to obtain informed and freely given consent from individuals before processing their personal data. This includes a provision of clear and understandable information about the purposes, methods, and probable consequences of the data processing. When applying quantum processing of the information, organizations should provide individuals with the specific details, such as the potential impact on data security, encryption methods, and any risks associated with the technology. It is essential for data subjects to comprehend the processing methods utilized for personal information. The complexity of quantum processing techniques, however, can make it challenging and barely impossible for data subjects to properly understand how their data is being processed. Quantum processing includes complex mathematical and computational techniques that data subjects might not be familiar with. It's obvious that the majority of data subjects lack the technical understanding or skill necessary to comprehend quantum processing methods. This knowledge gap is a serious obstacle to compliance with GDPR requirements. In this case, we should also consider the non-teleportation theory that quantum information cannot be converted into classical information, which limits the transparency of this data and makes it difficult for data processors to comply with this principle.

Last but not least, by applying quantum data processing, companies may potentially handle larger volumes of data, perform complex analytics tasks more productively, and accordingly significantly increase the speed of data processing that may not be feasible for classical computing approaches. The Velocity Principle is a principle in data provenance that associates the velocity (speed) of a data object with the transparency of the provenance of that object. Specifically, the principle states that as the velocity of a data object increases, the need for transparency in the object's provenance also increases. The velocity of a data object

[40] Id.
[41] Id.

refers to the rate at which the object is created, processed, or transferred over a period of time. Velocity is one of the three characteristics of big data, along with volume and variety, and is often used to describe the speed at which data is generated and processed in real-time applications such as social media, financial trading, and sensor networks. Data provenance refers to the history of a data object, including its origins, transformations, and ownership. It is important for ensuring the trustworthiness and quality of data, especially in applications such as scientific research, data analytics, and regulatory compliance. The Velocity Principle recognizes that data objects that are created, processed, or shared rapidly are more prone to errors, inconsistencies, and security breaches. Therefore, the development of quantum computing increases the risks associated with the velocity principle.

Intellectual Property Law and Quantum Technologies

One of the most important legal issues with respect to the development of quantum computers concerns the way in which the standards conditioning the operation of quantum computers are set. The development of quantum technologies is shaped by countless decisions of those who build and program them. These decisions are never impartial and their consequences usually have long-lasting impacts. The choices related to technology design can never be considered as neutral as they always reflect the values, assumptions, potential outcomes, and historical and social context in which the developers are. Consequently, the decisions made by the pioneers of quantum computing will undoubtedly influence the future normative development and utilization of quantum computers.

It is important to maintain a balance between promoting open innovation and protecting intellectual property (IP) in the field of quantum technology. Protecting IP rights is essential for encouraging investment, fostering innovation, and protecting inventors' rights while also having the potential for further groundbreaking advancements and commercial applications. The ecosystem for quantum computing regulation has to get stronger and more resilient. As success is gained in filling legal industry-affecting gaps, it can easily be replicated across the world, helping create a sustainable fundament for further developments. At the same time, the field of quantum computing is still in its infancy. Regulatory balance is required to ensure broader markets and stronger adoption of quantum technologies. It has been already observed that the commercial companies involved in the development of quantum computers have started to protect their developments by patents, making subsequent modifications more

challenging. If quantum computing innovations are developing by a limited number of nation-states and large organizations and it entailed the lack of transparency of technological outcomes. There is a higher probability that the use of these innovations for societal benefits, such as achieving sustainable goals, may be restricted by actors who has competitive or geopolitical advantages. Reasonable regulation will create positive competition and promote a more successful adoption process. Additionally, when an open innovation environment is created, it becomes easier to identify areas that need standardization.

In terms of formal and material requirements, flexibility, scope, and term of protection, regional variations may exist. From the perspective of IP rights, we can group the components of a quantum computer by hardware (chip rights, design, and utility patents), software (copyrights, creative commons), and algorithms[42] (open source or public domain). The protection term for patents is 20 years, compared to 70 years for software. In general, quantum computing hardware is much more difficult to develop and replicate than the accompanying software and algorithms. It requires more investments to make than writing the code. As a result of this, particular inventions can become subject to geopolitical conflicts and export control reforms, as, for example, observed in today's computer chips trade race between the US and China. To address the exponential rate of innovation in the Quantum Age, it is suggested to set shorter periods of IP protection, ranging from 3 to 10 years, for innovations that incorporate quantum and AI. Both software and hardware might fall under these shorter terms.

Patent

In the field of quantum technologies, various objects can fall under different IP rights such as chip rights (e.g. semi-conductor topography protection), patents, copyrights, trade secrets, design rights, and trademarks. Patent protection provides exclusive rights to the inventor, preventing others from using, manufacturing, or selling the protected invention without permission. By guaranteeing the inventor exclusive rights, it aims to promote innovative concepts and support researches and developments. In addition, it encourages innovators to enhance prior patents.

[42] Montanaro, A. "Quantum Algorithms: An Overview." NPJ Quantum Information, vol. 2, 2016

There are several quantum technologies[43] that are eligible for patent protection: technology building blocks such as qubits, quantum gates, and multipliers, as well as quantum integrated circuit chips, and various types of quantum processors, such as spin qubits and superconducting transmon qubits. Additionally, patent protection can be sought for quantum interference devices, compiler engines (optimizers, translators, mappers), decoders, simulators, emulators, circuit drawers, and the microarchitecture encompassing quantum execution and quantum error blocks[44]. The quantum-classical interface, quantum instruction set architecture, and quantum memory are further components that can be protected by patents. Furthermore, the overall system and processes involved in quantum computing can also be eligible for patent protection. This encompasses the combination and utilization of the aforementioned components to execute quantum computations. In addition to the specific components, the dilution refrigerator[45] used in quantum computing, including its individual cryoperm shield, quantum amplifiers, cryogenic isolators, mixing chamber, superconducting coaxial lines, input microwave lines, and qubit signal amplifier component, are also eligible for patenting. Seeking patent protection for these components and technologies can provide legal rights and exclusivity to the inventors or assignees, allowing them to control the use, manufacture, and commercialization of their inventions.

Copyright

Copyright guarantee that the exclusive right to reproduce, distribute, display, perform, and create derivative works based on the original work is protected against unlawful copying or dissemination. It aims to enforce freedom of expression, cultural diversity, technical advancement, and incentives for creativity. By allowing subsequent generations of authors to freely borrow from the works of their successors, copyright encourages the production and spread of varied cultural expression. In the realm of quantum technologies, copyright can also play a role in safeguarding intellectual property rights associated with quantum algorithms, quantum software development, quantum simulations, quantum communication protocols, and other innovative works in the field. According to The WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights, creative aspects of software source

[43] National Academies of Sciences, Engineering, and Medicine. Quantum Computing: Progress and Prospects. 2019. Link
[44] Yipeng, H., "Quantum microarchitecture." 2022 Link
[45] Lake, R., Simbierowicz, S. "The Bluefors Dilution Refrigerator as an Integrated Quantum Measurement System." Bluefors Quantum Team, Bluefors Oy, 2021. Link

code and firmware can be protected by copyright, as are literary works.[46] Software copyrights are acquired through registration and grant the creator exclusive rights for their lifetime, plus 70 years. Given the lengthy duration of copyright protection, this form of IP protection could stifle innovation. Additionally, certain areas such as the protection of functionality, which is not covered by copyright laws, need special attention and legal innovation.[47] This raises the question of whether they should be protected by a patent. When it comes to a choice between copyright and patent protection, legal uncertainty often results in a shift to trade secrets, which usually stifles innovation. Whether copyright or patents are used to protect quantum computing technology, it may be challenging to identify infringers. Reverse engineering may be required to detect an infringement, but the hardware itself "may be inaccessible because much of today's quantum computing is cloud-based."[48] Reverse engineering of quantum processes will also be more challenging due to superposition. Quantum states are changed once observed, whereas existing logic processes only measure final outputs.

It is significant to highlight that the ideas, principles, or discoveries in quantum technologies are not protected by copyright. It merely addresses the specific expression or manifestation of such concepts in material form. Furthermore, the extent of copyright protection may differ based on the jurisdiction, as well as the particular criteria and restrictions set forth in the applicable copyright laws. Creators involved in quantum technologies may choose to assert their rights in another way. Before the expression of an idea is captured in a tangible medium, it can be time-stamped by an i-Depot. Ideas can also be protected contractually by a non-disclosure agreement.[49] The following components are eligible for copyright protection: quantum software, the APIs, quantum arithmetic unit (quantum addition, subtraction, multiplication, and exponentiation), runtime assertion and configuration, quantum computing platforms, program paradigm and languages, the BaconShor stabilization code, color codes, and surface codes.[50] If they are authentic original works of creative human authorship fixed in a physical medium of expression, then these elements are copyrightable subject matter.

---

[46] "The Agreement on Trade-Related Aspects of Intellectual Property Rights." *The World Trade Organization*, 1994. Link
[47] Gervai, D., & Derclaye, E. "The scope of computer program protection after SAS: are we closer to answers?" European Intellectual Property Review, vol. 34, no. 8, 2012, pp. 565-572.
[48] Kop, M. "Regulating Transformative Technology in the Quantum Age: Intellectual Property, Standardization & Sustainable Innovation." STAN.–VIENNA TRANSATLANTIC TECH. L. F., 2020. Link
[49] Id.
[50] Id.

The licensing plays a significant role in determining the permissions and limitations associated with the use, modification, and distribution of the open-source quantum software. By using an appropriate license, developers may get a guarantee that their work remains open and protected, and stimulates collaboration. Depending on the particular project and the preferences of the developers, different open-source quantum software may have various licensing requirements. A few typical licenses are frequently used for open-source quantum software projects such as GNU General Public License which covers open-source software, requiring publish any modifications of this software under the same license. There are some alternatives available, for example, it is possible that certain applied programming languages useful for quantum computing will be open sourced instead of copyright protected, or licensed for use via Creative Commons.[51]

In several jurisdictions, human creators are granted intellectual property rights under the current legislature. The issue of whether quantum-generated content is covered by copyright, patent, or other intellectual property laws is still subject to discussion and could result in new legislative updates or legal precedents. When adopting and integrating the rights on quantum/AI output, we can refer to Roman Law. The Romans invented public domain. Roman categories of non-exclusive property relevant for Al Made Creations are: res communes, res communes omnium, res publicae, res nullius, res divini iuris, res universitatis and res patrimonium.[52] Building on the multi- layered property paradigm a new model of Al specific propertization can be imagined. An explicit public domain regime for Al Made Creations in the form of Res Publicae ex Machina: Public Property from the Machine.In this articles it is suggested to consider an output created or invented by autonomous quantum/AI systems without human intervention as a public domain, since this output lacks human creativity and inventiveness and society benefits from a robust public domain.[53] Machine generated Quantum/AI Creations & Inventions should be Res Publicae ex Machina. These belong in an articulated public domain. However, there are still continuing ongoing researches and debates on legal and ethical frameworks for autonomous systems. These frameworks are intended to bring new solutions related to safety, liability, accountability, and the allocation of rights between human operators and AI/quantum systems.

---

[51] Creative Commons, Link
[52] Rahmatian, A. "Copyright and Creativity: The Making of Property Rights in Creative Works." Link
[53] Mauritz Kop, AI & Intellectual Property: Towards an Articulated Public Domain. Link

Trademarks and Trade Secret

It is necessary to raise an important question regarding the potential implication of trade secrets trademarks in the context of quantum computing, and an impact it could have on innovation, disclosure, and technology transfer. This types of protection have potentially unlimited terms, while patents, for example, have a limited duration. Some businesses and researchers may rely more heavily on trade secrets to safeguard their quantum computing assets as a result of the legal ambiguity surrounding the patentability of specific components of quantum computing systems and the need to preserve a competitive edge. Companies can maintain exclusivity and possibly prevent the spread of certain aspects of their technology by safeguarding proprietary algorithms, processes, or other important knowledge under trade secrets. This trend might ensue in a disincentive to disclose ideas and impedes dissemination of information, technology transfer to the market, and follow on innovation.[54] It is important that a trade secret rights do not provide direct protection against reverse engineering. Reverse engineering is the process of analyzing and understanding the design, functionality, or composition of a product, system, or technology. It may include disassembling software or hardware, analyzing protocols, or studying the components. To protect against reverse engineering, other forms of intellectual property rights, such as patents or copyright, may offer more specific legal remedies, including contracts that prohibit unwanted reverse engineering.

Supplementary Strategies for Intellectual Property Regulation

In the area of quantum computing, it is crucial to carefully balance the use of trade secrets and patents. Many companies adopt a hybrid strategy, utilizing IP rights to secure essential data. The choice of an intellectual property protection approach ultimately depends on a number of factors, such as the technology involved, corporate objectives, the state of the market, and the regulatory landscape. When it comes to promotion and allocation strategies for innovation, IP rights are not the only solution. Policy makers could apply innovation policy pluralism (i.e. match IP alternatives such as anti-trust law, contract law, consumer privacy protection, tax law, standardization and certification, as well as prizes, subsidies, public-private funding, competitions, penalties and fines). Innovation policy pluralism facilitates the diversity of protection approaches and helps to incorporate various instruments

[54] Drexl, J. "Designing Competitive Markets for Industrial Data - Between Propertisation and Access." Link

and customize particular contexts and purposes. It enables decision-makers to address the many possibilities and challenges associated with innovations while taking into account the needs of different stakeholders, balancing competitiveness, and promoting social benefits. Policymakers should more clearly differentiate across economic sectors when developing regulatory solutions because innovation incentive and reward mechanisms, effects, and safety/security issues vary by industry and technology. Furthermore, in a quantum and AI-driven future where creation, reproduction, and dissemination have become affordable, intellectual property laws might be less necessary.

Another pillar worth considering is the standardization of innovation policy. There are some key objectives of standardization. The first one is interoperability: standardization guarantees that various products, systems, and technology may coexist effectively together. The second one is quality and safety: standards are essential for guaranteeing the quality, security, and reliability of goods, services, and processes. They outline the minimal standards, performance benchmarks, and best practices that must be adhered to, improving consumer safety and trust. And the last ones are security and sustainability. Standards can address security issues and aid in risk mitigation in many areas, including vital infrastructure, privacy, and cybersecurity. Sustainability-focused standardization, in turn, could promote the minimization of negative effects of products, services, and processes on the environment. It encourages sustainable resource consumption, waste reduction, and environmentally friendly practices. As such, standardization has a significant impact on society, ranging from the safety and wellbeing of workers and citizens, the environment, and the circular economy, to innovation and overall prosperity.

Potential promise of quantum computing for computational law. Time aspect of quantum law.

With the spreading of quantum technologies, the concept of lawyers' thinking may also change. The question is already posed about the transformation of computational law into quantum computational law, which would allow making more objective judicial decisions and finding solutions to seemingly unsolvable legal problems, relying on the properties of quantum phenomena.[55]

[55] Atik, J., & Jeutner, V. "Quantum computing and computational law." Law, Innovation and Technology, vol. 13, no. 2, 2021, pp. 302-324. DOI: 10.1080/17579961.2021.1977216. Link

Computational law concerns the expression, application, and analysis of law in algorithmic form. It involves forming legal algorithms that proceed through logical processes (at the level of computer hardware, through the passage between 'logic gates') to create legal conclusions. Computational complexity theory is a good starting point to identify problems for which quantum computers might demonstrate 'quantum supremacy'. Despite the complexity of a problem beyond the capabilities of a classical computer, we cannot assume that quantum computers will inherently offer superior performance. Computational complexity theory – for the moment – is itself premised on the capabilities of classical computers. It will inevitably expand to include additional categories of problems by their relative difficulty to solve using quantum computers. The transition of law in computational form and the accelerating translation of law from human language to computer code will facilitate the advent of complex quantum legal algorithms. Natural language processing and machine learning are currently being deployed to model law and to build tools capable of legal analysis and predicting legal outcomes. Quantum computing will likely drive further developments in modeling and operationalizing. Already, operationalised algorithms are used in the emerging field of legal analytics to model, predict or instantiate the legal system. Inevitably, law will move – at least in part – to computer code, in a transition that resembles law's movement from orality to text.[5657] The promised range of AI-related technologies will supplement human operators of the legal system. In this regard, quantum computing opens up specific potentialities for computational law, enabling new (and possibly strange algorithms.[58] [59]

To see the possibilities for law, we have to ask whether there are legal questions that are suited to quantum computers. There is the possibility that law, or at least certain aspects of law, may be revealed to have a fundamental quantised structure. Therefore, it is necessary to consider the dispute about the determinism of the law. Providing a parallel with Schrödinger's Cat experiment, there are physics who, like Erwin Schrödinger and Albert Einstein,[60] think that the cat can never be both alive and dead at the same time, and there are

---

[56] Tiersma, Peter M., "Parchment, Paper, Pixels: Law and the Technologies of Communication." *University of Chicago Press, 2010.* Link

[57] Rosalind T. "Written in Stone? Liberty, Equality, Orality and the Codification of Law." (1995) Link

[58] Quantum phenomena, such as wave/particle duality, are often described as 'strange' or 'weird'. These phenomena display characteristics or behaviors that do not correspond to ordinary human sense experience. A 'strange' quantum algorithm might follow a surprising pathway to reach its result.

[59] Styer, Daniel F. "The Strange World of Quantum Mechanics." *Cambridge; New York: Cambridge University Press.* Link

[60] Bohr N., "Discussions with Einstein on Epistemological Problems in Atomic Physics." Link

those, like Niels Bohr and Werner Heisenberg,[61] who believe that this is precisely what happens (not to a cat, but to a small particle) . Just as in the world of quantum physics, in law, there are those who do not accept that legal rules do not have a determined meaning until the Court states it. For them, the rule already means either A or B even before the Court has decided. At the same time, there are those who believe that legal rules indeed mean both A and B, until the Court 'collapses' them (to use an expression from physics) into only one meaning. The conclusion, expressed in terms of quantum mechanics, is that neither applicable substantive legal rules nor the rules of legal reasoning are determined before being 'observed' by judges. The rules of legal reasoning are, thus, also in a state of 'superposition' together with the applicable substantive legal rules until 'observed' by judges.[62] Computational law presumes just the opposite: that much of law is deterministic and can be faithfully expressed in algorithmic form. Given certain inputs and the execution of the algorithm, a consistent outcome is expected to result. Computational law that engages quantum computing may reconcile these two views, permitting robust outputs while addressing the well-recognized sources for law's asserted indeterminacy. Superposition could be helpful to conceptualize situations in which a certain kind of conduct, as a matter of positive law, entails legal cases. For example, when norms belonging to different normative orders (for example, domestic and international law) collide. Similar questions arise with respect to law's rule / exception dynamic – a phenomenon that has been well explored in computational legal theory. Classical computing more than adequately handles the rule/exception dynamic once the rule and any accompanying exception have been defined. But classical computing is inadequate in predicting when a new exception will be found. The formation of a new exception constitutes a rupture from the settled deterministic pathway. Here the phenomenon of superposition may serve to better model this kind of legal phenomenon. The task of modeling a legal system also becomes more difficult where formal status is assigned to decisional law, as in the Anglo-American common law system. Machine learning could be a possible solution for this issue. However, if law as we now know it is imperfectly deterministic, then translating legal operations into computational form will result in imposing determinism on it, which would constitute a fundamental change to the law we have known.

---

[61] Faye, J., "Copenhagen Interpretation of Quantum Mechanics", T*he Stanford Encyclopedia of Philosophy* Link

[62] Capeta, T. "Do Judicial Decision-Making and Quantum Mechanics Have Anything in Common? A Contribution to Realist Theories of Adjudication at the CJEU." SSRN Electronic Journal. (2019). Link

Overall, quantum computing and its phenomenon of superposition allows computational law to capture and produce more muted, more subtle legal outputs. This possibility – together with increasing command in generated quantum legal algorithms – may not only facilitate the making of new law but might also shed new light on the debate concerning law's (in)determinacy.

It is equally important to consider the shift of time focus to real-time regulation. For example, the London Air Quality Network provides real-time air quality information to the public, which is used by the authorities to enforce air pollution regulations. In 2020, the London borough of Camden used the network's data to fine a construction company for violating air pollution limits. Real-time reporting resulted in real-time enforcement. The actions of observing behavior, and the act of recording what occurs within the behavior, have become concurrent with the behavior. The cornerstone is the Consensus to Surveillance. To build on this cornerstone, digital justice rejects two substantive qualities of earlier legal systems. First, efficiency requires abandoning the complications of trying to assign and administer rights or privileges to specific data assets under the legal constructs of trade secrets or personal privacy. Compliance has become real-time decisioning—and, in many operations, anticipatory. At the same time, the raising question is how to fullycalculate our trust in a data object and its provenance while not collapsing the velocity of that object across the Net?

The same question persists for production systems, infrastructure components, and ourselves. At what point does calculating compliance degrade the utility and function of the asset being evaluated? Another issues is the standard quantum limit (SQL). The SQL is a fundamental limit on the precision with which certain measurements can be made, as predicted by quantum mechanics. This feature is also expressed in the quantum uncertainty principle that implies that there is a limit to the amount of information that can be transmitted or processed with a given level of precision. It arises from the fact that any measurement of a quantum system will inevitably disturb that system to some degree, a phenomenon known as the Heisenberg uncertainty principle. Each observation of the behavior of a data object creates uncertainty. For example, consider a measurement of the position of an electron in an atom. In order to measure the position of the electron with high precision, it is necessary to shine a light on the atom, which causes the electron to absorb and re-emit photons. This process inevitably alters the electron's momentum and hence its energy level, which can in turn affect the behavior of the atom as a whole. Overcoming the SQL requires sophisticated and

resource-intensive quantum technologies, including specialized quantum sensors and error correction techniques.

In any case, developers of quantum computers and quantum algorithms must decide which margin of error they are willing to accept and which degree of probability they require before a result can be communicated as the correct one. In cases where the stakes are low, a low degree of certainty might be defensible. In other cases, when the stakes are high – in the medical sector, for example, a higher degree of certainty might be required. With respect to these standard setting decisions developers of quantum computers can exercise a remarkable degree of discretion. From a legal point of view, this is significant since these decisions could affect the interests of others even at a very early stage of development.[63]

Performing measurements with high precision while minimizing disturbance to the quantum system being measured is a challenging task, but there are several strategies that researchers use to accomplish this goal. Here are a few examples:

- Weak measurements: One approach is to perform a "weak" measurement that minimally disturbs the quantum system. A weak measurement is one in which the coupling between the measurement device and the system being measured is very weak. This approach allows for some information to be extracted about the system without causing significant disturbance.
- Quantum non-demolition measurements: Another approach is to use a technique called quantum non-demolition (QND) measurements. QND measurements can be used to measure one property of a quantum system without perturbing other properties. This is accomplished by designing the measurement process in such a way that the interaction between the measurement device and the quantum system is highly selective.
- Feedback control: A third approach is to use feedback control to minimize the disturbance caused by measurement. In this approach, the measurement device is designed to be highly sensitive to the quantum system being measured, and the results of the measurement are used to adjust the measurement device in real time. This allows for more accurate measurements while minimizing the disturbance caused by the measurement. This disturbance caused by measurement can be especially

[63] Jeutner, V. "Morals & Machines." "The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers." (2021). Link

significant in the realm of quantum computing, where the delicate quantum states of qubits must be measured in order to perform computations. The measurement process can introduce errors and disrupt the coherence of the qubits, leading to a phenomenon known as decoherence. As we fine-tune our sensors to be capable of observing and measuring behaviors of the photons transporting and storing data, limits exist as to the measurement precision to be achieved. There is a balance in deciding whether, and in what conditions, we can be indifferent to further accuracy.

In conclusion, the exploration of legal aspects related to quantum technologies has revealed a complex and rapidly evolving landscape. Throughout this chapter, we have delved into several key legal issues surrounding quantum technologies. It is evident that the legal landscape related to quantum technologies is in a state of flux, and the path forward will require a multi-faceted approach involving policymakers, legal experts, scientists, and industry leaders. As quantum technologies continue to reshape our world, the legal community must proactively engage in ongoing dialogue and iterative updates to adapt and develop cohesive and forward-looking legal frameworks.

VI. Safeguarding Data in the Quantum Age: Importance of Post-Quantum Cybersecurity

Examining Current Cryptographic Threats

The advent of quantum computing brings about fresh perspectives and new approaches and methodologies for ensuring information security and confidentiality. On the one hand, progress in quantum computing has enhanced the confidentiality, integrity, and availability of networks by protecting their defense against attacks, on the other hand there is a need for the development of more robust and secure methods of information transaction. Quantum era alters our comprehension of confidentiality and security, resenting at the same time new issues and novel tools to safeguard information against attacks and interception. This shift from classical to quantum computation carries significant implications and has the potential to undermine the security of currently established methods of information protection. Due to a significant rise in the amount of data available, there has also been a substantial increase in cyber threats, making it urgent to safeguard personal, commercial, and governmental data.

Data confidentiality and security might be compromised if a post-quantum security system is not implemented before an attacker gains access to a quantum computer. Security could be ensured by Post-Quantum Cryptography (PQC). PQC is a family of cryptographic algorithms including key establishment and digital signatures that ensures a conjectured security even against an attacker equipped with quantum computers. It is crucial to provide a division between Post-Quantum Cryptography and Quantum Cryptography as PQC focuses on developing cryptographic tools that can be used on existing classical computers and that might be resistant to attacks from both classical and quantum cryptanalysis, while Quantum Cryptography involves cryptographic solutions that leverage the principles of quantum physics (for example Quantum Key Distribution (QKD)).

Public key cryptography (PKC) is one of the cryptographic approaches the most vulnerable to attacks from quantum computers. PKC, also known as asymmetric cryptography, is a method that permits safe communications between entities, users, or servers, that do not share any pre-established secret. It is the foundation for the security of the bulk of digital infrastructures. More specifically, PKC performs two primary functions: the creation of secured channels (key establishment) and the authentication of digital information (including the use of digital signatures to verify the identities of parties within a communication protocol). Today, these techniques are essentially based on two mathematical problems: the factorization of large numbers and the discrete logarithm computation.

These problems are currently considered extremely difficult to solve using our existing computational resources and mathematical understanding. If a large-scale quantum computer is created, these two main issues will no longer be intractable, and the security of currently used PKC may therefore be compromised. Indeed, in 1994 P. Shor proposed a quantum algorithm[64] that has potential to break public key encryption schemes, such as RSA and Elliptic Curve Cryptography, by efficiently factoring large numbers or solving the discrete logarithm problem. Public Key algorithms, such as RSA and Elliptic Curve, are widely employed for encryption purposes. These algorithms utilize a mathematical approach where a private key is derived from a corresponding public key, eliminating the need to consider all possible scenarios. The private key is computed by factoring a number that is the product of two prime numbers. For instance, a private key can be obtained by multiplying the prime

[64] Shor, P. "Algorithms for quantum computation: Discrete logarithms and factoring." In 35th FOCS, IEEE Computer Society Press, Nov. 1994, pp. 124–134.

numbers 7 and 3, resulting in 21. The security of these algorithms relies on the length of the key. RSA, for instance, employs a key length of 2,048 bits, equivalent to 617 decimal digits, which is currently considered highly secure against conventional computing capabilities. However, the advent of quantum computers raises concerns as they can potentially crack key pairs with lengths as long as 4096 bits in just a few hours using Shor's algorithm.

Cryptographically Relevant Quantum Computers (CRQCs) is a concept introduced by the UK's National Cyber Security Centre (NCSC)[65] to distinguish between small-scale prototypes of quantum computers and quantum computers that have the potential to execute specific cryptographic algorithms that threaten public-key cryptography. A CRQC is a family of method based on physical principles rather than mathematical foundations, unlike classical cryptography. These techniques facilitate the establishment of a shared secret, known as a key, through a communication exchange between two parties. It can perform Shor's algorithm, posing a serious threat to current public-key cryptography techniques. Since existing quantum computer prototypes lack the necessary stability and scalability for CRQCs, they do not yet pose a threat to public key cryptography. Before scaling up to huge quantum computers capable of solving the factorization and discrete logarithm issues on which the existing PKC is built, there is a need to overcome number of scientific obstacles in physics, engineering, and computer science that must be addressed. Nowadays, the goal of creating a functional quantum computer is driving significant investments from businesses and states. There is no absolute assurance that we will be able to create quantum computers, and the timescale for their realization is still unclear.

The threat of retroactive attacks also cannot be ruled out as any encrypted communication intercepted today could be decrypted by the attacker once they have a powerful quantum computer at their disposal, regardless of how much time ago years encryption had a place. Digital signatures potentially may also be impacted by the quantum danger. A CRQC might be utilized to counterfeit signatures and enable impersonation attacks. This threat would only be feasible if the signatures are created at a time when a CRQC is created, unlike the retroactive threat. Thus, the signatures cannot be directly influenced before the existence of a CRQC. But in the context of document signing, long-term validity is occasionally necessary for particular situations, and these signatures might be jeopardized by the presence of a

[65] "Preparing for quantum-safe cryptography." *National Cyber Security Center,* Link

CRQC. To prevent any a posteriori impersonation attack, the transition from pre-quantum signatures to post-quantum ones should be addressed prior to the emergence of any CRQC.

Potentially powerful quantum computers may target also symmetric cryptography. A generic Grover's algorithm is a quantum algorithm introduced in 1998, that sufficiently accelerates searching of secret keys in symmetric algorithms. It can also speed up collision-finding attacks on hash functions. However, these attacks require the use of CRQCs. Nevertheless, for many algorithms, adjusting the sizes of hash outputs and keys could potentially mitigate these attacks. For instance, a symmetric-key block cipher known as the Advanced Encryption Standard (AES) uses 10 rounds of encryption with a key size of 128 bits, or 16 bytes. Although it has been difficult to crack AES on conventional computers, since it would take an unreasonable period of time, the emergence of post-quantum computing has raised questions about its security. AES can still be effective in the post-quantum age by doubling the current key size and increasing the number of encryption cycles. Consequently, the overall impact of Grover's algorithm on symmetric cryptography is considerably more limited compared to the impact of Shor's algorithm on PKC. All communication systems with public key encryption (using asymmetric keys) may be swiftly cracked, allowing for the compromising of enormous volumes of sensitive data. One tool for ensuring secure communications, which uses quantum channels and do not vulnerable to classical and quantum computers is QKD. However, this method does not offer public key cryptography's full functional equivalent. Its applications are restricted since it requires a dedicated communication infrastructure and lacks genuine routing capabilities. As a result, aside from specialized applications where QKD is used to provide some additional physical security on top of algorithmic cryptography (and not as a replacement), it is not considered an effective defense against the quantum threat.

Modern Initiatives in Post-Quantum Cybersecurity Standards

The development of post-quantum cybersecurity standards has become a crucial focus for agencies in developed countries. This thesis examines the attempts and efforts undertaken by these agencies to transform the future of cybersecurity standards in the face of quantum advancements.

The National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce is the global hub for analyzing post-quantum cryptography algorithms. It initiated an open competition of quantum-resistant cryptographic algorithms and encryption schemes that are resistant to attacks from quantum computers.

In the first stage, 50 encryption schemes were presented by various scientific organizations (including Korean University, Chinese Academy of Sciences, Sorbonne University, University of Waterloo, etc.) and technology companies (IBM Research, Microsoft, Philips Research, Intel, etc.). The first four competition winners - CRYSTALS-Kyber for asymmetric encryption, CRYSTALS-Dilithium and FALCON for signatures, and SPHINCS+ for stateless hash-based signatures - were presented by NIST in the summer of 2022[66]. The algorithms are specifically created to realize two primary purposes for which encryption is commonly used: general encryption, which safeguards information transmitted over public networks, and digital signatures, which provide identity authentication. These four algorithms were designed through collaborative efforts involving experts from various countries and institutions. NIST has chosen specific algorithms for both general encryption and digital signatures. For general encryption used in secure website access, the CRYSTALS-Kyber algorithm has been selected. It offers advantages such as relatively small encryption keys that can be easily exchanged between parties and fast operation speed. For digital signatures, which are commonly used for identity verification in digital transactions or remote document signing, NIST has selected three algorithms: CRYSTALS-Dilithium, FALCON, and SPHINCS+. Reviewers have recognized the high efficiency of the first two algorithms. NIST recommends CRYSTALS-Dilithium as the primary algorithm, while FALCON is suitable for applications that require smaller signatures than what Dilithium can provide. The third algorithm, SPHINCS+, is slightly larger and slower than the other two but serves as a valuable backup option because it is based on a different mathematical approach than the other three algorithms selected by NIST. Three of the selected algorithms, namely CRYSTALS-Kyber, CRYSTALS-Dilithium, and FALCON, are built upon the principles of structured lattices, having a mathematical structure. On the other hand, SPHINCS+ utilizes hash functions as the basis for its approach. Further, there are presented the finalist algorithms that are competing to be considered by NIST ready for standardization, and the

[66] "Post-Quantum Cryptography - PQCrypto 2022." Lecture Notes in Computer Science.
Link

algorithms that NIST considers promising, but still not ready to be applied. A quantum-resistant encryption technique will thereafter be certified by the American authority.

New cryptographic standards are planned to be published before 2024, but already today the regulator recommends that "cryptographic flexibility" be taken into account, which ensures that encryption can be easily updated or replaced. As the standard is still being developed, NIST encourages security experts to explore these new algorithms and assess how they can be utilized in their applications. However, it is advised not to integrate these algorithms into systems at this stage, as there might be slight changes before the standard is finalized. To prepare for the future, users are advised to take inventory of their systems and identify applications that rely on public-key cryptography. These applications will need to be replaced with algorithms that can withstand attacks from cryptographically relevant quantum computers. Users should also inform their IT departments and vendors about the forthcoming change to ensure readiness for the transition.

NIST is currently considering four additional algorithms for general encryption that do not rely on structured lattices or hash functions. Although this new post-quantum toolbox may seem handy for developers, the maturity level of the post-quantum algorithms presented to the NIST process should not be overestimated. Many aspects lack cryptanalytical hindsight or are still research topics, e.g., analysis of the difficulty of the underlying problem in the classical and quantum computation models, dimensioning, integration of schemes in protocols, and more importantly the design of secure implementations. This situation will probably last some time after the publication of NIST standards.

China has also made substantial investments in research and development, aiming to become a global leader in quantum cybersecurity. It has emerged as a leader in the field of quantum communication, establishing a secure communication line protected by quantum encryption protocols that spans an impressive 4,600 kilometers. The functioning of the Chinese quantum communication line is provided by two satellites. To support the advancement of quantum key distribution, China has reformed the regulatory framework. In 2020, the Encryption Law was adopted, which aims to ensure the development, standardization, and management of cryptography, as well as stimulate the growth of the cryptographic industry and incentivize the creation of high-quality market products. In line with this regulatory legal act, China continues to rigorously control the cryptographic tools used to safeguard the data of public

agencies while allowing the development of «commercial cryptography». In 2021, the PRC approved three standards for equipment used in the process of quantum key distribution. In addition to hardware standards, the Chinese regulator in 2021 approved sixteen new cryptography standards, two of which are entirely dedicated to quantum key allocation.

China and USA are not alone in recognizing the importance of quantum key-sharing technologies for national security. Europe also aims to be ready for the cyber challenges of tomorrow. EU Member States are preparing for the transition of data to quantum-safe cryptography. The European regulator, ETSI, has developed a Migration Strategy and provided recommendations for implementing quantum security algorithms. The document promotes the adoption of the Fully Quantum Safe Cryptographic State. As per the ETSI standard, this is the state of the system in which all cryptographic assets within the system utilize quantum-secure cryptography, with the underlying principles defined by the regulator. Another body, focusing on quantum technologies is ENISA, the European Union Agency for Cybersecurity[67]. It was established in 2004 with the goal of ensuring a high level of cybersecurity across Europe. It contributes significantly to the development of EU cyber policy, increases the credibility of ICT goods, services, and processes through cybersecurity certification schemes and collaboration with Member States and EU organizations. Since the beginning, the EU has been a key player in this area, and with a planned investment of €1 billion over 10 years, the EU Quantum Flagship[68] is mobilizing around 2000 scientists and industrialists, in a collaborative initiative on a precedented scale to position Europe as a leader in the industrial landscape. The EU Cybersecurity Strategy[69], jointly presented by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy in December 2020, considers AI, quantum computing, and encryption as key technologies in order to achieve resilience, technical sovereignty, and leadership. The Strategy underlines the importance of these technologies for the purpose of building operational capacities to prevent, deter, and respond to cyber threats as well as to promote global and open cyberspace.

[67] The European Union Agency for Cybersecurity, Link
[68] Id.
[69] Id.

Quantum Resilience: Implementing Post-Quantum Schemes for Cybersecurity

Transitioning to post-quantum cryptography takes time. Currently public and private entities are waiting for national authorities to standardize PQC algorithms and outline a clear transition plan. However, there are situations where the quantum risk is simply unacceptable. In such cases, a more assertive strategy can be adapted by implementing hybrid solutions that combine pre-quantum and post-quantum schemes. These hybrids also involve incorporating pre-shared keys into all keys established through public-key cryptography, effectively safeguarding the confidentiality of their data against the formidable threat of a quantum-capable attacker.

Two requirements must be met in order for a hybridization approach to be successful:

1. In other words, the security offered by the recognized pre-quantum method that is included in the hybrid approach should at least be as robust as the security offered by the hybrid mechanism.

2. Although there is no set formula for choosing a post-quantum public key algorithm (either for the key establishment or signature mechanisms), it is better to choose one with reliable and thoroughly researched specifications. The algorithm should be a NIST finalist or a trustworthy alternative tool. The chosen algorithm should also strive to achieve a high post-quantum level, ideally NIST level V. For example, the NIST candidates FrodoKEM, Kyber, Dilithium, or Falcon may be appropriate choices for early installations at the time of writing. The selection of NIST-selected algorithms for standardization is not, however, a necessity.

To preserve consistency within the chosen post-quantum public key cryptography technique, it is advised to use a conjectured post-quantum security level for symmetric primitives. This implies using security levels that are at least equivalent to AES-256 for block ciphers and SHA2-384 for hash functions. It's vital to remember that the hybridization strategy does not apply to hash-based signatures. It is estimated that these methods may now be employed without hybridization due to their well-studied underlying mathematical issues. However, their application range may be limited, particularly when there are either a low number of

signature queries or large signature sizes. This phase is anticipated to persist until after the first NIST standards are published, which is until 2025.

In the next phase, it is supposed to be mandatory to integrate pre-quantum security. Except for hash-based signatures, whose hybridization is optional as mentioned above, all post-quantum PKC methods must be consistently incorporated in hybrid mechanisms. The application of the post-quantum component in cryptographic techniques during this period goes beyond mere defense-in-depth. Therefore, it is imperative to guarantee post-quantum security assurance for both symmetric and public key techniques. This assurance, which emphasizes the significance of resolving possible vulnerabilities provided by quantum computing, should be an integral component of the overall security analysis. During that timeframe, the European regulatory bodies should establish precise standards for determining relevant post-quantum public key cryptography algorithms which are permitted based on their corresponding post-quantum security assurance. European regulators will independently evaluate and select the best algorithms based on their effectiveness in providing post-quantum security. This phase should last until 2030.

In the last phase, post-quantum algorithms are expected to provide security assurance levels equivalent to present pre-quantum standards after thorough examination and review. Due to the fact that some post-quantum systems will provide adequate quantum resistance on their own, they can be used without the necessity for hybridization.

It is important to mention that post-quantum cryptography develops at a global level and agencies' standardization efforts expand, so the recommendations provided may change over time. The estimated timeline of the roadmap could be adjusted accordingly, either accelerated or slowed down, based on these factors.

VII. Securing the Quantum Future: Responsible Regulatory Measures

The Need for New Regulatory Approaches

Given the lack of comprehensive best practices regarding Responsible QT-oriented policymaking, the normative power to provide specific substantive guidance is limited. The key difficulty is addressing the growing need to review and reassess our data protection, IP,

cybersecurity, and other regulations, that are applicable to QT governing. We cannot ensure that our regulatory frameworks remain effective. We should consider a new regulatory approach to adapt to the changing landscape of technology and its legal implications. It is essential for developing efficient and comprehensive regulatory frameworks to create a delicate balance between innovation support and safeguarding individual rights.

We had the privilege of sitting down with Giuseppe D'Acquisto, Senior Technology Advisor for the Italian Data Protection Authority, to shed light on this intricate topic. With his extensive expertise in data protection and vast knowledge as a national expert on Big Data in the European Union Agency for Cybersecurity (ENISA) and the Garante within the Technology Expert Subgroup of the European Data Protection Board, he offers a unique perspective on the regulatory aspects surrounding quantum computing. Throughout our in-depth interview, we explored the complexities of quantum technologies regulation, the challenges posed by the specificity of inner workings of quantum algorithm and possible regulatory solutions. G. D'Acquisto's insights helped to understand the possible approaches for future quantum regulation.

The main challenge in his opinion resides in the fact that existing regulatory principles are not adapted to the velocity of technological development. The legal regulation of quantum technologies should defy traditional conceptual frameworks, posing a base for the principles governing secure innovation. The contradiction between legal frameworks and the laws of physics is a problem that needs to be addressed through new innovative regulatory approaches, and it requires a transformation of our legal principles. Traditional strategies are no longer viable, necessitating their comprehensive readjustment to align with the capabilities of technology. A reevaluation is necessary when faced with technology that strongly opposes the application of recognized concepts as we have understood them. We have to reconsider the very essence of basic principles like confidentiality, purpose limitation, safeguarding, and others. Transparency, for instance, is one of the fundamental concepts in data processing. G. D'Acquisto emphasized that the superposition phenomenon makes it impossible to fall under the transparency requirements of GDPR, because of the specificity of a quantum algorithm's inner workings. We are in a state of uncertainty when executing quantum operations, and we are unaware of their outcomes while still in superposition. We cannot eliminate uncertainty and achieve certainty of computation before we observe the results of these computations. In light of this, he came to the conclusion that quantum data processing needs a novel

understanding of transparency. This applies to other legal concepts as well. Additionally, G. D'Acquisto highlited that today, there is an urgent need to reformulate legal principles in response to the rapid development of technology. In order to be consistent with Article 25 of the GDPR[70] and the concept of 'data protection by design', this reformulation should take a predominantly technical perspective. Technological innovation has fundamentally changed the landscape of privacy, security, and ethical considerations. By adopting a technical lens, we can ensure that laws and regulations remain relevant, adaptable, and able to address complex issues related to privacy, cybersecurity, and the responsible use of quantum and other emerging technologies. "There are many promising technologies for implementing data protection principles in a technology oriented way, which can be fruitfully used in the context of quantum computing" said G. D'Acquisto. We can provide many examples of technical approaches supporting implementation of data privacy and security rules. One of them is differential privacy is an approach for providing privacy while sharing information about a group of individuals, by describing the patterns within the group while withholding information about specific individuals. This is done by making arbitrary small changes to individual data that do not change the statistics of interest. Another example is zero-knowledge proof. It is a cryptographic protocol that enables users to demonstrate their knowledge or the validity of specific information without revealing the underlying documents or facts that support it. Incorporating technical rules enhances the efficacy of legal measures and nurtures a proactive, forward-looking environment that prioritizes safety.

We came to the point that first, we have to create a theoretical regulatory framework, revise existing legislation, adapt it, make it more flexible, and take risks into account. We should accept that on the way to responsible quantum development, various risks could appear. Regulators need to recognize the risk factors, then to examine them, and lastly use this knowledge to mitigate them. Once we have achieved clarity, we can proceed to the practical implementation of a new approach using regulatory sandboxes. This approach serves as a starting point for developing a new understanding of traditional regulation within the context of this new paradigm.

Furthermore, G. D'Acquisto stressed the need for a multilateral approach to creating an effective regulatory environment taking into consideration the complexity and potential

[70] "General Data Protection Regulation (GDPR)." *Horizon 2020 Framework Programme of the European Union.* Link

consequences of using and developing these technologies. For optimal use of quantum developments, while protecting human rights from unexpected implications, legislation should include ethical principles, technical standards, and a human-centric and sustainable approach. A robust ethical framework that determines the application and advancement of quantum technologies should be a crucial component of quantum regulation. It is possible to guarantee that quantum innovations are developed and implemented in an ethical manner, taking into account the impact on society, by incorporating ethical principles into regulatory standards. Alongside ethical guidelines, technical standards are essential for managing and mitigating risks related to quantum technologies. Technical rules are necessary to protect against any potential vulnerabilities and guarantee the reliability and security of quantum systems. "Nonetheless, it is essential to acknowledge that, despite rigorous technical rules, certain ineliminable constraints might persist," mentioned G. D'Acquisto. We will be able to keep up with the dynamic nature of quantum technologies if we place an emphasis on adaptation and constant improvement in technical standards. While technical and ethical aspects are crucial, a human-centric approach remains paramount.

Quantum regulation's ultimate purpose is to facilitate outcomes that are beneficial to humanity and prevent damage to individuals or society as a whole. Quantum regulation should be inclusive, diverse, and ensure an extensive societal interaction to ensure that decisions are based on diverse perspectives and correspond to public interest. In order to do so it is necessary to raise quantum awareness. As quantum technologies continue to progress, understanding their implications becomes increasingly crucial. Raising quantum awareness among individuals, policymakers, and businesses can foster an informed and responsible adaptation of these technologies, allowing us to harness their benefits while addressing potential risks.

Searching for optimal approaches to regulating quantum technologies and forming the legal applications of such technologies, we should apply experimental legal regimes - regulatory sandboxes. Under such a regime, certain regulatory requirements are temporarily abandoned in order to check the viability of invention and to try to create its optimal legal regulation. It should be noted that the said flexibility of regulatory sandboxes allows creating proactive law, keeping pace with digitalization.[71] Thus, we could create flexible legal frameworks adapted for forefront technologies staying in the area of safe quantum innovations.

[71] Gromova, E., & Petrenko, S. "Quantum Law: the Beginning." Link

Responsible Quantum Technology - Regulatory Framework

In order to ensure that ethical, legal, socioeconomic, and political frameworks are developing while QTs are still shapeable, it is suggested to create the concept of responsible QT. From a normative standpoint, the goal is to adapt current legal principles while minimizing any downside risk by implementing technical, organizational, and policy measures that are appropriate to the risk.

In this study, the risks posed by quantum computing were analyzed to form the base for Responsible Quantum Technology (RQT) framework. It incorporates ethical, legal, social, and policy implications into the quantum regulation. The development of quantum innovation should be guided by a set of principles ensuring a flexible, safe, and open environment. Principles for Responsible QT could be imagined as follows:

1. **Safety:** Information security should be considered a key component of ensuring the responsible development of quantum computing. To do this, risk-based technology impact assessments (TIA) that in particular address security threats have to be conducted. It is important to take precautions against potential threats like data hacking during transfer or the storage of personal data that could be processed by quantum computers or other related technologies. TIA aims to define the unintended, indirect, or delayed societal impacts of technological innovation. Additionally, it strives to permanently analyze and examine the impact of the integration, updating, and modification of particular innovations including technological synergies. In the context of quantum impact assessments (QIA) it could be, for instance, performed analysis for possible outcomes of integration of quantum cloud computing and precision robotics. However, focus on new ethics, innovative regulation, and new legal principles is crucial for social well-being and minimization of negative impacts. It is impossible to foresee the complete and precise impacts of quantum technology, let alone how those effects will interact with one another and with other socioeconomic factors.Thus, there is a need to improve and update technology impact assessment tools and basic principles. The objective of performing QIA should not be centered on predicting the precise outcomes of QT and its associated factors. Instead, the focus should be on identifying potentially significant vectors of change. Identifying potential issues (and advantages) can alert technology developers and overseers to potential problems and i.e., an early warning system. QIA

will be an important practical tool to facilitate responsible quantum technology adoption.[72]

2. **Cybersecurity:** As has been discussed in the previous chapter, post-quantum cryptography should be used to establish quantum-safe security mechanisms, protect information assets, prevent illegal access, and ensure privacy. Both entrepreneurs and regulators must take a proactive approach to prevent the malicious use of quantum applications and the risks connected with dual use. This requires using forecasting[73] and horizon scanning techniques.[74] Additionally, it is suggested to consider Calculated Compliance Limit (CCL), which refers to the threshold for quantum computers' computing power. As quantum computers are expected to have the potential to break traditional encryption methods, there is growing concern over their potential misuse for malicious purposes, such as hacking or cyber-attacks. To address this concern, some regulatory bodies have proposed setting a CCL for quantum computers, which would define the point at which companies and organizations must implement specific security measures to protect their data.[75] This compliance limit would be based on the estimated number of qubits and computational power of the quantum computer that would be required to break the encryption used to protect sensitive data. Once the quantum computer reaches this limit, organizations would need to comply with specific security standards, such as implementing post-quantum encryption or using quantum-resistant cryptographic algorithms. It's worth noting that there is no universally agreed-upon CCL for quantum computing yet, and the issue is still being actively discussed by policymakers and experts.
3. **Standardization:** Standardization is essential for the development of innovative technologies and effective supply chains.[76] It promotes innovation, increases market competition, and makes it possible for interoperable goods by unifying technologies, processes, and interfaces. Numerous benefits of standards include cost savings, increased effectiveness, product safety, and regulatory compliance.[77] It guarantees market access

---

[72] Kop, M., & Aboy, M., et al. "Towards Responsible Quantum Technology." (2023). Link
[73] Zhang, Y., Porter, A., Chiavetta, D., et al. "Forecasting technical emergence: An introduction." Technological Forecasting and Social Change. Link
[74] Greely, H., "Governing Emerging Technologies - Looking Forward with Horizon Scanning and Looking Back with Technology Audits." Glob. Pub. Pol'y & Governance, 2022. Link
[75] Ritter, J., "Digital Justice in 2058: Trusting Our Survival to AI, Quantum and the Rule of Law." Link
[76] O. van Deventer, N. Spethmann, et al. "Towards European Standards for Quantum Technologies." (2022). Link
[77] Jenet, A., Trefzger, A., et al. Standards4Quantum: Making Quantum Technology Ready for Industry - Putting Science into Standards. EU Publications Office, Luxembourg, 2022. Link

and product compatibility. However, premature standardization may limit exploration during the research phase, and early benchmarks might be biased or difficult to test. Futhermore, horizontal regulations should be complemented by a tailored vertical approach that caters to specific industries and their legislative needs concerning the quantum regulatory gap.[78] This approach should align with the policies of innovative pluralism.

4. **Availability and open innovation:** Due to the high level of complexity, infrastructure dependence, and cost associated with quantum research and development, there is a chance that, without proactive measures, the technology may only be available to a privileged group of people and enterprises with relevant resources, widening the digital gap. Along with respecting IP and related rights including trade secrets, state secrets, and fair-trade conditions, competition law concepts[79] [80] should also help to ensure fair and equitable access to QT and address market inefficiencies. It is necessary to seek international collaboration based on common values to combat the winner-takes-all dynamic. To speed up quantum R&D and actively influence its vector of development, states, and research institutions should look for worldwide alliances founded on ideals like liberal democracy, human rights, and the rule of law. In order to encourage innovation, the Principle highlights the necessity to strike a balance between confidentiality and openness. Even if trade secrets may be more commercially viable at this early stage, the patent system currently promotes public disclosure of quantum technologies. Responsible quantum innovation policy decisions should be based on Evidence-based QT studies.
5. **Sustainable innovation:** The Principle places a strong emphasis on connecting quantum R&D to societal objectives, particularly the SDGs. Although quantum technology has enormous potential to be beneficial to people and the environment, using rare materials like rare earth metals and helium-3 for cooling raises some possible environmental concerns. The ecological footprint should be reduced as much as possible and the application of QT should support socially and environmentally beneficial outcomes.

---

[78] Hemel, Daniel J., and Lisa Larrimore Ouellette. "Innovation Policy Pluralism." Yale Law Journal, vol. 128, 2019. Link

[79] Kop, M., & Aboy, M. "Intellectual property in quantum computing and market power: a theoretical discussion and empirical analysis." Journal of Intellectual Property Law & Practice, vol. 17, no. 8, 2022, pp. 613-628. Link

[80] Kop, M., & Brongersma, M. "Integrating Bespoke IP Regimes for Quantum Technology into National Security Policy." Working Paper, 2021. Link

6. **Quantum awareness:** By providing accessible educational materials on QT and encouraging open discussion, Principle aims to actively engage society and create a shared vision of a desirable quantum future. This guarantees that various viewpoints are taken into account at all stages of the process.
7. **Ethics and risk social risks mitigation:** The Principle incorporates the pyramid of criticality, which divides the spheres of applications of quantum technology into low, mid, and high-risk.

The establishment of this comprehensive set of principles marks a pivotal milestone in shaping the regulatory framework for quantum technologies. These principles provide a solid foundation upon which governments can collaboratively build responsible and ethically sound development and deployment of quantum advancements. As quantum technologies continue to evolve, these principles will serve as a dynamic roadmap, adapting to new challenges and possibilities, and guiding the evolution of regulations that reflect both the transformative power and the responsible stewardship of quantum innovation.

Moreover, given the inherent uncertainties surrounding the application of emerging QT in practical scenarios, products, and systems, there is a need for a risk-centered strategy. This approach encourages enduring innovation, possibly through Quantum Technologies Regulatory Sandboxes (QTRS) through which organizations and researchers can investigate and advance quantum technologies in dedicated environments called under specified rules and supervision, enabling them to realize their full potential free from immediate regulatory restrictions. The QTRS should operate as follows:

1. **Selection Procedure:** The regulatory authorities established a committee made up of legal experts, quantum experts, legal professionals, and representatives from relevant industries. Applications from businesses, research institutes, and startups interested in taking part in the sandbox should be reviewed by this committee.
2. **Eligibility Criteria:** Organizations wishing to participate in the sandbox have to submit a quantum-related project that they intend to develop within the sandbox as part of their application. Participants must have the required technical know-how and must describe their objectives, risks, and safety measures. Participants should be willing to work together in the sandbox, share non-sensitive data, and further the

group's learning and development. The proposal should be able to contribute to quantum regulation and show the potentiality of realization after the sandbox phase.

3. **Guidelines and Boundaries:** The regulatory authorities, collaboratively with the committee, set up certain restrictions within which the participants must operate. These guidelines should outline: the limitations of scale and scope of experimentation and define boundaries on the access to resources and infrastructure, such as energetic, transportation, financial, and government systems, to prevent interference with critical systems or networks; requirements to ensure responsible experiments (conduct environmental impact assessments, etc.); and ethical considerations that must be followed during the experimentation phase.
4. **Scope and Duration:** Scope of the sandbox should be clearly determined, including the list of QT that are eligible for testing and development, as well as the duration for each project's participation in the sandbox.
5. **Regular Evaluations:** The regulatory authorities periodically review the process to evaluate their progress, risks, and results.
6. **Real-world Simulation:** The regulatory sandbox creates simulated real-world conditions, where participants can examine their projects without putting in danger critical infrastructure or public safety. It may involve virtual networks, quantum computing hardware, and communication devices tailored to mimic real-world scenarios.
7. **Public Awareness and Transparency:** For the purpose of raising awareness of the community about sandboxes and their use, the regulatory authorities provide information about these initiatives. By regularly publishing updates and achievements of the projects in the sandbox, they also maintain transparency.
8. **Graduation and Regulation:** After a predefined period (e.g., 2-3 years) of testing within the sandbox, participants graduate from the program. They transition into the market while adhering to the regulatory frameworks designed based on the insights gained from the sandbox experience.

The rules could be modified as appropriate to take quantum technological breakthroughs into account. The specifics of each QTRS will vary, as different regions may have varying priorities and considerations regarding quantum technologies. However, the overall goal is to facilitate innovation, mitigate risks, and promote responsible development of quantum technologies in a controlled environment.

In conclusion, a multilateral strategy for quantum regulation is vital to strike a delicate balance between development and regulation. We can create a strong regulatory quantum framework that promotes positive outcomes while reducing potential dangers by embracing ethical guidelines, technical standards, and human-centric approaches.

Raising Quantum Awareness

The first crucial step towards increasing quantum awareness involves promoting discussions and debates on the topic. It is essential to educate the general public about quantum technology. Despite significant interest and investment in Quantum Technologies from academic, technological, and policymaking communities, there has been limited effort to understand the public's perspective on this subject. The UK National Quantum Technologies Programme[81] has a commendable example of an initiative in polling public opinion regarding quantum technologies. As part of this program, the Engineering and Physical Research Council (EPSRC) commissioned Kantar Public, a social research agency, to conduct a public dialogue aimed at gathering insights from a representative sample of the general public regarding their views on Quantum Technologies.

A stakeholder dialogue was divided into two waves of full-day public workshops held in Oxford, Glasgow, Birmingham, and York. The 77 participants took part in both sessions of these programs. To provide a complete representation of the UK population and to capture a wide range of viewpoints and perspectives, participants were carefully recruited. It is crucial to remember that this qualitative research's goal was to explore the participants' nuanced opinions and responses rather than aiming for statistical representativeness.

The findings highlight a widespread familiarity with the term "quantum" but a limited understanding of its underlying principles. The majority of participants had a small number of superficial associations, which were primarily related to "advanced technology" and science/physics. As several stakeholders had anticipated, no one mentioned quantum being "spooky" or "weird." Nevertheless, a significant number of participants showed various emotions based on their level of engagement with science. Those less involved in science exhibited anxiety, while participants with a greater interest in science felt curious and excited. Participants' enthusiasm and engagement levels improved as they learned more about QTs, mostly as a result of the anticipated advantages QTs could have for their own lives. No

[81] The UK National Quantum Technologies Programme, Link

participant showed signs of becoming more unfavorable toward QTs, while a few remained disinterested in science.

Concerns were raised during the discussion regarding the creation and application of QTs, as well as more general technological issues. Participants questioned who would be in charge of QT development and whether choices might be made solely for corporate profit, potentially at the expense of the general welfare. Access to QTs and the potential for widening socioeconomic divides were also raised. Participants expressed concern about the automation of certain jobs, notably those involving driving, analysis, and logistics. Participants questioned the total contribution of QTs to climate change, which was another concern. Additionally, particular issues with the QTs covered in the sessions came to light. Participants raised concern over the possibility of a global arms race in which countries would feel obligated to make defensive quantum computer investments to maintain security. The misuse of encryption technology for illicit activities including terrorism, organized crime, and tax evasion was also addressed, as well as the misuse of QTs for hacking and cyberwarfare.

It is essential to convey accurate information and involve the general public in comprehending the underlying ideas and implications of quantum mechanics given the great potential of quantum technology to transform numerous sectors. A complex strategy that includes educational initiatives, outreach programs, public lectures, interactive demonstrations, and collaborative partnerships with educational institutions, industry stakeholders, and government bodies could help to contribute to public awareness. By fostering a scientifically informed society and facilitating active dialogue, we strive to empower individuals with the necessary knowledge to make informed decisions regarding quantum technologies, ultimately ensuring their responsible and beneficial integration into our rapidly advancing world.

VIII. Conclusion

Summary of the main arguments and findings of the thesis.

Quantum technologies have emerged as a revolutionary innovation, attracting the attention of the world community to their ability to significantly transform all the dimensions of our lives and solve complex problems at unprecedented speeds. This has sparked a race among leading nations to achieve quantum supremacy. However, as this technology advances, it raises a host

of legal, ethical, and security concerns that require careful consideration. This thesis explores the unique field of quantum technologies and examines the legal, social, political and ethical issues it raises today. It is in line with European authorities' goals to create flexible legal frameworks, ensuring a transition to post-quantum security, and re-evaluate fundamental legal principles in the field of quantum technology. This thesis examines the regulatory dynamics in different countries, the potential impacts, and the risks associated with the development of quantum technology and digital transformation of society forced by quantum development.

There is a proposal to introduce the concept of responsible QT and establish Principles for Responsible QT in order to guarantee that the ethical, legal, economical, and political factors advance alongside the shaping of QTs. Normatively, the objective is to adapt existing legal principles while reducing potential hazards by putting appropriate technical, organizational, and policy measures in place. Quantum Technologies Regulatory Sandboxes can be used to promote QT's continuing development. To achieve a balance between development and regulation, a multilateral strategy for quantum regulation is necessary. It is necessary to develop a strong regulatory framework that promotes beneficial outcomes while limiting potential risks by adopting ethical principles, technical standards, and human-centered strategies. After profound analyzing of the legal practice, conclusions were drawn about possible adjustments in the QT regulatory approaches. The complexity of applying General Data Protection Regulation principles to the realm of QT is explored in depth in this paper. Here also were discussed issues related to IP rights and were suggested possible regulatory measures. It contributes significantly to the effort to regulate quantum technologies by offering a comprehensive and innovative approach and proposing provisionss into how ethical and legal regulation can interact with the specific nature of quantum technology.Additionally, this thesis provides a valuable guide for incorporating post-quantum cryptography into already-in place security procedures. PQC is crucial for strengthening data protection against future quantum attacks, and it's effective implementation is essential for guaranteeing the security of sensitive data in our increasingly quantum-driven environment. Furthermore, due to the enormous potential of quantum technology to change numerous industries, thia thesis suggests raising awarness and involving the general public in comprehending QT and consequences of it's implementation, arguing that it is essential, and proposes realization of educational initiatives, outreach programs, public lectures and other appropriate measures.

IX. Bibliography

Legislature and National Strategies

1. "Australian National Quantum Strategy." *Australian Government, Department of Industry, Science and Resources.* Link
2. "Army Quantum Technology Roadmap." *Australian Army Research Center.* Link
3. "National Quantum-Safe Network." *Centre for Quantum Technologies (CQT).* Link
4. "Cybersecurity Legislation in 2021." *National Conference of State Legislatures (NCSL)*. Link
5. Directive 2009/24/EC, of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs. *2009 Official Journal of the European Union (O.J.)*, L 111, p. 16. Link
6. "Regulation (EU) 2021/694 of The European Parliament and of The Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240." *Official Journal of the European Union.* Link
7. "European Declaration on Digital Rights and Principles for the Digital Decade." Brussels, 26.1.2022. COM(2022) 28 final. *Europien Comission.* Link
8. "Executive Order on Improving the Nation's Cybersecurity." *The White House.* Link
9. Fairfield, J. "The Law of Quantum Computing." *Harvard Journal of Law & Technology.*Link
10. "General Data Protection Regulation (GDPR)." *Horizon 2020 Framework Programme of the European Union.* Link
11. "GOST R 57257-2016 Nanotechnologies. Part 12. Quantum Phenomena. Terms and Definitions." *Federal Agency for Technical Regulation and Metrolog.* Link
12. "GOST R 58568-2019 Optics and Photonics. Photonics. Terms and Definitions." *Federal Agency for Technical Regulation and Metrolog.* Link
13. "Canada's National Quantum Strategy." *Government of Canada.* Link
14. Childs, A. "Quantum Algorithms: An Overview." Communications of the ACM, vol. 55, no. 10, 2012, pp. 58-67.
15. "Horizon 2020 - Funding Programmes and Open Calls." *European Commission - Research and Innovation,* Link
16. "Strategic Planning on the Quantum Science and Technology R&D." Quantum in Korea. *Link*

17. "Made in China 2025: Plan to Dominate Manufacturing." *FDIChina*. Link
18. "National Security Strategy of the Russian Federation dated July 02, 2021." *Ministry of Foreign Affairs of the Russian Federation*. Link
19. "Preparing for quantum-safe cryptography." *National Cyber Security Center*. Link
20. "Proposal for a Decision establishing the 2030 Policy Programme - Path to the Digital Decade." *Shaping Europe's digital future - European Commission*. Link
21. "Quantum technologies Roadmap for developing the "end-to-end" digital technology." *Ministry of Digital Development, Communications and Mass Media of the Russian Federation* Link
22. "Quantum Technologies Flagship.Digital Strategy." *European Commission*. Link
23. "Quantum Technologies - RP2023." Rolling Plan ICT Standardisation - Joinup - *European Commission*. Link
24. "Regulation (EU) 2021/694 of the European Parliament and of the Council Establishing the Text - H.R.813 - 118th Congress (2023-2024): Global Investment in American Jobs Act of 2023." *Library of Congress*. Link
25. "Standardization Roadmap on Quantum Technologies." *CEN-CENELEC Focus Group on Quantum Technologies*, 2023, Link
26. "Text - H.R.6227 - 115th Congress (2017-2018): National Quantum Initiative Act.", *Library of Congress* Link
27. "The Agreement on Trade-Related Aspects of Intellectual Property Rights." *The World Trade Organization*, 1994. Link
28. "The European Quantum Communication Infrastructure Initiative." *Shaping Europe's digital future - European Commission*. Link
29. "UK National Quantum Technologies Programme (NQTP)." Link
30. "285-Years Plan for Quantum Technologies." *The Ministry of Science and ICT*. Link

Books, monographs, articles, reports

1. Aho, B., & Duffield, R. "Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China." Economy and Society, 49, 1-26. Link
2. Atik, J., & Jeutner, V. "Quantum computing and computational law." Law, Innovation and Technology, vol. 13, no. 2, 2021, pp. 302-324. DOI: 10.1080/17579961.2021.1977216. Link

3. Beullens, W., D'Anvers, J., et al. "POST-QUANTUM CRYPTOGRAPHY: Current State and Quantum Mitigation." (2021). Link
4. Bohr, N. "Discussions with Einstein on Epistemological Problems in Atomic Physics." Link
5. Capeta, T. "Do Judicial Decision-Making and Quantum Mechanics Have Anything in Common? A Contribution to Realist Theories of Adjudication at the CJEU." SSRN Electronic Journal. (2019). Link
6. Calzati, S. "Shaping a Data Commoning Polity: Prospects and Challenges of a European Digital Sovereignty." Link
7. Copenhagen Interpretation of Quantum Mechanics. Link
8. Ritter, J., "Digital Justice in 2058: Trusting Our Survival to AI, Quantum and the Rule of Law." Link
9. De Angelis, M. "Omnia Sunt Communia. On the Commons and the Transformation to Postcapitalism." (2017). Link
10. Deltorn, J., Franck M. "Authorship in the Age of Machine Learning and Artificial Intelligence." *Ctr. Int'l Intell. Prop. Stud., Research Paper No. 2018-10*, Link
11. Drexl, J. "Designing Competitive Markets for Industrial Data - Between Propertisation and Access." Link
12. Hemel, Daniel J., and Lisa Larrimore Ouellette. "Innovation Policy Pluralism." Yale Law Journal, vol. 128, 2019. Link
13. Heisenberg, Werner. "The Physical Principles of the Quantum Theory." Dover Publications, 1949. Link
14. Hossenfelder, S. "Einstein's Spooky Action at a Distance." (2021). Link
15. Feynman, R. P. "Simulating physics with computers." International Journal of Theoretical Physics, vol. 21, 1982, pp. 467-488.
16. Gervai, D., & Derclaye, E. "The scope of computer program protection after SAS: are we closer to answers?" European Intellectual Property Review, vol. 34, no. 8, 2012, pp. 565-572.
17. Ghose, S. "A Beginner's Guide to Quantum Computing." Link
18. Goldstein, Paul, and Bernt Hugenholtz. *International Copyright: Principles, Law, and Practice*, 4th ed., 2019.

19. Greely, H., "Governing Emerging Technologies - Looking Forward with Horizon Scanning and Looking Back with Technology Audits." Glob. Pub. Pol'y & Governance, 2022. Link
20. Gromova, E., & Petrenko, S. "Quantum Law: the Beginning." Link
21. Hess, C., & Ostrom, E. (Eds.). Understanding knowledge as a commons: From theory to practice. MIT Press, 2007. Link
22. Huang, Y. "Quantum microarchitecture." (2022). Link
23. Jenet, A., Trefzger, A., et al. Standards4Quantum: Making Quantum Technology Ready for Industry - Putting Science into Standards. EU Publications Office, Luxembourg, 2022. Link
24. Jeutner, V. "Morals & Machines." "The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers." (2021). Link
25. Kop, M., & Brongersma, M. "Integrating Bespoke IP Regimes for Quantum Technology into National Security Policy." Working Paper, 2021. Link
26. Kop, M., & Aboy, M. "Intellectual property in quantum computing and market power: a theoretical discussion and empirical analysis." Journal of Intellectual Property Law & Practice, vol. 17, no. 8, 2022, pp. 613-628. Link
27. Kop, M., et al. "Forecasting and Social Change." Elsevier, vol. 146(C), 2019, pp. 626-627.
28. Kop, M. "Regulating Transformative Technology in the Quantum Age: Intellectual Property, Standardization & Sustainable Innovation." STAN.–VIENNA TRANSATLANTIC TECH. L. F., 2020. Link
29. Kop, M., & Aboy, M., et al. "Towards Responsible Quantum Technology." (2023). Link
30. Lake, R., & Simbierowicz, S. "The Bluefors Dilution Refrigerator as an Integrated Quantum Measurement System." Bluefors Quantum Team, Bluefors Oy, 2021. Link
31. Lemley, Mark A. "Property, Intellectual Property, and Free Riding." *Texas Law Review*, vol. 83, 2005, pp. 1031-1032.
32. Massmann, R., Grantham, N., & Mailewa, A. "Quantum Computing: An Assessment into the Impacts of Post-Quantum Cryptography." (2023). Link
33. Matteo M. Wauters, Emanuele Panizon, Glen B. Mbeng, and Giuseppe E. Santoro. "Reinforcement-learning-assisted quantum optimization." (2020). Link

34. Menell, Peter S., Mark A. Lemley, Robert P. Merges, and Shyamkrishna Balganesh. *Intellectual Property in the New Technological Age*, 2020, p. 35.
35. Montanaro, A. "Quantum Algorithms: An Overview." Npj Quantum Information, vol. 2, no. 1, 2016. Link
36. Murgia, M., & Waters, R. "Google Claims to Have Reached Quantum Supremacy." *Financial Times*, 2019. Link
37. National Academies of Sciences, Engineering, and Medicine. Quantum Computing: Progress and Prospects. 2019. Link
38. Nederveen Pieterse, J. "China's contingencies and globalization." Third World Quarterly, 36(11), 1985–2001.
39. Ness, S. & Chase, P. "How GDPR could affect the transatlantic relationship." Link
40. "NIST's Quantum-Safe Standards." *IBM Research Blog*. Link
41. O. van Deventer, N. Spethmann, et al. "Towards European Standards for Quantum Technologies." (2022). Link
42. Olejnik, L., & Riemann, R. "Quantum Computing and Cryptography." (2020). Link
43. "Progress and Prospects." The National Academies Press. Link
44. "Post-Quantum Cryptography - PQCrypto 2022." Lecture Notes in Computer Science. Link
45. "Quantum Computing Report: Analysis." GQI. Link
46. "Quantum Technologies and the Advent of the Quantum Internet in the European Union." *EUR. UNION*, Link
47. Rahmatian, A. "Copyright and Creativity: The Making of Property Rights in Creative Works." Link
48. Rosalind T. "Written in Stone? Liberty, Equality, Orality and the Codification of Law." (1995). Link
49. Rahmatian, A. "Copyright and Creativity: The Making of Property Rights in Creative Works." Link
50. "Science, research and innovation performance of the EU 2020." Link
51. Shor, P. "Algorithms for quantum computation: Discrete logarithms and factoring." In 35th FOCS, IEEE Computer Society Press, Nov. 1994, pp. 124–134.
52. Styer, Daniel F. "The Strange World of Quantum Mechanics." Cambridge; New York: Cambridge University Press. Link

53. Szpunar, Maciej. "Territoriality of Union Law in The Era of Globalisation." In *Evolution des rapports entre les ordres juridiques de l'Union Européenne, international et nationaux: Liber Amicorum Jiří Malenovský*, 149, 2020.
54. Tiersma, Peter M., "Parchment, Paper, Pixels: Law and the Technologies of Communication." *University of Chicago Press, 2010.* Link
55. "Transformative Technology in the Quantum Age: Intellectual Property, Standardization & Sustainable Innovation." Stan.–Vienna Transatlantic Tech. L. F., 2020. Link
56. Yipeng H., "Quantum microarchitecture." 2022. Link
57. Zhang, Y., Porter, A., Chiavetta, D., et al. "Forecasting technical emergence: An introduction." Technological Forecasting and Social Change. Link

Summary

In the history of science, some discoveries are remembered as turning points that changed the direction of human development. One such revolutionary frontier has been the development of quantum technologies, a field where the conventional and the transcendental coexist. These innovations have caught the interest of the scientific community.

At its core, quantum technology aims to take advantage of the complex laws that regulate how particles behave at the quantum level—a domain where particles can exist in multiple states at once, where information can be sent instantly over great distances, and where computing power can exceed the limits of what is imaginable. We have the chance to rethink the limits of what is possible because of these quantum innovations.

The promise of unmatched computational power, unbreakable encryption, and revolutionary advancements in fields as diverse as medicine, materials science, and artificial intelligence motivate nations and institutions to enter this race in search of quantum supremacy. However, as they explore this quantum frontier, they also run into a number of deep yet baffling legal, ethical, and security issues.

This thesis aims to shed light on the unique world of quantum technology, where quantum laws replace classical and where there is room for both ground-breaking invention and significant disruption. We will consider possible legal frameworks, moral conundrums, and geopolitical dynamics that quantum technologies unfold outside the confines of the lab. This thesis acts as a guide to traverse the new landscape that quantum technologies present, from intellectual property conflicts to the ethical implications of quantum monitoring, from global collaboration to the race for quantum dominance.

As we already mentioned the potential of quantum technologies is promising. This potentiality goes beyond simple technological development and affects the very core of how we see the world. It symbolizes a domain where the fundamental rules of physics may be potentially bent, where qubits and classical bits (qubits) coexist in a delicate and precarious equilibrium, and where the traditional view of the future may encounter enormous difficulties.

Leading nations are competing to establish their quantum dominance due to its ability to transform whole industries and provide unparalleled speedy solutions to complicated challenges. But as this technology develops, it raises a number of moral, ethical, and security issues that need to be carefully taken into account. In this essay, we examine the contemporary legal, social, political, and ethical issues that surround the unique field of quantum computing. Undoubtedly, a detailed grasp of the characteristics of quantum computers is necessary for thorough regulation.

New methods of processing and sending information, sensing, and carrying out computations are being developed thanks to the cutting-edge and quickly developing field of quantum technologies. A fundamental theory of physics called quantum mechanics defines how particles behave at the tiniest scales and introduces a number of unusual and illogical occurrences that serve as the foundation for quantum technology. A thorough foundation for understanding the complex behaviour of matter and energy at the tiniest scales is provided by quantum mechanics. It mostly functions at the level of atoms and subatomic particles, where traditional physics is no longer relevant. To appreciate the broader legal implications, it is sufficient to comprehend the underlying quantum characteristics that distinguish them apart from classical computers, such as the principles of superposition, entanglement, and interference. A cornerstone of quantum mechanics is the concept of quantum superposition. Things like location or momentum are always well defined in classical mechanics. Even while we might not always be aware of what they are, this is a problem with our comprehension rather than with the physical system. A particle can exist in a superposition of several states according to quantum physics. It only interacts in ways that can be described by having a superposition of multiple states, even though a measurement always finds it in the same state. It only interacts in ways that can be described by having a superposition of multiple states, even though a measurement always finds it in the same state. Another crucial idea is called entanglement, which occurs when quantum particles are so closely connected that their states are instantly affected by one another even though they are separated by great distances. This phenomena has significant implications for quantum information, communication, and encryption, and was frequently referred to as "spooky action at a distance" by Einstein.

The interaction and combining of diverse outcome probabilities results in quantum interference, a consequence of the wave-like structure of quantum particles. Complex

behavioral patterns are produced as a result, which traditional systems are unable to reproduce. In some situations, quantum algorithms use interference to do computing tasks more effectively than traditional computers. The fundamental idea of quantum mechanics is energy quantization, which restricts energy levels to certain discrete values as opposed to the continuous spectrum of conventional physics. The quantized electron energy levels within atoms are one of the characteristic phenomena that result from this quantization.The fact that particles like electrons and photons show wave-particle duality is another aspect of quantum physics. These particles exhibit both wave-like and particle-like properties, with wave functions acting as probability distributions to describe their activity.Uncertainty principle, made famous by Werner Heisenberg, is a cornerstone of quantum physics. It claims that knowing some pairs of particle attributes simultaneously, such as location and momentum, has inherent restrictions. Quantum measurements now have a basic unpredictability.

The idea of quantum tunneling, in which particles can go around energy barriers that traditional physics deems impassable, is also introduced by quantum mechanics. This phenomenon has real-world uses, particularly in nuclear physics and electronics.Probability plays a key part in quantum mechanics. It provides a probabilistic framework for forecasting measurement results while providing information on the likelihood of different outcomes without making precise individual predictions.

Due to its computational capability, QT has the potential to alter political priorities, economic sectors, and social institutions. Breakthroughs in a variety of fields, including but not limited to cryptographic systems, pharmacological research, materials engineering, and meteorological forecasting, have been made feasible by their ability to significantly speed up operations and carry out tasks that are difficult for traditional computers. Quantum optimizations improve accuracy and efficiency in a variety of industries, such as financial modeling, supply chain logistics, and energy grids.

Quantum sensors also advance space exploration, climate modeling, environmental monitoring, and aviation navigation. Applications for artificial intelligence are made possible by quantum machine learning, while cybersecurity is improved by quantum communication networks. Since quantum technologies have the potential to transform businesses, boost productivity, and address challenging global issues, they are an important study field with wide-ranging implications for the world.

"How can existing regulatory frameworks be adapted to address the unique characteristics and capabilities of quantum technologies?" is the research issue that is addressed in this study. It is a crucial investigation in the quickly developing field of emerging technology regulation. Modern regulatory paradigms are put to the test by quantum technologies' unparalleled computational capacity and transformational potential. This query emphasizes the importance of investigating novel regulatory strategies and coordinating current laws with quickly evolving developments. Understanding how to modify regulatory frameworks is crucial as quantum technology enters a variety of industries, including finance, healthcare, public administration, and many others, to ensure responsible and secure integration. This research question provides an essential starting point for examining the dynamic governance environment of quantum computing, illuminating approaches.

The article's methodology, which incorporates a thorough literature research, expert interviews, and comparative analysis, is based on a comprehensive approach. First, a thorough analysis of the body of research on quantum technologies and how to regulate them was done. In order to pinpoint the most important trends, obstacles, and best practices in the area, a detailed analysis of academic papers, legal documents, government reports, and business publications was conducted. Since its commencement at the turn of the 20th century, the field of quantum technologies has made remarkable progress. Quantum mechanics was first established by scientists like Albert Einstein, Niels Bohr, and Erwin Schrödinger, who later opened the path for quantum technology. Contextualizing the existing regulatory landscape involves understanding the practical applications of quantum technology. As a result, this article's examination of quantum technologies is thorough and includes a look at the major factors that support a sensible approach to using them. It is essential to have a solid understanding of the technical features in order to examine the application and regulation of technologies.

By presenting a thorough and original strategy, this thesis significantly advances the goals of regulating quantum technology. It addresses the objectives established by European authorities to develop novel and adaptable legal frameworks, migrate to post-quantum security measures, and evaluate core regulatory principles in the quantum technology sphere. The European Commission unveiled the Quantum Flagship initiative in 2018 as a significant and substantial research endeavor. In addition to providing significant support for the growth of a vibrant quantum technology industry in Europe, this endeavor aims to strengthen

European leadership and know-how in the field of research. The 2030 Path to the Digital Decade strategic program also included infrastructure development and quantum technology promotion as major objectives. The technological maturity and widespread application of quantum technologies are increasing. Therefore, the promotion of well-coordinated and specialized regulation activities is one of the initiatives mentioned by the Quantum Flagship in its Strategic Research Agenda to speed growth and adoption.

Organizations like CEN & CENELEC, ENISA, and ETSI are working to advance European regulation in this area. For the Quantum Technologies industry, regulation can cover quality standards, cybersecurity, and adherence to European law in addition to criteria that serve as a foundation for certification. The article's goal is to encourage the development and general use of quantum technologies by promoting an innovative approach in this area. This article's insights help shape the regulatory environment for quantum technologies, encourage their safe and efficient integration into a variety of businesses, and eventually help them reach their full potential.

This thesis explores the legal implications of quantum technologies, emphasizing their complex and dynamic character. We explore a number of important legal topics, such as data protection, intellectual property rights, and the recently developed area of quantum law. Quantum technologies have the potential to revolutionize a variety of aspects of our lives, including data processing, communication, and encryption. It is more crucial than ever to address any potential effects these technologies might have on data privacy and protection.

The General Data Protection Regulation (GDPR) of the European Union is where the primary concerns are raised. As there are certain laws that govern the quantum world, the process of gathering, processing, storing, and sending quantum information is different from the classical one. The manner in which the criteria governing the functioning of quantum computers are set is one of the most significant legal challenges relating to the development of quantum computers. The numerous choices made by individuals who design and implement quantum technologies have a significant impact on their evolution. These choices are never neutral, and the results frequently have long-lasting effects. Technology design decisions can never be thought of as neutral since they are always influenced by ideals, presumptions, possible consequences, and historical and social context.

As a result, the choices taken by the quantum computing forerunners will likely affect how quantum computers are used and developed in the future. The potential implications of trade secret trademarks in the context of quantum computing and the potential effects they may have on innovation, disclosure, and technology transfer are also vital to bring up.

The use of trade secrets and patents must be carefully balanced in the field of quantum computing. Many businesses use a hybrid approach, securing crucial data with IP rights. The final decision on an intellectual property protection strategy is influenced by a number of variables, including the technology involved, company goals, the state of the market, and the regulatory environment.

IP rights are not the only option for allocation and promotion tactics for innovation. The application of innovation policy pluralism (i.e., matching IP alternatives like antitrust law, contract law, consumer privacy protection, tax law, standardization and certification, as well as awards, subsidies, public-private finance, contests, penalties and fines) is a tool that policymakers can use.

The range of protection strategies is made possible by innovation policy pluralism, which also makes it easier to combine different instruments and tailor policies to specific settings and objectives. It helps decision-makers to meet the various opportunities and difficulties brought about by innovations while also balancing competition, fostering social benefits, and attending to the demands of various stakeholders. Because innovation incentive and reward processes, consequences, and safety/security concerns varied by industry and technology, policymakers should more explicitly discriminate across economic sectors when devising regulatory solutions. Furthermore, intellectual property rules might not be as important in a quantum and AI-driven future when invention, replication, and distribution are all affordable.

The way that lawyers think may alter as quantum technologies become more widespread. It has already been raised if computational law should be transformed into quantum computational law, which would enable more objective judicial decisions and the solution of supposedly intractable legal issues by drawing on the characteristics of quantum phenomena. The investigation of the legal ramifications of quantum technology has found a complicated and quickly changing environment. We have examined a number of significant legal concerns relating to quantum technologies throughout this chapter. It is clear that the legal environment around quantum technologies is in flux, and the way forward will need for a multifaceted

strategy combining decision-makers, legal professionals, scientists, and business leaders. The legal community must actively participate in continuing discussions and iterative updates as quantum technologies continue to transform our environment in order to adapt and create coherent and futuristic legal frameworks.

Furthermore, a risk-centered approach is required given the inherent uncertainties surrounding the use of new QT in real-world scenarios, goods, and systems. This strategy promotes long-term innovation, perhaps through Quantum Technologies Regulatory Sandboxes (QTRS), which allow organizations and researchers to explore and advance quantum technologies in designated environments under predetermined rules. The development of controlled experiments and the advancement of quantum technologies in a field that is constantly changing and fundamentally uncertain is made possible by the use of regulatory sandboxes for quantum technologies, which is a ground-breaking paradigm in the regulatory landscape. Given the developing and transformative character of quantum technologies, these specialized regulatory frameworks seek to strike a delicate balance between supporting innovation and protecting against possible hazards.

These "sandboxes" give researchers, companies, and governments a controlled setting in which to test and improve quantum-based applications like quantum computing, quantum communication, and quantum cryptography, while also giving regulators a chance to learn more about the particular difficulties and implications brought on by quantum advancements. Regulatory sandboxes encourage a cooperative environment where participants can jointly investigate the limits of quantum technologies, evaluate their feasibility, and refine regulatory frameworks to assure compliance, safety, and security. The advent of Quantum Technologies Regulatory Sandboxes as quantum technologies develop emphasizes regulatory bodies' proactive approach to adjusting to a time when the traditional principles of technology governance are being redefined by the complexities of quantum physics.

A summary of the current state of Post-Quantum Cryptography (PQC) standardization activities is also provided by this research. PQC is a group of cryptographic methods that includes key creation and digital signatures that provides conjectured security even from an adversary using a quantum computer. A distinction between PQC and Quantum Cryptography is essential because PQC focuses on creating cryptographic tools that can be used with current classical computers and that may fend off attacks from both classical and

quantum cryptanalysis, whereas Quantum Cryptography deals with cryptographic solutions that make use of quantum physics (for example, Quantum Key Distribution).

The goal of post-quantum cryptography, a subfield of cryptography, is to create cryptographic protocols and algorithms that will continue to be secure in the presence of quantum computers. By utilizing their superior processing power and capacity to complete some mathematical problems much more quickly than classical computers, quantum computers, in contrast to classical ones, have the potential to crack many of the commonly used cryptographic systems. The awareness that once large-scale, operational quantum computers are a reality, they could effectively overcome the challenges underlying popular encryption techniques, including RSA and ECC (Elliptic Curve Cryptography), leads to the necessity for post-quantum cryptography. As a result, quantum computers might be able to decrypt sensitive data, such as communications, financial transactions, and personal information. By creating cryptographic algorithms that are thought to be quantum-resistant, post-quantum cryptography aims to remedy this weakness. These algorithms are thought to rely on mathematical puzzles that are challenging for even quantum computers to answer effectively.

We examine the quantum era's digital transformation of society and underline the need for PQC to deal with the security issues these developments provide. It offers an assessment of the numerous suggestions made within the major PQC algorithm categories. Additionally, it offers a roadmap for the incorporation and acceptance of PQC measures, which recommends a plan for enforcing a safe quantum future.

With the introduction of quantum computing, new views, methods, and techniques for guaranteeing information security and confidentiality are now possible. While advances in quantum computing have improved networks' secrecy, integrity, and availability by strengthening their ability to fend off intrusions, more reliable and secure means of exchanging information are still required. Our understanding of security and secrecy is altered by the quantum era, which also brings forth new problems and innovative techniques for protecting data from intrusion and eavesdropping. The transition from classical to quantum computation has profound ramifications and the potential to compromise the security of the currently used information protection techniques. It is critical to protect personal, business, and governmental data because of the tremendous growth in cyber dangers brought on by the abundance of data.

If a post-quantum security mechanism is not put in place before an attacker has access to a quantum computer, data confidentiality and security may be jeopardized. Post-Quantum Cryptography (PQC) could provide security.

This study puts out a framework for Responsible Quantum Technologies (RQT), which takes into account issues of law, morality, politics, and society in the advancement of quantum technology. For organizations in wealthy nations, the creation of post-quantum cybersecurity norms has assumed critical importance. The attempts and initiatives made by various authorities to alter cybersecurity standards in the context of quantum developments are examined in this article.

At this early stage, when quantum technologies are still adapting and developing, the suggested regulatory framework seeks to serve as a starting point for continued development. It should be viewed as a unique methodological framework created for the features of quantum technology. The main objective is to develop a regulatory framework for QT that carefully examines legal doctrines and incorporates safeguards to properly provide the required degree of cybersecurity. This effort aims to involve a wide range of stakeholders, including policymakers, scientists, and researchers, in order to establish a cooperative atmosphere for the creation and application of QT rules. In order to ensure that the development of QT remains morally upright, it is crucial to lay the foundation for responsible QT. Post-quantum cryptography requires a gradual transition. Public and private organizations are currently waiting for national authorities to standardize PQC algorithms and provide a precise transition strategy.

There are, however, circumstances where the quantum risk is just intolerable. In these circumstances, hybrid systems that mix pre-quantum and post-quantum techniques can be used to adopt a more assertive attitude. Pre-shared keys are also incorporated into all public-key cryptography keys created by these hybrid systems, thus protecting the secrecy of their data from the grave threat posed by a quantum-capable attacker. Given the dearth of comprehensive best practices for Responsible QT-oriented policymaking, there is little scope for normative authority to offer detailed substantive advice.

Addressing the growing need to examine and reassess our data protection, intellectual property, cybersecurity, and other legislation that are relevant to QT governance is the main challenge. We are unable to guarantee the effectiveness of our regulatory frameworks. To

adjust to the shifting nature of technology and its legal ramifications, we ought to think about a new regulatory strategy. A difficult balance between supporting innovation and preserving individual rights must be struck in order to construct effective and comprehensive regulatory frameworks.

It is proposed to construct the notion of responsible QT to ensure that ethical, legal, economical, and political frameworks are evolving while QTs are still formable. The objective is to adapt existing legal principles while reducing any negative risk by putting in place technical, organizational, and policy measures that are appropriate to the risk, from a normative perspective. This study examined the dangers of quantum computing in order to lay the groundwork for the Responsible Quantum Technology (RQT) concept. The quantum regulation takes into account the ethical, legal, societal, and policy ramifications. The adoption of this extensive set of guidelines represents a crucial turning point in the development of the regulatory environment for quantum technology. These guidelines offer a strong framework upon which governments can work together to develop and utilize quantum breakthroughs in a responsible and morally sound manner. These principles will act as a flexible road map for the development of rules that reflect both the transformational potential and the ethical stewardship of quantum innovation as those technologies continue to advance.

As different regions can have distinct interests and issues surrounding quantum technology, the specifics of each QTRS will differ. The main objective is to foster responsible development of quantum technologies in a regulated setting while facilitating innovation and risk mitigation. Quantum technologies pose a range of risks with varying degrees of seriousness, from potentially life-changing effects to very minor worries. As quantum breakthroughs proceed, it is crucial to comprehend and manage these risks. At the top of the risk hierarchy are life-and-death medical and judicial decisions, national security, and defense concerns. Quantum technologies, particularly in quantum computing, possess the capacity to break existing encryption methods.

However, a comprehensive approach also involves addressing the less severe but still significant issues. Economic implications, data security, ethical considerations, and operational disruptions all represent facets of the quantum technology landscape that require thoughtful and proactive management. Neglecting these lower-level risks can lead to unintended consequences and challenges that may accumulate over time. Understanding the

hierarchical pattern of dangers related to quantum technologies emphasizes the significance of striking a balance between current goals and long-term considerations. It necessitates a calculated strategy that addresses the most pressing issues without ignoring the wider moral, societal, and practical ramifications of this game-changing technology. Policymakers, researchers, and stakeholders should recognize the hierarchical nature of these hazards. It emphasizes the necessity for a multifaceted strategy that addresses both the less serious but still important problems related to the developing field of quantum technologies while also giving priority to the most important ones.In order to effectively minimize these high-stakes hazards, policymakers and academics must devote significant money and efforts.

In order to achieve a delicate balance between development and regulation, a multilateral strategy for quantum regulation is essential. By incorporating ethical principles, technical standards, and human-centric strategies, we may build a robust regulatory quantum framework that encourages beneficial outcomes while lowering possible dangers.

We should use experimental legal regimes, or regulatory sandboxes, in our search for the best methods for regulating quantum technologies and developing the legal applications of such technologies. In such a system, some regulatory obligations are temporarily suspended in an effort to evaluate the practicality of invention and provide the best possible legal framework for it. Notably, the flexibility of regulatory sandboxes enables the development of proactive law that keeps up with digitization. As a result, we could develop adaptable legal frameworks for cutting-edge technologies.

Although this dynamic connection between law and technology is sometimes depicted as a dialectical system, it often ignores the significant role that society plays. It is crucial to understand that culture and laws aren't the only things changing—the way society views and accepts technological advancements is also changing. This sociological change is advancing even more quickly than legal changes, making it a crucial element in determining the direction of technology in the future. customers are now challenging the paternalistic attitude that governments have historically had toward technology users and customers. Users are becoming more proactive in reducing dangers. Essentially, users are evolving into independent regulators.

Promoting debates and conversations on the subject is a key step in raising awareness of quantum issues. The general population must be made aware about quantum technologies.

Although the academic, technological, and policymaking sectors have shown a great deal of interest in quantum technologies, little has been done to learn the public's viewpoint on the matter. A notable example of a project to gauge public opinion on quantum technologies is the UK National Quantum Technologies Program. The Engineering and Physical Research Council (EPSRC) commissioned Kantar Public, a social research organization, to carry out a public dialogue as part of this program in order to gather opinions on quantum technologies from a representative sample of the general population.

Given the immense potential for quantum technology to alter a variety of industries, it is imperative to disseminate correct information and engage the general people in understanding the fundamental concepts and implications of quantum mechanics. Public awareness could be increased by implementing a sophisticated plan that combines educational initiatives, outreach initiatives, public lectures, interactive demonstrations, and cooperative relationships with educational institutions, business stakeholders, and governmental organizations. We aim to equip people with the information they need to make educated decisions about quantum technologies, thereby assuring their responsible and advantageous integration into our fast evolving world. To do this, we promote a scientifically informed society and actively encourage dialogue.

To sum up, a crucial component of the fast changing quantum technology landscape is the legal framework ensuring safe creation, adoption, and use of quantum technologies. Quantum technology has ignited a worldwide scramble to harness its power because of its tremendous potential to change industries as diverse as computing, cryptography, communications, and sensing. However, this revolutionary capacity raises a number of intricate regulatory problems, including those relating to security, intellectual property rights, morality, and international collaboration.

The whole community has taken notice of quantum technologies as a revolutionary development because of their potential to profoundly alter all facets of our life and swiftly find solutions to complex issues. Leading nations are now competing to become the quantum supremacy. But as this technology develops, it brings up a number of moral, ethical, and security issues that need to be carefully taken into account. This thesis addresses the contemporary legal, social, political, and ethical challenges that the novel field of quantum technology brings.

This thesis is consistent with the objectives of European authorities to develop adaptable legal frameworks, provide a transition to post-quantum security, and reexamine fundamental legal principles in the context of quantum technology.

It is suggested that the idea of responsible QT be introduced and the Principles for Responsible QT to be established in order to ensure that the development of QTs happens in tandem with the advancement of ethical, legal, economic, and political issues. Normatively speaking, the goal is to modify current legal principles while lowering potential risks by implementing the proper technical, organizational, and regulatory procedures.

It is a delicate balance to encourage the growth of quantum technologies while assuring responsible innovation and risk management. The creation of regulatory sandboxes designed especially for quantum technology is one efficient method for achieving this balance. These "sandboxes" offer regulated settings in which corporations and researchers can experiment with quantum applications. This promotes innovation while enabling regulators to keep an eye on and comprehend the particular difficulties presented by quantum developments. However, a multilateral approach to quantum governance is essential given the global nature of quantum technologies and their potential for revolutionary impacts. In order to prevent fragmentation and promote global cooperation, regulatory frameworks for quantum technology must be standardized across all relevant jurisdictions.

This thesis also examines the potential changes Quantum Technologies bring in terms of comprehensive digital transformation across society, instigating a paradigm shift in multiple domains. This holistic transformation encompasses a wide array of aspects that collectively redefine how our society operates. The interconnection between technology, the economy, society, and regulation represents a complex and mutually influential dynamic, forming the cornerstone of contemporary societal progress and development. This intricate interplay illustrates a mutual connection where technology exerts influence on, and is shaped by the broader economic, societal, and regulatory contexts.

Technological progress serves as a potent engine for economic growth and innovative regulatory approaches. Conversely, economic forces and laws also steer technological development. Market demands, legal incentives, and benefit motives significantly influence the direction and pace of technological innovation. Beyond economics, technology has profound implications for society and people's modus operandi.

By implementing ethical principles, technical standards, and human-centered solutions, it is essential to create a robust regulatory framework that encourages positive outcomes while reducing potential hazards. A thorough analysis of the legal system led to conclusions about potential changes to the QT regulatory framework. The difficulty of implementing the principles of the General Data Protection Regulation in the field of QT is thoroughly examined in this study. Here, issues relating to intellectual property rights were also considered, and potential regulatory actions were offered. By providing a thorough and cutting-edge methodology and suggesting insights into how ethical and legal regulation can interact with the unique character of quantum technology, it greatly contributes to the attempt to regulate quantum technologies.

This paper also offers a useful approach for integrating post-quantum cryptography into current security practices. PQC is critical for bolstering data protection against potential quantum attacks, and its proper use is crucial for ensuring the security of sensitive data in our environment that is becoming more and more quantum-driven. This thesis also suggests increasing awareness and involving the general public in understanding QT and consequences of its implementation, arguing that it is essential, and proposes the realization of educational initiatives, outreach programs, public lectures, and other appropriate measures. This is because of the enormous potential of quantum technology to change many industries.

In conclusion, the regulatory framework for quantum computing is at a critical crossroads and must now figure out how to go through the undiscovered territory of this revolutionary technological frontier. With its unlocked potential to solve complex problems at an unprecedented scale and its ability to advance scientific research to new heights, quantum computing has the potential to transform a number of industries. But this technology breakthrough also raises significant societal, ethical, and security issues. Given the significance and ramifications of quantum technologies on a global scale, a multilateral and cooperative strategy is necessary. To provide consistency, prevent fragmentation, and deal with the intrinsically global nature of quantum technologies, international cooperation and the harmonization of regulatory frameworks are imperative.

To achieve the necessary delicate balance in this dynamic environment, politicians, researchers, and industry players must collaborate. This means respecting ethical standards, protecting personal information, and assuring security in addition to promoting the

responsible development of quantum computing. The pursuit of effective regulation is a shared journey as quantum technology's frontiers continue to widen. Here, the need for innovation meets the need for ethical and responsible regulation.