Centre d'étude des évolutions des technologies quantiques
/
Center for the Study of the Evolution of Quantum Technologies

CevoteQ Working Papers

CevoteQ Working Paper 2025/01

Quantum Technologies and Legal Transformations – Initial Reflections

Raphaël Maurel

University Bourgogne Europe, CREDIMI

ISSN : *in process*

Le CevoteQ est une activité du CREDIMI – Université Bourgogne Europe (*www.credimi.ube.fr*) initiée dans le cadre de la Chaire « Encadrement éthique et juridique des technologies quantiques » de l'Institut Universitaire de France

CevoteQ is an initiative of CREDIMI – Université Bourgogne Europe (*www.credimi.ube.fr*) launched under the auspices of the Chair "Ethical and Legal Framework of Quantum Technologies" at the Institut Universitaire de France.

Directeur scientifique du programme :
Raphaël Maurel

CREDIMI
Université Bourgogne Europe
4, bvd Gabriel
21000 DIJON
contact@cevoteq.com
www.cevoteq.com

institut universitaire de France

CevoteQ Working Paper 2025/01 - doi.org/10.5281/zenodo.15619401

Quantum Technologies and Legal Transformations – Initial Reflections

Raphaël Maurel[1]

Associate Professor in Law at the University of Bourgogne Europe, CREDIMI

January 2024

* * *

On August 16, 2016, China stunned the world by announcing the launch of the first quantum satellite from the Gobi Desert[2]. This technological marvel could send "entangled" photons to Earth, meaning they share a common property allowing them to interact over distances exceeding 1000 km, a principle of quantum physics known as entanglement. This marked the beginning of quantum communications, touted as unhackable because intercepting the communication would corrupt the data and alert the recipient. Essentially, data within photons used for communication can self-destruct upon interception.

Three years later, Google announced achieving "quantum supremacy" through a publication in Nature. This milestone involved performing a task in 200 seconds with a quantum computer that a classical computer could never accomplish, or would take an impractical amount of time[3]. Although IBM claimed its supercomputers could achieve the same feat in a few days, this was still a revolutionary advancement[4]. Quantum computing leverages the principle of "superposition," potentially creating "qubits" that defy classical physics. Classical computing relies on bits, which are either 1 or 0, transmitted as light signals through fiber optics. Quantum computers, however, use qubits that can be both 1 and 0 simultaneously, offering unprecedented computational power. Despite progress, stable quantum computers remain elusive due to complex infrastructure requirements and the challenge of decoherence—the rapid transition from a quantum state to a classical state[5]. Thus, while there is a technological race, especially between the US and the EU, classical computers will not become obsolete.

In April 2019, France officially recognized the significance of these advancements. Deputy Paula Forteza was tasked by the Prime Minister to explore the emergence of quantum

---

[1] Raphael.maurel@u-bourgogne.fr. The first version of this article was published in French in January 2024 under the title "Technologies quantiques et transformations du droit – Premières pistes de réflexion" in the Revue générale du droit. It is accessible in open access: https://www.revuegeneraledudroit.eu/blog/2024/01/29/technologies-quantiques-et-transformations-du-droit-premieres-pistes-de-reflexion/. This version is a literal translation. Thanks to Dan Ibala, PhD student in international law at the University of Bourgogne Europe, for his assistance in preparing this document.

[2] « La Chine lance un satellite 'quantique', une première mondiale », Ouest-France.fr, 16 août 2016.

[3] Franck ARUTE and al., « Quantum supremacy using a programmable superconducting processor », *Nature*, n°574 (2019), pp. 505-510.

[4] Marine BENOIT, « Course à l'ordinateur quantique : Google confirme enfin avoir atteint la "suprématie", IBM réfute », *Sciences et avenir*, 23 octobre 2019.

[5] For an accessible but precise explanation of these issues, see the general public lecture by Pascale SENELLART-MARDON, director of research at the CNRS, on "The beginnings of the quantum computer", organized by the Paris-Sud section of the Société Française de Physique on January 14, 2020 : https://www.youtube.com/watch?v=bVO5wdnicD4.

technologies and anticipate their political development[6]. Her report, "Quantum: The Technological Turn France Will Not Miss," published in November 2019, included 37 recommendations[7], such as creating 50 quantum startups in France by 2024 and making massive investments in quantum technologies. In early 2021, the French President unveiled a national strategy for quantum technologies, allocating nearly 2 billion euros over five years to support researchers and industries in quantum computing, communications, sensors, and cryptography[8]. In early 2022, ministers announced the launch of a national quantum computing platform as part of "France 2030"[9]. In October 2022, physicist Alain Aspect[10], who resolved a 50-year debate between Niels Bohr and Albert Einstein with his thesis in the 1980s, was awarded for his work on quantum entanglement. By 2023, quantum technologies were included in the 2024-2030 military programming law as a priority for military development[11].

We are thus entering the second quantum era. The first quantum revolution brought us the transistor in 1947 and the integrated circuit in 1959, both based on quantum mechanics and pivotal for the development of computers and smartphones. The second quantum revolution aims to harness the consequences of quantum entanglement and superposition. Currently, there is limited research in the humanities on the implications of these developing technologies[12]. While quantum computers may not stabilize for another three to five decades, China's 2016 breakthrough and potential unpredictable technological leaps necessitate preparation. Significant investments by the US, China, and the EU underscore the need for states to ready themselves for these technological advancements and their societal impacts.

France, home to promising startups like Pasqal, which can compete with American giants in quantum prototype development[13], has recognized the importance of this field and plans substantial investments in the coming years. However, quantum technologies remain enigmatic to the public, politicians, and humanities scholars. The anticipated emergence of an operational "quantum Internet" by 2035[14] calls for the mobilization of legal experts to anticipate the obsolescence of existing frameworks, the impact on fundamental rights, and the need for new norms.

These preliminary reflections aim to explore how legal thought can address these technological evolutions and determine if they necessitate new legal rules. The interplay between new

[6] Décret du 5 avril 2019 chargeant une députée d'une mission temporaire.
[7] Paula FORTEZA, Jean-Paul HERTEMAN, Iordanis KERENIDIS, « Quantique : le virage technologique que la France ne ratera pas », Rapport de la mission parlementaire du 15 avril 2019 au 3 octobre 2019, novembre 2019, 68 p.
[8] « Présentation de la stratégie nationale sur les technologies quantiques », 21 janvier 2021 : https://www.elysee.fr/emmanuel-macron/2021/01/21/presentation-de-la-strategie-nationale-sur-les-technologies-quantiques.
[9] Secrétariat général pour l'investissement, « Stratégie quantique : lancement d'une plateforme nationale de calcul quantique », 4 janvier 2022.
[10] « Alain Aspect, prix Nobel de physique 2022 », *Le journal CNRS*, 4 octobre 2022.
[11] Loi n°2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense.
[12] Among the few works available in the legal sciences, see for example Mauritz KOP,« Establishing a Legal Ethical Framework for Quantum Technology », *Yale Journal of Law & Technology (YJoLT)*, The Record, 2021, en ligne : https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology ; Valentin JEUTNER, « The Quantum Imperative:Addressing the Legal Dimension of Quantum Computers », *Morals & Machines*, n°2021(1), pp. 52-59.
[13]https://www.pasqal.com/.
[14] « La stratégie quantique française », Rapport n°377 (2021-2022) de MM. Gérard LONGUET, sénateur et Cédric VILLANI, député, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, déposé le 20 janvier 2022.

technologies and legal frameworks is not new; the advent and democratization of the Internet are prime examples[15]. Regarding quantum technologies, which are just beginning to be integrated into French legal thought, at least three analytical methods are possible. The first involves observing how these technologies are being incorporated into positive law. The second examines the legal approaches that scholars, the state, and the EU might adopt. The third questions the resilience of existing laws and the need for new legal tools.

I. BINARY INTEGRATION INTO THE NATIONAL LEGAL ORDER

Quantum technologies truly emerged in French law in 2023 in the military domain. However, the European Union has been interested in this topic since at least 2016, suggesting that France could have legislated earlier and even been a driver of European initiatives, which it was not. Moreover, the EU is promoting an approach more focused on creating quantum communication infrastructures for non-military use.

A. Quantum Technologies: A Predictable Focus of French Military Programming Law

Apart from a 2001 decree on the ionization of foodstuffs mentioning "maximum quantum energy produced by ionizing radiation devices"[16] and the recommendations of the Commission for the Enrichment of the French Language, which have integrated terms related to quantum physics into the official vocabulary of the nation[17] in recent years, there was no mention of quantum technologies in French law or regulations[18] before the 2020s. Beyond the reports of the Parliamentary Office for the Evaluation of Scientific and Technological Choices (OPECST)[19], the quantum issue indirectly appeared in the Law on Research Programming

[15] See, for example, the symposium devoted in 2013 to the subject of interactions between the Internet and international law: SFDI (coll.), *Internet et le droit international. Colloque de Rouen*, Paris, Pedone, 2014, 496 p.

[16] Décret n°2001-1097 du 16 novembre 2001 relatif au traitement par ionisation des denrées destinées à l'alimentation humaine ou animale, article 3.

[17] See the following notices from the Commission d'enrichissement de la langue française, adopted since 2015: Vocabulaire des termes généraux de la chimie (list of terms, expressions and definitions adopted), JORF of September 19, 2015; Vocabulaire de la chimie et des matériaux (list of terms, expressions and definitions adopted), JORF of July 1, 2017; Vocabulaire de la chimie et de la mécanique quantique (list of terms, expressions and definitions adopted), JORF of March 31, 2022; Vocabulaire de l'informatique quantique (list of terms, expressions and definitions), JORF of december 20, 2022.

[18] Only one parliamentary question, in 2006, following the publication of research results from the United States, raised the issue of advances in quantum research in France. See question n°104780 from Mme Nathalie Kosciusko-Morizet, JORF of October 26, 2006, p. 9988, asking about the state of research in France on the theory of spin separation (a characteristic that mathematically classifies the way objects transform under the effect of rotations in three-dimensional space; and the answer published in the JORF of February 6, 2007, p. 1345.

[19] Office parlementaire d'évaluation des choix scientifiques et technologiques. It seems that the first report clearly – albeit cautiously – outlining the challenges of quantum technologies, essentially in terms of advances in computing, dates back to 2008; see the Rapport sur l'évolution du secteur de la micro/nanoélectronique n° 997 déposé le 25 juin 2008 par M. Claude Saunier.

(LPPR)[20] and more clearly in the Law of August 1, 2023, on military programming for the years 2024 to 2030[21].

The extent of the military and industrial developments of quantum technologies is difficult to imagine at this stage. However, the work carried out by OPECST[22] and the available knowledge suggest that communications, particularly diplomatic and strategic ones, will likely be revolutionized and reach unprecedented levels of security in the coming years. At a time when contemporary conflicts demonstrate the operational necessity of advanced communications—consider the Russian army communicating on Ukrainian soil via public radio waves[23]—the race towards quantum communication is a crucial strategic issue. Beyond communications exploiting quantum entanglement, the emergence of quantum computers will weaken, if not render obsolete, the effects of classical cryptography, which protects military communications and data. The computing power of a quantum computer indeed challenges the effectiveness of so-called classical cryptography.

Asymmetric cryptography, developed to overcome the limitations of symmetric cryptography (a system in which the sender and receiver of a message must share a decryption key in advance, with the risk of interception during the sharing of the common key), still relies, schematically, on the difficulty of breaking a code. This system provides for the existence of a pair of keys to encrypt any message: a public key for encryption and a private key for decryption. The public key is freely distributed, while the private key remains secret, held by the recipient. This system, although slower—hence the interest in quantum communications—solves the key-sharing problem. However, RSA (Rivest, Shamir, Adleman[24]), one of the most widely used asymmetric cryptography algorithms, relies on the difficulty of factoring a large composite number into its prime factors. In other words, as long as this task remains complex and time-consuming, the message remains secure; this will no longer be the case with quantum computers. As Henri Gilbert (ANSSI) points out, "[i]t is difficult to predict whether such computers will ever exist and, if so, whether they will appear before or after 2035, but prudence dictates that we start protecting ourselves now against attacks from such computers, in order to prevent retroactive attacks of the type 'record now on current systems, cryptanalyze n years later'. For highly sensitive data that needs to be protected durably, we are already exposed to this threat. ANSSI

[20] See the relevant extract from the report appended to Law no. 2020-1674 of December 24, 2020 on research programming for the years 2021 to 2030 and on various provisions relating to research and higher education: "The computing power of conventional computers, which has grown exponentially since the 1960s, has now reached a plateau. The 'second quantum revolution' may lead in the years to come to a new type of computer, with unrivalled power. [...] If it comes to pass, this quantum technology will be at least as important a breakthrough as the classical computer, making it possible to solve complex optimization problems, with applications in the search for new materials, new drugs and so on. As this new computing power will make it possible to break the cryptographic codes that secure all our sensitive communications today, we need to start working now on the cryptography of the future that will withstand the quantum computer, and more broadly on the development of new quantum algorithms".

[21] Aforementioned law. It is notable that the previous military programming law, loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, only mentions quantum computing very incidentally, n'évoque l'informatique quantique qu'à titre très incident.

[22] « La stratégie quantique française », rapport aforementioned.

[23] The press picked up on this: « Guerre en Ukraine : ce que dévoilent les communications des soldats russes sur des fréquences radio non sécurisées », Le Monde.fr, 25 mars 2022.

[24] Ronald RIVEST, Adi SHAMIR, Leonard ADLEMAN, « A method for obtaining digital signatures and public key cryptosystems », *Communications of the ACM*, vol. 21, no 2, 1978, p. 120–126.

recommends, like most global security agencies, that we start addressing this quantum threat as soon as possible."[25]

It is therefore necessary to develop new methods to secure future communications. Two main approaches are currently being explored. Quantum cryptography aims primarily at the secure creation and distribution of cryptographic keys. Quantum particles—primarily photons—will be used to generate a shared secret key between two parties, such that any interception attempt will encounter the uncertainty principle of quantum mechanics (Heisenberg's uncertainty principle), which guarantees that such an attempt will be detected. Unlike quantum communication, which aims to secure the message itself, the main objective of quantum cryptography is to ensure the security of the key, which can then be used in a classical encryption algorithm to secure the transmission of multiple messages. Post-quantum cryptography, on the other hand, aims to design encryptions resistant to quantum attacks. Unlike quantum cryptography, it does not use quantum phenomena in its operation but relies on mathematical algorithms that remain difficult, if not impossible, to solve even with a quantum computer. The goal is to capitalize on the limitations of quantum technologies before their concrete emergence, which also allows for anticipatory experimentation[26].

These research efforts require massive investments for inevitable military uses, even if they are not perfectly clear at this stage. This is why the 2024-2030 military programming law fully integrates the subject. The report annexed to the law states that "[t]o maintain the operational superiority of our armed forces, a transformation must be undertaken to anticipate technological leaps and associated uses, particularly in the fields of space, the seabed, cybersecurity, drones, and various areas of fundamental and applied research derived from quantum physics or artificial intelligence," and that "quantum research in its various aspects and the field of high-performance computing must be the subject of particular investment and vigilance by the state to develop and protect sovereign sectors."[27] Quantum technologies occupy two of the ten "priority axes" of military innovation: sensors in the era of quantum technologies on the one hand, and quantum computing for sovereign capabilities such as intelligence or deterrence on the other. Finally, a government report on the possible uses of quantum technology in the French armed forces will be submitted to Parliament in 2025, ensuring that the topic will animate military strategic debates beyond the scientific community for several years.

The emergence of quantum technologies in the French legal order thus occurs through the military sector, which is not surprising. This is an approach based on military use coupled with a risk-based approach in terms of security. However, overall, it is late and limited.

B. A European Approach Focused on Civil and Commercial Uses

As early as 2016, a "Quantum Manifesto" proposed by a European team composed of Commissioner Aymard de Touzalin, the Dutch Minister of Economic Affairs, and four academics was put forward to develop a common EU strategy for the second quantum revolution[28]. Based on this, the European Union launched the Quantum Technologies Flagship

[25] « La stratégie quantique française », aforementioned.
[26] See, for example, the tests carried out in France: « Informatique quantique - La Banque de France expérimente la cryptographie post-quantique », Revue de Droit bancaire et financier, n° 6, Novembre-Décembre 2022, alerte 159.
[27] Aforementioned.
[28] See « Quantum Manifesto for Quantum Technologies », online: https://ec.europa.eu/futurium/en/content/quantum-manifesto-quantum-technologies.html.

in 2018, a research initiative with a budget of one billion euros. Additionally, within the framework of the European Joint Undertaking for High-Performance Computing (EC EuroHPC), efforts were initiated to achieve at least the deployment of quantum computers. On June 13, 2019, a declaration aimed at developing a quantum communication infrastructure covering the entire EU (EuroQCI) was signed by seven member states[29]. France only joined the initiative at the end of 2019. This initiative covers five areas: quantum communication, quantum computing, quantum simulation, quantum metrology and sensing, and the fundamental science of quantum technologies. This declaration, which forms the basis of European debates, does not envision military use—it does not consider it, as the Union lacks competence in this area. Indeed, the declaration states that the member states:

> "1. intend to work together to establish a cooperation framework—EuroQCI—to study, over the next 12 months, the possibility of developing and deploying within the Union, over the next 10 years, an end-to-end certified and secure quantum communication infrastructure (QCI), composed of space and terrestrial solutions, capable of transmitting and storing information and data in an ultra-secure manner and able to connect essential public communication means throughout the Union.
>
> [...]
>
> 3. agree that the target quantum-secure communication infrastructure should focus on the growing security needs of the public sector while exploring ways and conditions to make this infrastructure available to industry users, ensuring the best possible use of the infrastructure for public use and promoting an innovative and competitive European industry."[30]

Thus, the focus is on the industrial and civil exploitation of quantum communications—at a minimum—by 2030, which EU member states will need to anticipate at the national level. At the European level, these ambitious objectives are already reflected in several texts strengthening and developing existing infrastructures, whether in the European space industry[31] or the semiconductor industry[32]. The imminent emergence of certain quantum technologies is more broadly evident from reading the European texts adopted since 2019. It is noteworthy that the EU's common framework for screening foreign direct investments from 2019 includes, among the foreign direct investments likely to affect the security or public order of states, "critical technologies [...], including technologies related to artificial intelligence, robotics, semiconductors, cybersecurity, aerospace, defense, energy storage, quantum and nuclear technologies, as well as nanotechnologies and biotechnologies."[33]

[29] Commission, « The future is quantum: EU countries plan ultra-secure communication network », 13 juin 2019, en ligne : https://digital-strategy.ec.europa.eu/en/news/future- quantum-eu-countries-plan-ultra-secure-communication-network.

[30] Digital Assembly, Declaration of cooperation for exploring how to make available across the EU an integrated Quantum-secure Communication Infrastructure, Bucharest, 13-14 June 2019 (traduction personnelle).

[31] Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Programme for Secure Connectivity for the period 2023-2027.

[32] Regulation (EU) 2023/1781 of the European Parliament and of the Council of September 13, 2023 establishing a framework of measures to strengthen the European semiconductor ecosystem and amending Regulation (EU) 2021/694 ("Chip Regulation").

[33] Regulation (EU) 2019/452 of the European Parliament and of the Council of March 19, 2019 establishing a framework for screening foreign direct investment in the Union, Article 4.

In other words, the European Union has a certain lead in anticipating the social transformations related to quantum technologies. In truth, the EU's influence on European quantum development is particularly significant, as evidenced by Article 6 of Regulation 2023/588, which states that "[t]he Union is the owner of all tangible and intangible assets that are part of the governmental infrastructure developed under the program, [...] with the exception of the terrestrial EuroQCI infrastructure, which is the property of the Member States."[34] The EU's stated objective is to develop a European quantum policy and, at this stage, to be an economic and industrial driver in the ongoing technological race.

However, both the national and European approaches remain infrastructural rather than material. The idea that quantum technologies could affect the exercise of fundamental rights is thus never mentioned—except for Article 17 of the Charter of Fundamental Rights of the Union, which sets limits on the principle of the Union's ownership of all assets related to the future communication infrastructure[35]. In our view, it is on this basis that legal scholars must now consider the future framework for quantum technologies. Furthermore, the integration of quantum issues into France's military and research programming laws does not resolve the question of how these issues will be concretely addressed from a legal perspective—and the same is true at the European level.

II. THE NECESSARY CONSTRUCTION OF DOCTRINAL APPROACHES TO QUANTUM TECHNOLOGIES

It is well known that "digital law" raises formidable legal challenges, even in its definition. Theoretical approaches remain scattered, and the choice of terms is volatile. In the doctrinal galaxy of digital law, we speak of "law of digital activities" in general to refer to the regulation of activities based on digital technologies[36], and specifically of "Internet law" to refer to the rules, among those applicable to digital activities, intended to regulate the Internet[37]—whether its infrastructure[38] or the activities conducted thereon, or sectorally, of "cybersecurity law,"[39] "blockchain law,"[40] or—encompassing a broader field than just digital activities—of "personal data law."[41] Without delving into complex debates that exceed the scope of this preliminary reflection, it can be acknowledged that there are still conceptual discussions about the construction of a legal discipline[42] specific to the regulation of digital activities, and it is permissible to wonder if it should also include the subject of the legal regulation of the impact

[34] *Ibid*., article 6.
[35] *Ibid*., paragraph 22 of the preamble.
[36] Luc GRYNBAUM, Caroline LE GOFFIC, Ludovic PAILLER, *Droit des activités numériques*, 2ème éd., Paris, Dalloz, 1144 p.
[37] For e-commerce and e-sales only: Jean-Michel BRUGUIERE, Pierre DEPREZ, Frédéric DUMONT, Vincent FAUCHOUX, *Le droit de l'Internet*, 3ème éd., Paris, LexisNexis, 2017, 432 p. For a broader approach, see Céline CASTETS-RENARD, *Droit de l'internet : droit français et européen*, 2ème éd., Paris, Montchrestien, 2012, 492 p.
[38] Infrastructural approaches are rare ; see Raphaël MAUREL, *Droit de l'Internet*, Paris, Bréal, coll. Lexifac, 2024.
[39] See, since 2023, the Code de la cybersécurité published by Dalloz under the direction of Michel SÉJEAN.
[40] Alice BARBET-MASSIN, Faustine FLEURET, Alexandre LOURIMI, William O'RORKE, Claire PION, *Droit des crypto-actifs et de la blockchain*, Paris, LexisNexis, 2020, 432 p.
[41] See Antoine RENUCCI, Jean-François RENUCCI, *Droit et protection des données à caractère personnel*, Paris, LGDJ, Manuels, 2022, 258 p. ; Thibault DOUVILLE, *Droit des données à caractère personnel*, Paris, LGDJ, Précis Domat, 2023, 684 p.
[42] On this point, see the enlightening work compiled by Frédéric AUDREN, Ségolène BARBOU DES PLACES (dir.), Qu'est-ce qu'une discipline juridique ? Fondations et recompositions des disciplines dans les facultés de droit, Paris, LGDJ, coll. Contextes, 2018, 390 p.

of these technologies on society—the appropriate term perhaps being, as abroad, "digitalization law."

In any case, the regulation of quantum technologies and activities will inevitably join this vast semantic ensemble, and it will be necessary to adopt, on the one hand, an appropriate expression—"quantum law," "law of quantum activities"?—and, above all, on the other hand, an adequate legal approach. The diversity of disciplinary or sub-disciplinary titles mentioned above reflects a relative collective indeterminacy in the optimal scientific approach to understanding the legal phenomena arising from the use or existence of digital technologies—collective indeterminacy, not individual, as each author proposes a personal and justified approach to their subject of study. There is no reason why this theoretical ambiguity, likely favored by the post-regulatory nature of digital law[43], should dissipate when norms emerge to regulate quantum technologies. Thus, we can attempt to identify some possible approaches to these new rules or normative sets, which will necessarily borrow from other subsets while theoretically fitting within "digital law." Two approaches seem, at first glance, interesting among others[44]: infrastructural approaches (A) and risk-based approaches (B).

A. The Interest of an Infrastructural Approach

A first possible approach, based on the European approach but still too often lacking—in our view—in digital law doctrine, is to develop an infrastructural approach. Contemporary digital law manuals and doctrine have indeed strived to construct and present in an orderly manner a material approach to the rules applicable to digital technologies, sometimes leaving aside the issue of regulating the infrastructures enabling access to these tools (cables, satellites, data centers, etc.). These subjects, admittedly technical, sometimes fall more under technical standardization than anything else; however, the geopolitical stakes of these infrastructures are such[45] that legal scholars cannot disregard them—all the more so when international texts protect them[46].

However, quantum technologies are not independent of materials, structures, and infrastructures that are already, for some of them, subject to existing national legislations and international frameworks. Thus, Internet law immediately refers, under this approach, to the international regime of submarine cables[47] and, to a lesser extent, to satellite telecommunications law. In the field of quantum technologies, quantum satellites might be preferred over fiber optic cables—as evidenced by the Chinese experience of 2016 and the orientations of the European regulation on secure connectivity for the period 2023-2027[48]. The infrastructure of quantum networks remains to be built according to specific standards: these systems should prove extremely sensitive to interference and will need to be particularly protected. In another vein, while classical digital technologies mainly use semiconductor

[43] Technology is always evolving faster than the laws that govern it.
[44] Other works consider or adopt sectoral approaches, for example from the angle of intellectual property; see for example Mauritz KOP, « Regulating Transformative Technology in The Quantum Age: Intellectual Property, Standardization & Sustainable Innovation », Transatlantic Antitrust and IPR Developments, Issue 2/2020, 2020.
[45] For an example of a recent work on this theme, see Ophélie COELHO, *Géopolitique du numérique. L'impérialisme à pas de géants*, Éditions de l'Atelier, 2023, 272 p.
[46] This is particularly true of submarine cables, whose protection dates back almost to their creation with the Paris Convention of 1884 on the Protection of Submarine Cables; see also Articles 21 and 60 of the United Nations Convention on the Law of the Sea of December 10, 1982, and, more broadly, this legal regime, Camille MOREL, *Les câbles sous-marins*, CNRS Éditions, 2023, 192 p.
[47] *Idem*.
[48] Regulation (UE) 2023/588.

materials—subject to a "commercial war" between China and the United States[49]—quantum technologies should also rely on superconductors, whose market is currently dominated by the United States, Japan, and, to a lesser extent, Germany. An infrastructural approach to quantum law could thus begin with an analysis of the physical frameworks for the use of quantum technologies and a study of the applicable law to the likely commercial and technological wars that states will wage on these subjects, from the perspective of international economic law as well as fundamental and environmental rights. Overall, observers agree that the next quantum revolution will significantly reduce the environmental impact of our technologies. These currently "require specific hardware equipment, built using rare minerals (cobalt, lithium, neodymium, indium, ...) sometimes from conflict zones (referred to as 'blood minerals') and whose operation involves considerable energy consumption, even if this will decrease with advances in quantum technology."[50] Regarding semiconductors, the extraction of silicon (mainly in China), germanium, or gallium indeed raises issues of environmental protection and worker status. On this point, one of the missions of the European Semiconductor Board created by the Chips Regulation, which provides for a reduction in the environmental impact of these industries, will be to study and prepare "the identification of specific sectors and technologies likely to have a strong social or environmental impact or of importance in terms of security, and which must therefore be subject to certification attesting that their products are green, reliable, and safe."[51] Superconductors, also necessary for certain quantum technologies, involve the use of compounds based on niobium, titanium, or iron. The current and future extraction of some of these minerals, such as niobium in Africa, already raises geopolitical, ethical, and environmental issues that will be difficult to ignore[52] and could lead to the creation of national, regional, and global regulatory authorities for the mining sector.

An infrastructural approach would notably allow for the full integration of these primarily geopolitical and environmental issues into the debates on the regulation of the uses of quantum technologies, whereas they are generally underrepresented in those related to digital law.

B. The Essential Risk-Based Approach

A second possible approach is the risk-based legal approach. In a recent work, Arnaud Latil shows how digital law has been constructed as a risk law, and although quantum technology law is not yet part of his analytical scope, his conclusion resonates with the preceding remarks: "Risk law is a trajectory law. With it, the regulatory state shows the justifiable the paths to follow to prevent risks and overcome their negative consequences. [...] Risk law is also a pragmatic law. It indeed marks a methodological turning point for the production and application of law. The critical assessment of risk prevention objectives and resilience in the face of damage implies measuring the effectiveness of norms and moving away from an abstract logic of legal rule assessment. A pragmatic approach is essential. All normative phenomena

[49] See for example Zhou QI, « US Technological Decoupling from China: Strategic Motives and Policy Measures », *China International Studies*, vol. 98, 2023, pp. 101-126. It is worth noting that Joe Biden's presidential decree of August 2023 severely restricts US investment in China in the field of quantum technology ("États-Unis : adoption d'un décret présidentiel interdisant certains investissements américains dans des technologies sensibles en Chine", *Revue Internationale de la Compliance et de l'Éthique des Affaires*, n°5, 18 octobre 2023, actualité 214, p. 5).

[50] William FEUGÈRE, « Compliance et métavers – une éthique réelle dans un monde virtuel », *Revue pratique de la prospective et de l'innovation*, n° 2, Novembre 2022, dossier 16, p. 30.

[51] Regulation (UE) 2023/1781, article 28, 1. d).

[52] The African press, for example, Nicaise KIBEL'BEL OKA, "RDC. Niobium, minerai stratégique au cœur d'une géopolitique de l'insécurité au Nord-Kivu", *Echos d'Afrique*, December 11, 2022; "Malawi : la construction de la première mine de niobium d'Afrique commenceera d'ici septembre 2024", *Agence Cofin.com*, June 14, 2023.

must be measurable to determine the degree of risk resistance. The convergence of law and other sciences is then necessary to assess its effectiveness."[53]

In the field of quantum technologies, everything remains to be built, and we can only outline what such an approach might entail. A risk-based approach to quantum technologies, beginning with a taxonomy of quantum uses aimed at mapping the risks induced by quantum technologies, would first integrate an infrastructural logic but would go beyond it by addressing democratic and social risks. This is, moreover, the approach adopted by the first English-speaking reflections on the regulation of quantum technologies. Mauritz Kop thus identifies half a dozen key sectors—but no concrete use cases—(quantum computers, quantum communication, quantum sensors, quantum simulation, fundamental science, artificial intelligence) and considers ten pressing categories of social risks: the risk of increasing inequalities and monopolization of technologies by intellectual property initially, the risk to the stability of the economic and financial system, the risk to data confidentiality and security, the risk of massive disinformation, the risk of hacking, the risk of criminal activities, environmental risk, risks associated with authoritarianism and state surveillance, the risk of geopolitical recomposition and the quantum arms race, and, with alarming pessimism, risks related to scenarios of human extinction[54]. And the author concludes: "A lack of policy, inaction, and absence of international consensus will amplify these risks." Drawing on other normative sets and other sciences besides law, such as philosophy, ethics, management sciences, or life sciences, such an approach to quantum risks would have the advantage of immediately encouraging systemic reflections, going beyond the technical and sectoral approaches (military domain, cybersecurity, telecommunications, etc.) of these tools.

These two approaches, infrastructural and risk-based, are neither mutually exclusive nor the only possible ones. They could, however, constitute an initial basis for reflection to think about the future "quantum law." Beyond doctrinal approaches, it is nevertheless necessary to concretely analyze how quantum technologies—or some of them—raise or will raise legal questions.

III. THE ESSENTIAL REFLECTION ON APPLICABLE LAW TO QUANTUM PHENOMENA

The question of the doctrinal frameworks that need to be developed does not address the urgencies highlighted by experts on the subject[55]. However, when faced with new social phenomena, legal scholars generally identify two distinct but complementary approaches. The first approach often involves extending existing law through various legal techniques, such as dynamic interpretation, to encompass new situations. Another approach is to identify the gaps in existing law and supplement it with new instruments specifically dedicated to regulating the new element.

A. Considering the Relevance of Existing Frameworks

[53] Arnaud LATIL, *Le droit du numérique. Une approche par les risques*, Paris, Dalloz, 2023, p. 241.
[54] Mauritz KOP, « Establishing a Legal-Ethical Framework for Quantum Technology », *op. cit.*
[55] See for an attempt at synthesis Mauritz KOP, Mateo ABOY, Eline DE JONG, Urs GASSER, Timo MINSSEN, I. Glenn COHEN, Mark BRONGERSMA, Teresa QUINTEL, Luciano FLORIDI, Ray LAFLAMME, « Towards Responsible Quantum Technology », *Harvard Berkman Klein Center for Internet & Society Research Publication Series*, #2023-1, Harvard University 2023, 22 p.

One of the first questions to raise is the capacity of our current legal models to integrate the issues and risks induced by the development of quantum technologies. The international community, confronted with new technologies, has produced numerous rules—both soft and hard law—to regulate them in recent years and continues to do so. Thus, it initially seems pertinent to reason by analogy with the regulation of artificial intelligence (AI), which is currently in full development. As Mauritz Kop indicates, "A legal framework for quantum technology should build on existing rules and requirements for AI. We should connect AI to quantum,"[56] especially since quantum computers and other quantum tools will largely be hybridized with AI systems. This is why the ten basic principles that the author proposes for the development of safe and democracy-protecting quantum technologies are mainly inspired by work in the field of AI[57].

However, it is uncertain whether the approaches to AI regulation, which are regionally fragmented and late, can be as simply duplicated. The legal issues raised by quantum technologies are as numerous as the uncertainty of their operational date. Nevertheless, it is pertinent to first seek to apply existing legal frameworks. In this sense, Valentin Jeutner, focusing his analysis on quantum computers, chronologically distinguishes two major legal issues. The first, as much political as legal, is that of standardization in its development—drawing a parallel here with the standardization, including linguistic, that presided over the development of classical computers[58]. Technical and standardization norms, at the national (military) and international levels, will undoubtedly be necessary, as with any new technology. Indeed, it will be necessary to ensure the interoperability of quantum systems; otherwise, they will not be able to communicate with each other. However, the technical standardization process is intrinsically political: China, the United States, and the European Union will undoubtedly engage in underground diplomatic battles to impose their conception on global standardizers. The National Institute of Standards and Technology (NIST), a U.S. standardization institute, has already marked the field with its influence and begun to define future global quantum standards[59]. It is also likely that the ISO (International Organization for Standardization) will play a major role in standardizing quantum infrastructures, similar to its indispensable position in classical computer infrastructures. However, it is not inconceivable that, following the model of the Internet Engineering Task Force (IETF) created to develop standards dedicated to the functioning of the Internet, new standardization consortia will emerge to address issues specifically related to the interoperability of quantum technologies. States will then have to position themselves to determine the functioning of such organizations: will they be public, private, or mixed? What model, democratic or not, will be chosen for their operation and the formation of standards? These questions, related to the technical regulation of quantum tools, must be anticipated now.

The second legal issue posed by quantum computers, according to Valentin Jeutner, is the most pressing: the ability of these computers to overcome conventional encryption protocols. Although post-quantum cryptography aims to limit the difficulties, it remains that future quantum algorithms could be used to decrypt information a posteriori. In other words, it is possible to collect classically encrypted data today and decrypt it later when sufficiently

[56] Mauritz KOP, « Establishing a Legal-Ethical Framework for Quantum Technology », *op. cit.*
[57] Compare the ten principles, in the form of a declaration of intent that companies and states are invited to adopt, with the Declaration on Artificial Intelligence, Robotics and "Autonomous" Systems proposed by the European Group on Ethics in Science and New Technologies (European Commission), Brussels, March 9, 2018.
[58] Valentin JEUTNER, « The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers », *op. cit*., p. 55.
[59] « La stratégie quantique française », report.

powerful quantum computers are available[60]. Again, the solutions are as much political as legal: "[I]t is crucial to develop strategies to avoid a situation where, on the one hand, there are actors who have unlimited access to previously protected data and can communicate in encrypted form and, on the other hand, actors who have no access to quantum technology and are more or less at the mercy of the former."[61] The author recommends ensuring, through law, equal access to quantum technologies, which could be translated in an anticipatory manner—because it will be too late afterward—by a "right to quantum." Legally, "examples of such regulatory measures could include limiting the material or temporal scope of patents or making technology transfers obligatory in certain areas."[62]

As we can see, and as the author concedes in conclusion, several of the major principles or even necessary norms, according to him, for anticipating quantum technologies already exist in our legal systems: principles of equality, non-discrimination, transparency, and good governance in particular[63]. It is interesting to note that, from the outset, the link between technical standardization and fundamental rights is assumed. Such an approach seems particularly relevant to us, as the "detechnicization" of technological issues, the only way to allow citizens to grasp them, is a democratic imperative. Furthermore, we have emphasized above the importance of considering the risks of quantum technologies in terms of human rights and not limiting them to purely military and economic issues. However, the specific application of these major principles to the field of quantum technologies—here, only quantum computers—might require the adoption of new rules at the international, regional, or national levels.

B. Anticipating the Need for New Instruments

As Brunessen Bertrand rightly points out, "[L]aw is not always able to anticipate all technological developments—and all those that today's 'deep tech' suggests: high-performance computing, quantum technologies, blockchain represent a real challenge for the application of normative standards for the protection of rights. This is the whole issue of the technological neutrality of law and fundamental rights. This nevertheless requires constant reflection on the legal regulation of these technologies [...]. The risk, in this matter, is also that of the consecration of theoretical principles that are too abstract to be operational. Questions such as portability and interoperability show that technical standards are necessary for the effectiveness of law and rights in digital activities."[64] It is these standards that need to be anticipated, as much as possible, by identifying the relevant level of action.

At the European and state levels, questions will mainly arise regarding the respect for fundamental rights, the fight against cybercrime, and the protection of personal data. Improving encryption capabilities will necessarily impact surveillance techniques deployed by states and thus the right to privacy. If quantum technologies were to be commercialized and generalized in civil society, as computers, Internet access, and cell phones have been, many questions would need to be resolved. Will the European Union wish to harmonize regulations related to these new technologies to ensure a functional single market? This seems to be the path chosen by the

[60] Valentin JEUTNER, « The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers », *op. cit.,* p. 55.
[61] *Ibid*., p. 56.
[62] *Idem*.
[63] *Ibid*., p. 58.
[64] Brunessen BERTRAND, « Le modèle européen de partage de données », *Europe*, n° 2, Février 2021, étude 1, p. 2.

aforementioned regulations[65], although the issue of respect for fundamental rights, except for the desire to create equal access to these technologies and the general respect for the right to property, is still absent from European texts. A general declaration on the rights and freedoms guaranteed by the member states of the Union in the quantum era, drawing a roadmap parallel to that developed for secure connectivity in the Union, would certainly be a relevant initiative.

In international law, specific questions will undoubtedly emerge. The experience of transformations in international law due to the Internet—if only concerning debates on whether the law of war applies to cyberspace[66]—should serve as a lesson and help anticipate certain issues. The international regime of cybersecurity, which remains limited in density, will undoubtedly need to be refounded and deepened. Quantum entanglement also opens the way to future foreign activities on the soil of states, raising issues of territorial sovereignty, the fight against foreign interference, and cybercrime. The Council of Europe's Budapest Convention[67] on Cybercrime—open to accession beyond the organization—could usefully be supplemented by a third protocol on cybercrime in the quantum era. However, the issue of quantum technologies is not on the 2022-2023 work program of the Convention Committee[68], nor is it on the agenda of negotiations for the future international instrument on cybercrime. The 2019 report of the UN Secretary-General, which served as the basis for the creation by the General Assembly of the Ad Hoc Committee tasked with elaborating a comprehensive international convention on countering the use of information and communications technologies for criminal purposes[69], does not mention quantum risks at any point. Supposed to complete its work in 2024, the committee has produced a draft convention that, a priori, only imperfectly accounts for the upcoming quantum revolution—for example, the draft Article 22, paragraph 1, on establishing the territorial jurisdiction of states[70]. The issue of quantum has apparently not been addressed during the debates, despite a request from a multi-stakeholder NGO to the Ad Hoc Committee explicitly asking for it[71].

The international regime of telecommunications will certainly need to be adapted to integrate the issue of authorizations for sending data via quantum satellites and clarify how states can exercise control powers. For example, we think of the use of quantum communications for illicit purposes and the difficulty of applying Article 7 of the Telecommunications Regulation, under which states "should endeavor to take the necessary measures to prevent the spread of unsolicited bulk electronic communications and reduce their impact on international

[65] See in particular Regulation (EU) 2023/588 of the European Parliament and of the Council of March 15, 2023 establishing the Union Programme for Secure Connectivity for the period 2023-2027 (cited above)..

[66] There's little debate on the question any more: yes. The Tallinn Manual, published in 2013 by NATO, clearly sets out how international law applies to digital threats in armed conflict; a version 2.0, in 2017, explores the issue of cyber incidents not meeting the thresholds for the use of force or armed conflict, while a version 3.0 is expected for 2026. This text remains non-binding (it is not an international treaty) and marked, for its detractors, by a certain Atlanticism. France regularly reaffirms that international law applies to cyberspace..

[67] Budapest Convention on Cybercrime (ETS No. 185), November 23, 2011.

[68] COE, T-CY Workplan for the period January 2022 – December 2023, adopted by the 25th T-CY Plenary (15 November 2021).

[69] Resolution 74/247 adopted by the General Assembly on December 27, 2019, A/RES/247.

[70] Ad Hoc Committee for the Elaboration of a Comprehensive International Convention on Combating the Criminal Use of Information and Communication Technologies, Sixth Session, New York, August 21-September 1, 2023, Draft Convention Text, May 29, 2023, A/AC.291/22.

[71] Proposition by the Center for Cyber Risk Research and Policy at the Cyber Institute to the Ad Hoc Committee, August 2022. Referring to the fact that « [e]merging Technologies such as Artificial Intelligence, Quantum Computing, and Blockchain have become increasingly exponential enabling innovations for potential criminal actors exploiting Information and Communication Technologies », the Centre concludes its letter as follows: « we implore this Ad Hoc Committee explore and deliberately include aspects of emerging technologies into our discussions ».

telecommunications services as much as possible."[72] More broadly, new security standards will quickly become necessary within the ITU. Securing new networks—5G, the Internet of Things, 6G tomorrow—and their resilience to future quantum attacks also involves international standardization within the ITU. As a private company executive specializing in quantum technologies indicated in 2019, "[S]tandardization is relatively new to the quantum technology community, both in industry and academia. We did not fully anticipate the need for standards to support large-scale deployment of technologies [...]. Having now recognized this need, we have quickly built an ecosystem of quantum specialists within ITU, and we are learning ITU's procedures as we work together to draft a first set of ITU standards on quantum-safe security."[73]

Above all, the potential emergence of weapons based on quantum technologies should now be the subject of global discussions. In the absence of a treaty prohibiting the development of certain quantum weapons, which will certainly need to be considered in the future, a global declaration on the peaceful use of quantum technologies, at a time when the quantum arms race is limited to cybersecurity[74], would particularly be a relevant first step. Certainly, the usefulness of yet another global declaration can be debated, especially since it may seem somewhat premature. However, it is important to remember that the 1967 Outer Space Treaty, which set the requirement for the peaceful use of outer space, was adopted even before humans had set foot on the Moon. It is undoubtedly a visionary tool of this kind, setting an incredibly futuristic framework that has certainly prevented many conflicts[75], that the international community needs to avoid being caught off guard once again by technologies whose advances can still be observed today.

Technological advancements based on quantum physics, although seemingly complex, deserve our attention from now on. Some proposals, centered around principles affirming the necessity that the development and use of quantum technologies respect human rights, are indeed gradually emerging in academic literature[76]. However, the very existence of this second quantum revolution, whose effects will not be measurable for years, remains poorly understood by the public and the legal community, who must nevertheless address it as quickly as possible.

[72] ITU, International Telecommunication Regulations (ITR), Final Acts of the World Conference on International Telecommunications (WCIT-12), Dubai, 2012, Article 7.1.
[73] « Quantum specialists are racing to join the ITU membership: ID Quantique explains why », *ITU News*, May 21, 2019, en ligne : https://news.itu.int/why-quantum-specialists-join-itu/.
[74] Neil THACKER, « Cybersécurité : la course aux armements quantiques a commencé », *Silicon.fr*, 31 janvier 2023.
[75] On this point, we refer to Raphaël MAUREL, "Les garanties du maintien de l'utilisation pacifique de l'espace extra-atmosphérique : l'exemple de l'inspection internationale spatiale", in SFDI (collectif ; dir. Clémentine BORIES, Lucien RAPP), *L'espace extra-atmosphérique et le droit international. Colloque de Toulouse*, Paris, Pedone, 2021, pp. 359-376.
[76] See the above-mentioned example of Mauritz KOP, « Establishing a Legal-Ethical Framework for Quantum Technology ».