POSITION PAPER – Quantum & Law

Prof. Vanessa Mak, Dr. Julia Cramer, Prof. Bart Custers, Melissa Hernandez Vindas, LL.M.

Leiden Law School, Leiden Institute of Physics (LION)

Unlocking Quantum – What's Law Got To Do With It?

Quantum technology is no longer the theoretical playing field of physicists and mathematicians. Applications are being developed for instance in health care, where quantum sensing can be used for ultraprecise imaging, and in finance to safeguard encryption used by banks. For general application, quantum computers are being built that promise unprecedented computational power that can become a powerful engine for other technologies, in particular Artificial Intelligence (AI). Law and policy can provide frameworks for unlocking the benefits of quantum technology as well as managing risks that may arise. But what are those risks and can the law contain them?

Towards Quantum Readiness

Theories of quantum science have been developed by theoretical physicists and mathematicians for decades. Their work focuses on the smallest particles in the natural world and their ability, in theory, to be in several states at once. Only for an observer they crystallize into one state. For a non-scientist, the example of Schrödinger's cat – which can be both dead or alive inside a box until the observer opens the box – is perhaps the best-known metaphor for this phenomenon. Another special feature of quantum particles is that a connection between particles can exist – called 'entanglement' – by which each particle 'knows' the state of the other, regardless of distance. Einstein referred to this as "spooky action at a distance".

Translating quantum science into quantum technology has practically focused on the development of quantum sensing, quantum computing, and quantum communication applications. Quantum particles' special features enable ultraprecise sensitivity in quantum sensors, for instance, used for image improvement in MRI scans in hospitals. Furthermore, quantum computers promise unprecedented computing power, enabling exponentially faster computation than is currently possible on standard computers. The greatest obstacle to a wide span use of quantum computers are practical impediments to fault-free functioning (e.g., the need for extremely cold environments in order to minimize 'noise' between particles), but those are expected to be overcome by scientists in the coming years. After that, quantum computers can become powerful engines in particular by providing computational power to other technologies, such as AI. Finally, quantum particles' entanglement enables communication without the transfer of particles and with unprecedented security. While this may sound like science-fiction, actual applications are being developed in particular in the form of encryption and decryption tools.

In 2025, the European Union published a Quantum Europe Strategy, positioning Europe as a global leader in quantum research and technologies by 2030. This strategy is expected to be followed by an EU Quantum Act in the second semester of 2026, which is likely to become the principal legal instrument for quantum technology in Europe. The EU is not alone in its investment in the development of quantum technologies. China and the US are equally set on taking up a leading position in this area. With quantum applications in finance being at the forefront of technological development, banks have set their sights on 2030 as the year to be 'quantum ready' (BIS Papers no 158, Quantum-readiness for the financial system: a roadmap). With these investments it is likely that quantum technology will become a reality and move beyond the 'hype' status that it has had in the past years. Initial applications are already being rolled out on the market. Quantum technologies have advanced to the point where researchers can begin testing proof-of-concepts and realistic applications. In recent years, software tools, programming languages, and development frameworks for quantum computing have grown rapidly (see SURF Tech Trends 2026).

Regulating Quantum Technology

Quantum applications are likely to benefit society in many ways, as the examples above highlight. However, use of the technology also generates risks. By way of example, the strategy for introducing quantum computers in the Netherlands is a proactive one, meaning that a beta version will be released onto the market when ready, so that users can experiment with it. The objective of running a beta version is to explore benefits, but also to detect risks early on. Contrary to what happened with AI, where generative AI such as ChatGPT appeared on the market very suddenly, with quantum there is still time to prepare. A beta version will allow users to be involved in that process. Small and medium-sized enterprises, for instance, can benefit from this as they do not have the resources to build their own quantum computing applications. However, despite the benefits of this approach, they run certain risks. Regulation can in some ways already provide a safety net, of which we highlight two aspects.

First, a beta version is likely to contain errors and can cause harm to users. From a regulators' perspective, this means that the developer who brings a beta version of a quantum computer onto the market will have to be transparent about risks. Moreover, if developers want to escape liability for harm caused by the technology, some safeguards should be applied. One may think of contractual exclusion clauses, damages clauses, or preventative measures. Within existing frameworks of contract and tort law, such instruments each have a place and legal advisors should be able to indicate what solution works for what type of case. Variation of outcomes is likely depending on the application, its users and the harm that may occur. For instance, legal protection for consumers is often stronger than for business users. Furthermore, exclusion of liability for death or personal injury is often impossible or significantly limited in comparison to liability for material damage to goods. Besides contract and tort law, legal safeguards can also be explored in other areas, such as data protection law or – where quantum provides an engine – AI regulation.

Second, quantum technology applications as they develop have to overcome large error margins. The hardware issues described above – e.g., the need to minimize 'noise' – are stubborn and as long as they remain quantum applications will suffer from faulty performance. This means that users will have to reckon with uncertain performance targets. From a regulatory perspective here also contract and tort law can provide frameworks for expectation and risk management between developers and users.

The specific tools for regulation are very much dependent on the type of quantum application and the context in which they develop. Quantum computers will not replace personal computers but are envisaged to operate in specific areas, for instance, as engines for AI or as encryption tools in finance. In some fields safeguards will be more urgently needed than in others. Furthermore, quantum computing is but one of the potential applications besides sensing and communication, and further variations within those categories.

Innovating Quantum Science & Law: A Roadmap

How to get a grip on risk management for quantum? We believe that different speeds can apply to different areas of application, depending on the level of risk. Like city cycling, some infrastructures (e.g., in the Netherlands or Denmark) are safer than others (e.g., London, Berlin or New York). This is often reflected in the obligation for cyclists to wear a helmet, which in the Netherlands until now has not been adopted. Notably, we observe changes there too as electric bicycles have introduced new risks even in more safely organized road infrastructures. Even Dutch cyclists may be obliged to wear helmets at some point, even if they will not like it.

For quantum technology, we are still exploring whether and which regulation can provide safeguards that allow for innovation at different speeds, whilst protecting users. The EU's AI Act seems a useful starting point for inspiration. Instruments that regulators can employ are distinctions between high-risk and low-risk applications, the development of technical standards, and the use of regulatory sandboxes for experimenting with technological applications and the effects of varying types of regulation. Still, quantum technology differs from AI and it is likely to require different risk management approaches, even if the tool kit from the AI Act is useful.

The framework of market regulation that underlies the AI Act, however, also has important limitations. In particular, it focuses on market access and market regulation. It is less powerful when applications are simply put into use without going through the regulatory steps for market access, such as for warfare or dual use applications. Also, there is little stopping developers from putting applications out onto the market, as we have seen with generative AI. In these cases, liability claims, injunctions or prohibitions can be *ex post* responses to rein in the use of the technology. For warfare or geopolitical power struggles, the law may be powerless.

Other power dynamics also require attention. Quantum technology is expensive to develop and big firms are in the lead. In this type of market, a small group of tech firms can become very powerful, in particular as patent laws protect them from sharing the technology. Incumbents are likely to adopt strategies preventing newcomers to enter the market. In order to maintain space for innovation, competition law should set boundaries to the power of big tech firms.

In sum, the emergence of quantum technology requires regulators to reconsider some fundamental issues of market regulation, innovation, fundamental rights protection, and liability. Power dynamics in some respects can also be managed through law. Legal analysis can identify where regulation is already in place and where new rules may be needed. The law can therefore support a safe environment for innovation and further development of quantum applications.

Innovation can also be triggered within law & technology scholarship itself. Risk management is inherent to many fields of law – private law, public regulation – but acquires new meaning when the science itself operates under conditions of uncertainty, as quantum technology does in the examples described above. Scholarship has started to develop new risk management models for AI, for instance, with a view to protecting fundamental rights (see Rotolo et al. 2025), which could be a basis for analysis of quantum technology too. The development of technical and legal standards for quantum is already happening (see e.g. NIST post-quantum cryptographic algorithms (FIPS 203, 204, 205)) and can provide fertile ground for developing approaches to private regulation and, more generally, lawmaking in a pluralist legal order (for a legal pluralist theory of lawmaking in European contract law, see Mak 2020).

Finally, quantum regulation does not need a 'Law of the Horse', the famous idea dismissed by Lawrence Lessig that every new technology requires a new law (Lessig 1999). What the law can do is offer a theoretical framework that envelops normative values and provides guidance on how to weigh or balance them in new situations. The EU, as one player in the geopolitical dimension of quantum development, has its own values enshrined in Art. 2 of the Treaty on European Union. They include "respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities". Let these be the guiding values in Europe, perhaps inspiring other parts of the world, for a safe way of unlocking the potential of quantum technology for society.