Philosophy & Technology (2023) 36:48
https://doi.org/10.1007/s13347-023-00651-6

RESEARCH ARTICLE

Ethics of Quantum Computing: an Outline

Luca M. Possati[1]

Received: 4 August 2022 / Accepted: 20 June 2023 / Published online: 10 July 2023

Abstract
This paper intends to contribute to the emerging literature on the ethical problems posed by quantum computing and quantum technologies in general. The key ethical questions are as follows: Does quantum computing pose new ethical problems, or are those raised by quantum computing just a different version of the same ethical problems raised by other technologies, such as nanotechnologies, nuclear plants, or cloud computing? In other words, what is new in quantum computing from an ethical point of view? The paper aims to answer these two questions by (a) developing an analysis of the existing literature on the ethical and social aspects of quantum computing and (b) identifying and analyzing the main ethical problems posed by quantum computing. The conclusion is that quantum computing poses completely new ethical issues that require new conceptual tools and methods.

Keywords Quantum technologies · Computing · Ethics · Cryptography

1 Introduction

1.1 Context and Motivation

This paper intends to contribute to the emerging literature on the ethical impact of quantum technologies (QT). This objective is of fundamental importance because if we can manage to identify possible problems and solutions at an early stage of the development of a technology, we can employ good forms of ethics and governance to direct the technology's development, that is, policies, procedures, and standards for the correct use and management of the technology. Ethics provides not only a strategy of opportunity, allowing us to exploit the social value of technologies, but also a solution for risk management, as it allows us to anticipate and avoid costly mistakes. Compared to other forms of technology ethics, such as AI ethics, the ethics of QT is more complex and delicate. On the one hand, QTs are still a young

✉ Luca M. Possati
lupossati@gmail.com

[1] Delft University of Technology, Delft, The Netherlands

technology whose development is largely uncertain and often influenced by a rhetoric of the "futuristic revolution" very similar to that used for nanotechnologies and AI (Coenen & Grunwald, 2017), albeit with less hype. On the other hand, when we discuss QT, we use an umbrella term referring to a range of technologies that are very different from each other and that can have different social and ethical impacts in different contexts.

For the latter reason, in this paper, I intend to focus on only one sector of QT: quantum computing (QC). QC designates the use of quantum mechanical phenomena, such as interference, superposition, and entanglement, to perform computations roughly analogous to—although operating quite differently from—those performed on a classical computer.

The paper is structured as follows: Sect. 2 contains an analysis of the current literature on the societal and ethical impacts of QC and QT in general. Section 3 identifies and analyzes some ethical issues about data management and the opacity of processes in QC. Section 4 focuses more on algorithm design in QC. Section 5 examines quantum cryptography and its possible ethical consequences in terms of privacy.

1.2 Technical Gaps

QC can be considered part of the broader field of quantum information science, a field which includes the following two intertwined subfields: (a) quantum communication (quantum networking and quantum cryptography) and (b) quantum sensing and metrology (quantum clocks, quantum antenna, quantum radar, quantum sensors, quantum imaging). Currently, the main applications of QC (see Jaeger, 2018; Nielsen & Chuang, 2011) are:

- *Quantum simulations*, that is, the simulation of quantum systems, by facilitating the discovery of new materials and new drugs, will have a huge impact on the chemical and pharmaceutical industries.
- *Quantum cryptoanalysis*: one of the most well-known QC applications, is the factorization of large prime numbers by exponential speedup, as described by Shor's algorithm. This can be a threat for public-key cryptography schemes, such as RSA, DH, and ECC, which are based on large prime number multiplications, the discrete logarithm problem, or the elliptic-curve discrete logarithm problem-based schema, all of which are considered to be computationally very hard or even intractable for classical computers. At the same time, quantum cryptographic techniques can ensure maximum levels of confidentiality and security in communications.
- *Quantum searching*, that is, the development of new faster and more efficient techniques for Big Data analysis (however, it should be noted that this type of work would require a large amount of memory and therefore a quantum memory capable of containing and protecting large amounts of data for a long time, which can be technically problematic).
- *Quantum optimization*, that is, the possibility of solving very complex problems and, in general, of enhancing our computational capabilities in different sectors, such as logistics or finance.

- *Quantum linear algebra*, that is, the ability to solve linear equations faster, which has with important implications for engineering, construction, and weather forecasting.
- *Quantum machine learning*, that is, QC will likely strengthen artificial intelligence systems, although it is unlikely that there will be full quantum AI due to several technical problems, such as the difficulties of translating classical data into quantum data, the lack of effective quantum memory systems, and the ineffectiveness of QC application for many problems.

In addition to being an emerging field, QC is also an undeveloped technology. We do not yet know all of its possible applications. For this reason, it is very difficult to make predictions and fully understand the potential consequences of this technology. This is not just a technical gap; given the co-evolution of technology and society, we cannot understand the impact of a specific technology before it has entered society (Geels, 2005, Rip, 2018). Nevertheless, scholars agree that we should consider QC as disruptive technology (Krelina, 2021; Inglesant et al., 2018; Hayashi et al., 2015). This makes ethical analysis complex, but necessary.

1.3 Regulation Gaps

New and emerging technologies are a challenge to governance. The need for strong regulations and policies on QTs is globally recognized, as demonstrated by the various regulatory frameworks developed so far (Hoofnagle & Garfinkel, 2022). However, current regulatory initiatives do not consider specific ethical problems. In the UK quantum strategy and the EU midterm report, the terms "ethics," "ethics," and "morals" never appear.[1] These terms are also absent from the US National Strategic Overview for Quantum Information Science.[2] There remain important gaps and open questions that are not even mentioned, for example: How to manage the quantum divide, that is, the imbalance between populations with advanced quantum technology (and therefore secure communications) and those without? How does privacy change in a quantum ecosystem? What ethical questions can quantum simulation bring? What impact can quantum networks have on finance and market regulations?

For example, QC could raise entirely new problems in international relations (see the relevant considerations about geostrategic implications of quantum Internet in Rodhe, 2021). In the US National Security Memorandum published in March 2022, it is stated that, in order to cope with the risk posed by quantum cryptography, the US "must promote professional and academic collaborations with overseas allies and

[1] https://www.gov.uk/government/consultations/uk-quantum-strategy-call-for-evidence; https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship#:~:text=The%20Quantum%20Technologies%20Flagship%20is,1%20billion%20from%20the%20EU.

[2] https://www.quantum.gov/strategy/

partners."[3] This international engagement "is essential for identifying and following global quantum information science trends and for harmonizing quantum security and protection programs."[4] However, it is likely that the development of quantum cryptographic systems will lead to the creation of impenetrable communication systems. This could have dangerous effects in alliances like NATO because it could cause (a) a power imbalance between countries with advanced quantum systems and countries without; (b) an increase in mistrust between diplomacies and opacity in institutional relations; and (c) a significant weakening of the influence of the US on its European allies. The Memorandum does not touch on any ethical features of quantum cryptography.

1.4 How This Helps to Fill the Technical and Regulatory Gaps

This paper intends to bridge these gaps from a specific perspective: that of QC and its main applications. The key issues tackled here are as follows: Are the ethical problems raised by QC just a different version of the same issues raised by other technologies, such as nanotechnologies, nuclear plants, or cloud computing? In other words, what is new about QC from an ethical point of view? The paper aims to answer these questions by (a) developing an analysis of the existing literature on the ethical and social aspects of QT and QC and (b) studying these problems through already existing approaches to ethics of emerging technologies (Brey, 2012a, b). The conclusion is that QC poses new ethical issues that require new conceptual tools and methods. Some of these problems are augmented versions of those already posed by other digital technologies such as AI. Others are completely new; these are mainly problems posed by purely quantum phenomena, such as entanglement and its applications, for example, quantum teleportation, quantum swapping, and the concept of "virtual connectivity."

The methodology followed is based on a review and analysis of existing literature. Starting from this review, some fundamental ethical problems related to the technical characteristics of QC have been identified and analyzed. The identification and analysis of ethical problems were carried out with reference to engineering ethics (Taebi, 2021), data ethics (O'Keefe & O'Brien, 2018), and AI ethics (Coeckelbergh, 2021).

2 Literature Survey

A systematic literature search was performed via keyword queries on four widely used indexing services—Scopus, Web of Science, Philpapers, and Google Scholar—to identify and analyze the literature on the ethical and societal impacts

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[4] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

of QC and QT. The research was limited to English-language literature. Five key search terms were used: “ethics and quantum technology,” “morals and quantum technology,” “ethical quantum technology,” “society and quantum technology,” and “social quantum technology.” I selected only those papers whose central topic was the ethical and societal impacts of QT and QC, therefore excluding all papers that did not consider QT and QC as their core focus and treated them just as examples or secondary topics. I have isolated 21 recent relevant papers and will only comment on the most relevant ones.

The first group of studies analyzed can be classified as a type of essay focused on problems of a social and communicative nature, for example, how we should communicate about QT. Wolbring, (2022) analyzes social issues, especially those concerning equity, diversity, and inclusion (EDI), for specific marginalized groups in debates, policy documents, and the academic literature on QT. The results of the survey pose a serious problem: “The quantum technologies-focused academic literature rarely if ever engages with the ‘social’ of quantum technologies” (24). However, the findings indicate opportunities for broadening the quantum technologies discourse to the “social” and to EDI, as well as for “an increase in inter-intra-trans-disciplinary and intersectional collaborations” (24). Mapping the effects of QT on the “social” is essential for identifying the stakeholders and enhancing EDI efforts, understanding, and governance.

Four other studies have followed this same line of research. The first, Vermaas (2017), stresses the need for all stakeholders to understand QT to a reasonable degree as the basis for an effective and lasting public debate. QT are technologies that “make quantum theory technologically applicable, and quantum theory is up to this day framed as an enigmatic theory whose counterintuitive descriptions of the physical realm are difficult to master” (242). For this reason, philosophers of physics can play a key role by showing how quantum mechanics and related technologies are close to everyday practices. The second study, by Coenen & Grunwald, (2017), proposes a strong RRI approach, envisaging the involvement of parliaments. In a strong RRI approach, at least some public dialogue and engagement activities should be designed such that they allow for input from citizens and representatives of social interests to be fed into parliamentary and other political deliberation and decision-making processes in a systematic, transparent, and responsive manner. The third study, de Wolf, (2017), identifies some ethical challenges posed by quantum cryptography, quantum simulation, and quantum optimization, focusing above all on the problem of the quantum divide. The fourth study, Grunwald, (2017), concentrates on the narrative around QT and how important it is to produce a different non-mathematical and less mysterious narrative of the technology that is accessible to the general public and thereby helps foster trust in QT. To popularize QT, we must convey the beauty and complexity of quantum mechanics.

The present paper intends to develop this line of research by focusing on the originality of the ethical problems posed by QTs and, in particular, by QC.

The second group of studies is more concerned with the legal aspects of QTs. Kop’s approach (2021; see also Kop & Hiscott, 2021) proposes ten guiding principles for the development and application of QT that are inspired by AI ethics (i.e., the Asilomar principles) and nanoethics. However, these 10 principles and the corresponding social risks identified by Kop are very generic. It is not clear what really differentiates QT from AI and nanotechnology. Understanding whether this difference exists—how QTs are different on an ethical and social level compared to other technologies—is the purpose of this paper. Furthermore, Kop has a legal-oriented approach that is only partially ethical (see also Kop, 2022; Jeutner, 2021; Paperin, 2007).

Quantum technologies are dual use and therefore also have military applications. The third group of studies considered in this survey concerns the application of QT and QC to military technologies. Krelina, (2021) reviews and maps possible quantum technology military applications: serving as an entry point for international peace and safety assessment, ethics research, military policy, governmental policy, strategy, and decision-making. Quantum technologies used for military applications (e.g., quantum radar, quantum simulation for chemistry, quantum cryptoanalysis, quantum key distribution) provide new military capabilities, such as improved effectiveness and increased precision. Military use of these technologies would lead to “quantum warfare,” wherein new military strategies, doctrines, policies, and ethics should be established. The topic of military use of QT and QC is discussed in other studies and reports, such as Lele (2021), Neumann et al. (2020), Smith (2020), Parker (2021, 2022), McKay (2022), Wolf (2019), Grobman (2020).

Perrier (2022) sets guidelines for what he calls the “quantum ethics research program.” Perrier (2022) is rightly convinced that “there are unique characteristics of quantum computation, quantum information processing and certain quantum technologies which motivate the development of quantum-specific ethical epistemology” (Perrier, 2022, 10). However, despite the importance of his contribution, Perrier can be criticized. He makes an important contribution, but in my opinion, it is a limited one in the sense that it is only deals with some aspects of the ethical investigation on QC. Furthermore, Perrier indicates four key factors for quantum ethics: computability, complexity, consistency, and controllability, which are not strictly ethical concepts (27–29), although they can obviously have an ethical impact.

3 Generic Ethical Issues in Quantum Computing

3.1 The Technology

In 1982, physicist Richard Feynman suggested that quantum mechanical phenomena could be used to simulate a quantum system more efficiently than a naïve simulation on a classical computer (Feynman, 1982; Lloyd, 1996). In 1993, Bernstein and Vazirani demonstrated that quantum computers could violate the extended Church-Turing thesis—a foundational principle of computer science that said that the performance of all computers was only polynomially faster than that of a probabilistic Turing machine (Bernstein & Vazirani, 1993). The quantum algorithm they elaborated on offered an exponential speedup over any classical algorithm for the computational task of recursive Fourier sampling. Simon (1997) invented another example of a quantum algorithm demonstrating exponential speedup for a different computational problem. Quantum computation can violate the extended Church-Turing thesis;

therefore, only quantum computers are capable of exponential speedups over classical computers (I only provide an outline here; so for more technical details, see Hayashi (2006), Hayashi et al. (2015), Nielsen and Chuang (2011), and Zygelman (2018)).

On an abstract level, computation is a procedure that transforms inputs into outputs through a sequence of elementary operations (Hayashi et al., 2015, 37). In classical computation, the input/output system is not interpreted in terms of quantum mechanics in the sense that all quantum effects present in the device are systematically neglected. In quantum computing, on the other hand, the input/output system is interpreted according to quantum mechanics. Therefore, the first essential difference between these two models is the interpretation of the data and the computational process. QC introduces a completely new conceptual and logical framework that differs from the classical one.

The difference between classical and quantum computations is evident in the distinction between bits and qubits. In a classical computational system, there are only two possible states—1 and 0—which are ontologically determined, while epistemologically, they can be determined or indeterminate, that is, known in an approximate and probabilistic way. In other words, classical computation is based on the measurement of a physical system represented as a set of two possible states whose structure is governed by Boolean logic. Consequently, "uncertainty about what state a classical system is in is thus not ontological, but epistemological, a representation of the uncertainty of our knowledge rather than any intrinsic indeterminacy about the system state itself" (Perrier, 2022, 17).

In a quantum computational system, the possible states are ontologically and epistemologically indeterminable. The notion of the "state of the system" changes radically based on interpretations of calculations (see Susskind & Friedman, 2014, 36). In fact, the state of a quantum system is indeterminable in the sense that the only thing we can know about it is a set of probabilities and their interpretations, the so-called probability amplitudes. A quantum bit, or qubit, has two quantum states analogous to classical binary states. While the qubit can be in either state, it can also exist in a superposition between the two. These states are often represented in the so-called Dirac notation, where the state's label is written between two "kets", | and ⟩. Dirac's formalism is used more generally in mathematics to denote abstract vectors in a Hilbert space. Thus, a qubit's two component—or basis—states are generally written as $| 0\rangle$ and $| 1\rangle$. In general, the physical state of a qubit is the superposition $| \psi \rangle = \alpha | 0 \rangle + \beta | 1 \rangle$(where α and β are complex numbers). The states $| 0 \rangle$ and $| 1 \rangle$ are known as the computational basis states, and form an orthonormal basis for this vector space. According to quantum theory, when we try to measure the qubit in this basis in order to determine its state, we get either $| 0 \rangle$ with probability $| \alpha | 2$ or $| 1 \rangle$ with probability $| \beta | 2$.

In other terms, any qubit wave function may be written as a linear combination of the two states, each with its own complex coefficient:

$$a_i : |\psi >= a_0|0 > |+a_1|1 >$$

Since the probability of reading a state is proportional to the square of its coefficient's magnitude, $| a_0 |^2$ corresponds to the probability of detecting the state $| 0\rangle$ and $| a_1 |^2$ to the probability of detecting $| 1\rangle$. The sum of the probabilities of each possible output state must be 100%, mathematically expressed in this case as $| a_0 |^2 + | a_1 |^2 = 1$ (i.e., the qubit is a unit vector in the aforementioned Hilbert space; see Hagar & Cuffaro, 2022; Grumbling & Horowitz, 2019, 35; Ayoade et al., 2022).

This leads us to focus on some fundamental aspects of QC that can only be touched on in this section but have a major impact on the design of quantum computational systems:

- *Superposition.* A quantum system can exist in two or more states at once, which is referred to as a superposition of states or a "superposition state." The wave function for such a superposition state can be described as a linear combination of contributing states with complex coefficients. The latter describes the magnitude and relative phases between the contributing states. This feature is essential: "quantum superposition is the framework for understanding all quantum phenomena" (Hughes et al., 2021, 24).
- *Coherence.* When a quantum system's state can be described by a set of complex numbers, one for each basis state of the system, the system state is said to be coherent. Coherence is necessary for quantum phenomena, such as quantum interference, superposition, and entanglement. Short interactions with the environment cause quantum systems to slowly decohere. Environmental interactions make even the complex coefficients for each state probabilistic.
- *No-cloning theorem.* This theorem prohibits copying an unknown quantum state (Nielsen & Chuang, 2011). As a consequence, it is not allowed to copy and re-transmit—or to transmit multiple copies of—a qubit whenever its state is unknown. This theorem has profound consequences for qubit error correction, as well as for quantum communication security (see Dieks, 1982).
- *Entanglement.* Regardless of the distance between them, the entangled particles exhibit special correlations that are instantaneous and appear to defy classical notions of locality. When the state of one entangled particle is measured, it instantaneously affects the state of the other(s), even if they are far apart, leading to what Einstein called "spooky action at a distance." This phenomenon arises when the wave functions for different particles are not separable—in mathematical terms, when the wave function for the entire system cannot be written as a product of the wave functions for each particle (Grumbling & Horowitz, 2019, 28).

3.2 Data Management

As Perrier, (2022) states, "there are potential ethical issues to be explored about the ethics of encoding data (such as from a fair representation learning)" (20), which is also a concern found in AI ethics (McNamara et al., 2019). These characteristic aspects of QC entail a radical transformation of the understanding of data on multiple intertwined levels. Table 1 schematically illustrates the impact of QC on different aspects of understanding of data:

Data mining is the process of collecting, filtering, and cleaning the data before storing it in a data warehouse or some other storage device. The data must be filtered

Table 1 The impact of QC on different aspects of understanding of data

Data features	Impact
Volume	High impact: risk of a new data deluge
Velocity	High impact: speedup of production and analysis
Variety (data types)	High impact: need for new data classifications
Veracity (truthfulness)	High impact: risk of high fragility of data
Variability (inconsistencies)	High impact: need for new types of controls
Validity (correctness for intended uses)	High impact: need for more supervision
Visualization	High impact: need for new types of visualization

and compressed so that it does not throw away any relevant information. Defining such filters is one of the major challenges (Gupta & Rani, 2019). Another challenge is enabling the automatic generation of metadata. Metadata describes what data are logged and how they are logged and measured. In this case, QC can make a difference by providing new tools and conceptual solutions. For example, it is likely that QC will provide new resources for tagging data and establishing new categories of metadata thanks to (a) heuristic methods optimization, (b) improved database searching, and (c) dense coding technique, that is, the ability to communicate a number of classical bits of information by only transmitting a smaller number of qubits, under the assumption of sender and receiver pre-sharing an entangled resource (Horodecki et al., 1997, 10–11). In certain contexts, QC exponentially increases the capacity to produce and process data.

However, there is a crucial problem that makes the integration of QC in classic data mining very complex: the concept of quantum information is completely different from that of classic information. QC requires a major paradigm shift for harnessing the peculiarities of quantum mechanics. Here are some points to note regarding quantum information—however, the implications of decoherence, entanglement, and superposition for data mining remain to be fully explored:

1. Decoherence and the no-cloning theorem make it impossible to think of information in the classical sense, that is, as something that can be copied and recorded indefinitely and safely.
2. Entanglement is the essential feature of quantum information and communication. This quantum phenomenon has enormous repercussions for data storage and networks. The digital identity in QC is not linked to the data stored and copied but rather to connectivity and synchronicity.
3. Superposition allows you to encode data in a completely new way. In the same qubit, we can encode and use very different types of data.

Quantum information is therefore (a) fragile and (b) unstable. It is fragile because it cannot be copied and stored, and it is unstable because it depends on entanglement and superposition. Quantum information is distinguished by these aspects, but it is not the case that all quantum information is in a superposition state or entangled.

Table 2 Quantum characteristics that pose fundamental ethical problems in data management

Identity	Disintegration of identity understood as the definition of boundaries between individuals and groups. Entanglement, superpositions, and the no-cloning theorem pose high risks of lack of identification and autonomy. The superposition would allow for combining and mixing data from different sources to build increasingly complex and stratified identities. For example, in the encoding phase, the superposition would allow the building of digital identities using data that does not belong to that identity, individual, or group
Privacy	It is impossible to think of privacy in the classical sense, that is, as the protection of personal information and their communication. The no-cloning theorem guarantees maximum security but also causes data fragility, that is, difficulties in controlling data. Moreover, the use of quantum superposition in encoding data would make it possible to encode sensitive data and misuse this data without getting caught
Ownership	Difficulty in controlling access and data management. For example, blind quantum computing guarantees maximum security, but is also a big risk because it could be used for the purpose of hacking servers
Traceability	The complexity of quantum data makes it more difficult to reconstruct their history, location, and application. Entanglement and superposition erase the very idea of a data location. This damages the trust in the data and their degree of reliability (more on this later)

The instability of quantum information is made clearer by two other characteristics of QC:

1. In a quantum network, any node sharing entanglement resources can act either as source or as destination—there is not a fixed, pre-established order. Moreover, it has been discovered that the order among the communication channels traversed by quantum information carrier can be indefinite (Illiano et al., 2022, 11).
2. Also, unlike classic bits, qubits are "stateful," in the sense that to use the qubit, we need information about its state (Illiano et al., 2022, 9). While to operate on the classic bit, we do not need further information on its state, in the case of the qubit, the situation changes; for example, any qubit inevitably degrades over time due to the decoherence phenomenon, so to properly use a qubit, it is necessary to have information on the residual coherence time. This greatly increases the complexity of quantum data management.

These characteristics pose fundamental ethical problems (Table 2):

Another important consideration concerns the risk of a new "data deluge." The enhancement of current digital technologies thanks to QC will certainly lead to the production of much more data and, therefore, an acceleration of the pace of expansion of the digital universe. Moreover, other QT applications such as quantum sensors, quantum clocks, quantum radar, and quantum imaging will provide new types of Big Data. This poses a huge problem in terms of storage. Increasingly complex data centers will be needed, and this could pose new environmental issues with ethical consequences.

3.3 Processes: a New Form of Opacity

Given the stochastic nature of the quantum computational system, the relationship between inputs and outputs is not necessarily always the same: "running the same program over and over again will not necessarily lead to identical output" (Perrier, 2022, 11). This aspect has enormous implications, as it forces us to rethink the crucial problem of process opacity, which is closely related to the question of accountability for unjust results and unintended consequences, and the ethical criteria to be used in the design of quantum algorithms (Ayoade et al., 2022; Weiss & Saffman, 2017).

However, the stochastic nature of the system is not an essential feature of QC. The crucial problem is that there is a fracture between the data and the information in QC.

When we extract data from the qubit, we take a measurement. By measuring the system, we extract the data and build information. Now, in the act of measurement, what physicists call the "collapse of the wave function" occurs. The wave function in quantum mechanics evolves deterministically, according to the Schrödinger equation, as a linear superposition of several states. However, the actual measurement always finds the physical system in a defined state. There are many different interpretations[5] of measurement in quantum mechanics (see Vermaas, 1999, Chapters 10 and 14). The state determines, through the Born rule and Schrödinger equation, the probabilities of finding outcomes after the measurement. The interpretation of these results allows us to deduce the properties of the system. The point is that "all information about the [probability] amplitudes is destroyed upon measurement" (Grumbling & Horowitz, 2019, 71). This means that all data prior to the measurement are lost. Measurement fundamentally disrupts a quantum state: "it [the quantum state] 'collapses' the aspect of wave function that was measured into a single observable state, resulting *in a loss of data*. After the measurement, the quantum object's wave function is that of the state that was detected, rather than that of its premeasurement state" (Grumbling & Horowitz, 2019, 57; emphasis added). This is what physicists call the "measurement problem," which is crucial. De Lima Marquezino et al., (2021) say that "the amplitudes of the state $|\psi\rangle$ as it is before measurement are inaccessible. The measurement process inevitably disturbs $|\psi\rangle$ forcing it to collapse to one vector of the computational basis. This collapse is non-deterministic, with the probabilities given by the squared norms of the corresponding amplitudes in $|\psi\rangle$" (19). From this standpoint, the measurement is only a statistical tool—a way to predict the evolution of certain measures without any ontological or semantic commitment. As Maudlin (2019) writes, this problem has nothing to do with measurement itself: "It is rather the problem of physically explaining how experiments come to have the sorts of outcomes we take them to have" (Maudlin, 2019, 98).

A thorough discussion of these issues is beyond the scope of this paper. However, I believe that the problem of measurement is fundamental for QC because it is connected to another crucial problem: that of transparency, that is, the communication,

[5] By "interpretation" I do not mean that these theories are mere arbitrary inventions. Instead, they are all well-constructed scientific theories with numerous experimental ramifications (Carroll, 2020, 26).

explanation, and interpretation of the quantum algorithm and its decisions. Can we open the quantum black box? Most people do not know how most algorithms (or technology) work and are not provided with any explanation of why they do. Yet, they accept the technology in their lives. There is considerable debate as to whether people actually want interpretability. This issue becomes even more complex in QC because the opacity of QC is not only epistemic, like that of classical AI, but ontological.

For instance, the lack of transparency is an inherent characteristic of self-learning algorithms, which alter their decision logic and produce new sets of rules during the learning process, making it difficult for developers to maintain a detailed understanding of why certain changes have been made (Floridi, 2022; Tsamados et al., 2022; Burrell 2016; Buhmann et al., 2019). However, this does not necessarily translate into opaque outcomes, as even without understanding each logical step, developers can adjust hyperparameters, i.e., the parameters that govern the training process, to test for various outputs. The complexity of neural networks is due to the large amount of data and processes and therefore to the human cognitive inability to process them. In QC, the situation is much more complex because opacity does not concern only human limits, but rather the processes themselves. The explanation and justification of the algorithm's behavior therefore need two interpretative levels: (a) the epistemic one, which is in common with classical systems, and (b) the ontological one, which requires an interpretation of quantum mechanics.

From an engineering point of view, the problem of measurement is irrelevant, as it is an interpretative issue and therefore does not concern the technical functioning of QC. However, it poses serious problems on an ethical level. How can we explain and justify the decision-making process of a quantum algorithm if we lose all the data before the measurement? How can we be sure that the process followed by a quantum algorithm is ethically correct if we cannot completely access it as it unfolds before the measurements? How can we be sure that phenomena such as entanglement and superposition do not produce effects contrary to ethical standards and protocols, such as the use of sensitive data to reduce the decoherence of the system? The new form of quantum opacity complicates the problem of trust in the algorithm, which is connected to transparency (Coeckelbergh, 2021). This also has consequences for the level of responsibility analysis, that is, what Floridi, (2016) calls "distributed moral responsibility" in a network of agents. Therefore, QC requires a rethink of the relationship between the explainability and transparency of algorithms as well as the limits of each.

4 The Algorithm Design

Research on the ethics of algorithms has grown substantially over the past decade. Alongside the exponential development and application of machine learning algorithms, new ethical issues and solutions relating to their ubiquitous use in society have been proposed (Tsamados et al., 2022). For example, racial minorities might be less likely to find housing via algorithmic matching systems, algorithmically controlled job matching systems might restrict the information available for use by the economically disadvantaged, or online markets might unfairly make goods more expensive for particular demographics or geographic locations. These issues are all cases of algorithmic biases (Bozdag, 2013; Datta & Tschantz, 2015). Studies also suggest evidence of racial discrimination in prediction algorithms and gender bias by Google (Zhu et al., 2018).

Tsamados et al. (2022) propose distinguishing six types of ethical problems raised by algorithms:

- Inconclusive evidence (focusing on non-causal indicators can distract attention from the actual causes of a given problem)
- Inscrutable evidence
- Misguided evidence
- Unfair outcomes
- Transformative effects
- Traceability

The first three have an epistemic nature concerned with the accuracy and quality of the data for the ongoing process. The fourth and fifth are more normative in nature, concerned with the effects of processes. The sixth is relevant from both an epistemic and a normative point: it is the problem of transparency of the processes.

Let us try to translate them into QC:

- Inconclusive evidence: This is the practice of *apophenia*, that is, "seeing patterns where none actually exist, simply because massive quantities of data can offer connections that radiate in all directions" (Boyd & Crawford, 2012, 668). Focusing on non-causal indicators may distract attention from the underlying causes of a given problem, and this can have major ethical consequences (Floridi et al., 2020). Now, QC will increase the connectivity of our algorithms and networks. In fact, "the nonclassical correlations provided by entanglement can be leveraged not only for transmitting classical and quantum information, but also for enabling groundbreaking applications with no-counterpart in the classical Internet, ranging from secure communications through blind computing to distributed quantum computing" (Illiano et al., 2022, 2). Entanglements allow new forms of connectivity, such as quantum teleportation and quantum swapping (Briegel et al., 1998). While classical connectivity strictly depends on classical physical channels, in quantum networks, we can use "virtual links" and "virtual connectivity" or "augmented connectivity" (Illiano et al., 2022, 13) that are not affected by the conditions of classical physical channels; for example, quantum teleportation is a form of virtual link because it enables the transmission of one qubit without any use of a physical channel—"as long as an entangled state is shared between two nodes, they can transmit a qubit regardless of the instantaneous conditions of the underlying physical quantum channel" (Illiano et al., 2022, 14). These new forms of connectivity increase the complexity of the analysis and, therefore, the risk of apophenia.

- Inscrutable evidence: This problem is related to what was said above about the specific opacity of the QC; we need to establish new testing and auditing tools suited to QC characteristics, as well as new types of explanations and communications.
- Misguided evidence: The problem of bias in QC is strictly related to access and use. It is likely that quantum computers will not be available to the public for various reasons (economic, social, intellectual, etc.). Restricted access can be connected to the prevalence of restricted social groups in the use of these machines. This situation comes with the risk of facilitating discrimination, fake news, and exclusion of minorities.
- Unfair outcomes: Many definitions of algorithmic fairness have gained prominence in the recent literature (Kleinberg et al., 2016; Corbett-Davies & Goel, 2018). The greater computational power provided by the QC could allow the development of strategies capable of improving fairness, conceived as statistical parity between social groups. For example, a quantum algorithm could take advantage of "virtual connectivity," which is more dynamic than physical connectivity, to remedy the problem of inequality in a service distribution network. In fact, augmented connectivity can redefine the same concept of "neighborhood" in a city; "two nodes can be 'neighbors' in the augmented graph whenever they are directly connected by an augmented link, even though they are physically remote from each other. This new concept of neighborhood has no counterpart in the classical network" (Illiano et al., 2022, 16). Therefore, the algorithm could exploit the "virtual connectivity" of QC to activate and develop the services, even in those areas that are most discriminated against because they are not reached by classical physical connectivity.
- Transformative effects: It is foreseeable that quantum algorithms will make AI much more dynamic, pervasive, and proactive than classical AI. This could seriously damage the autonomy of humans. The problem is complicated by the low opacity of these algorithms.
- Traceability: The technical complexity and dynamism of AI algorithms make them prone to concerns of "agency laundering," which consists of distancing oneself from morally suspect actions, regardless of whether those actions were intended or not, by blaming the algorithm (Rubel et al., 2019). This is practiced by organizations as well as by individuals. It is foreseeable that the complexity of QC could exacerbate this phenomenon. It is likely that the no-cloning theorem will have a huge impact on the traceability of responsibility in QC.

Let us now analyze a concrete use case. An important question is the moral implications of entanglement. As mentioned earlier, entanglement is the phenomenon that characterizes quantum mechanics more than any other. Entangled particles exist in a shared state, such that any action on a particle instantaneously affects the other particle(s) as well, i.e., they are perfectly synchronized. This quantum correlation and synchronization, with no counterpart in the classical world, holds regardless of the distance between the particles. Entanglement is not about information, but correlation. If Alice, Bob, and Eve share three entangled qubits, and all agree beforehand to follow the same procedure with them (measuring in this basis, if it is 0, do this, if it is 1, do that), in the end they can use it to get synchronous actions, but would have no control on whether that action is 0 or 1. Therefore, entanglement as a resource gives us access to a nonlocal correlation, but not to information. Alice, Bob, and Eve's actions become correlated irrespective of whether the information is 0 or 1. This means that entanglement gives them distributed and nonlocal randomness, but cannot be used to transmit either 0 or 1. If Alice sends Bob 0s or 1s (and not a combination of both simultaneously) using a qubit, this is not an entangled state (it is technically called a "separable state," which is still quantum mechanical, but not entangled). Therefore, if Alice does not have the measurement results from Bob, she cannot use entanglement to reconstruct the information.

Now, the ability to produce and manage entanglement over great distances could be used as a lethal weapon. Entanglement distribution over long distances can be achieved via quantum repeaters with satellite links (Boone et al., 2015; Sangouard et al., 2007).

A potential enemy wishing to attack a quantum network could use remote entanglement distributions to warp information within the network and manipulate it without being detected. The potential hacker could produce an entanglement between a photon encoding the qubit flowing in the network (A) and another photon outside the network (B). In this way, they would be able to influence and modify the synchronization used in the network. Entangling qubit A with qubit B would allow them to influence the synchronization between B and A without needing any contact or any kind of classical interaction. This could seriously affect communication in the network. The hacker could even use the entangled pair to send information somewhere else through teleportation, using the attacked network as a repeater. The attack could not be discovered for several reasons: (a) in general, the duration of entanglement is very short; (b) there are several strategies for the detection of entanglement, but implementing them is very complex—and it is not certain that they can detect the entanglement (Ayoade et al., 2022); (c) creating network security barriers may not help as the enemy could use quantum tunneling.

This is obviously a futuristic scenario, but it is also a realistic eventuality. For this reason, the design of the algorithm should include certain limitations in the use of entanglement based on clear and shared rules and values. An important research direction is therefore that of governance of entanglement in the quantum Internet.

5 The Case of Quantum Cryptography

5.1 Introduction

Cryptography is an indispensable means used to protect information in computer systems and is widely used to protect communications on the Internet. In 1994, Peter Shor showed that several important computational problems could, in principle, be solved significantly more efficiently using a quantum computer—if such a machine could be built. Specifically, he derived algorithms for factoring large integers and solving discrete logarithms rapidly—problems that could take even the largest computer today thousands or millions of years, or even the lifetime of the universe, to compute. This was a striking discovery because it also suggested that anyone with a real-world quantum computer could break the cryptographic codes, compromising the safety of encrypted communications and stored data, and potentially uncovering protected secrets or private information. Indeed, most of our digital infrastructure, and basically anything we do online—whether it is video conferencing, sending e-mails, or accessing our online bank account—is encrypted through cryptographic protocols based on the difficulty of solving factorization problems (i.e., the RSA algorithm). A breakdown caused by a quantum computer could have serious implications. The first organization able to develop a quantum computer implementing Shor's algorithm will be able to decrypt any communication and code. Privacy and intelligence will be seriously damaged, and governments will face major problems as they try to defend their communications. Potential hackers could also steal classified information today and decrypt it in the future when they will have a quantum computer.

5.2 Moral Analysis

The ethical problem at the heart of this QC application concerns, above all, the clash between security and privacy. Both are considered intrinsic values: "The right balance between privacy and justified surveillance for safety purposes is a very tricky ethical question" (de Wolf, 2017, 274). There are four stakeholders involved: institutions, customers/users, companies, and academia. Institutions are tasked with maintaining safety and surveillance; this is their key value. Companies and users ask for privacy or the protection of their identity. Furthermore, companies want to be able to develop trade and business, which are their main values, and they contribute to the main moral problem—that is, the clash between security and privacy.

Now, how should a government interfere in the transition phase from current cryptographic systems to quantum ones? The crucial problem at this stage is that our hypothetical government does not know if other governments, hackers, or companies have already developed a quantum computer big enough to break systems and steal data. It would only know this once the attack had occurred, and so would have no time to react.

There are two options at this point. The first is to immediately guarantee higher levels of safety by strengthening current systems, such as using post-quantum algorithms (e.g., lattice systems, coding-based systems, supersingular isogenies, hash-based signatures, etc.). This option, however, implies (a) a significant increase in controls and a progressive diminishment of the privacy and autonomy of companies and citizens, (b) a decrease in the transparency of government activities, and (c) the moral risk of paternalism, that is, the government deciding what is best for citizens and companies without consulting them. The second is to accelerate the migration from our current cryptographic systems to fully quantum systems. The risk, in this case, is that this migration is too slow and therefore (a) incomplete, exposing it to possible attacks, and (b) does not cover some of the interested parties, that is, users and companies that have not yet developed the appropriate technology. Both consequences could greatly increase the inequalities between countries and citizens and between those who already have quantum cryptographic systems and those who do not and who have less security and privacy as a result. This could fuel new forms of exploitation and damage to human dignity.

Dismantling existing safety systems and replacing them with post-quantum systems could take a long time. Grumbling & Horowitz, (2019, 109) argue that the process could last at least 20 years. Furthermore, migration does not ensure complete security since even if the migration started today, many sensitive data (i.e., government-classified documents whose content cannot be made public for at least 50 years) could be stolen and stored before being decrypted when a large quantum computer running quantum error correction becomes available. If a fault-tolerant quantum computer with a large number of qubits is built over the next 25 years, all documents classified today are potentially at risk.[6] The encryption keys that quantum key distribution produces cannot be broken by Shor's algorithm. This poses a further problem, namely, that of an excess of privacy and security. Criminal organizations and individual citizens could use quantum keys to bypass controls and commit crimes. This could lead to an increasingly decentralized quantum Internet, with all the consequences that this entails in terms of distributive justice. Furthermore, rethinking privacy also means rethinking the ethics of welfare and, therefore, key concepts, such as interdependence, solidarity, happiness, and the value of citizenship. A question remains crucial: Is non-breakable cryptography—that is, an absolute secret—ethically acceptable?

It would be simplistic to oppose security and privacy strictly. Obviously, the QTs will require us to find new balances between these values. Discussing the relationship between security and privacy in more depth is not the purpose of this paper. Here, I will limit myself to emphasizing that quantum cryptography and QC force us to rethink the concept of privacy itself.

The QC forces us to separate two sides of privacy: (a) privacy as information control and (b) privacy as the construction of one's social identity (Elliott & Soifer, 2022). These two concepts are connected in classic communication systems: privacy implies control over the dissemination of information and, therefore, over one's social identity, that is, how we are seen and considered by others. In the quantum world, this changes. On the one hand, the control of information becomes increasingly complex due to the fragility of the information itself, of the storage and management systems, and therefore also of security, as we have seen in the previous parts of this paper. On the other hand, QC asks us to rethink the construction of our digital identity in different terms. This is an unexplored problem that calls for new research.

5.3 The Overlapping Consensus

Finding a good balance between privacy and security in an ever-changing context requires a solid international regulatory framework. Even if companies and institutions

[6] See: https://csrc.nist.gov/Projects/post-quantum-cryptography

have different values and goals, they can agree on the moral assessment that the right balance must be found between privacy and security in a post-quantum world. A possible dialogue model could be Rawls's overlapping consensus (Rawls, 1993, 2001).

An overlapping consensus is not a compromise because it requires each of the discussants to justify it in terms of their own reflections and evaluations. There are three fundamental conditions for reaching this type of consensus: (a) all parties must accept a reasonable level of pluralism in moral views; (b) inclusiveness, in the sense that all relevant perspectives must be included in the debate; and (c) openness, meaning that new considerations and parts can always enter the debate (van de Poel & Royakkers, 2011, 156–57). This means that the actors in the process do not necessarily have to share the same values, but they must be able to justify the common agreement reached through their values and reflective processes.

In the case of quantum cryptography, the overlapping consensus model can be a useful tool when actors who do not share the same values, such as US and China, need to establish a common regulatory framework. The need to avoid the danger of a "cryptographic war" could require finding a vast international agreement, even among those nations that have different conceptions of democracy and communication about sensitive data but that recognize the common danger. This does not mean that I think the Rawlsian model is perfect. Many criticisms can be made of this model (Watene & Drydyk, 2016). However, in such delicate and complex situations as a "cryptographic war," a moderate level of overlapping consensus could be the starting point for reaching a greater consensus about certifications and standards.

6 Conclusions

This paper is intended to contribute to research on the ethical impact of QT and QC. I analyzed some of the main ethical problems raised by QC on three levels: technology, artifact, and applications. A very complex picture emerges. QC features such as the no-cloning theorem, blind computing, superposition, entanglement, or the concept of "virtual connectivity" are extremely ambiguous because they pose both risks and opportunities in terms of security, privacy, data management, etc. New research is needed to better understand these problems and their implications. I indicate two important possible future research directions:

- Centralized versus decentralized regulation
- Strategy of communication to popularize QT and QC and increase public acceptance and trust

Abbreviations *QT*: Quantum technologies; *QC*: Quantum computing

Author Contribution Not applicable.

Data Availability Not applicable.

Declarations

Ethics Approval and Consent to Participate Not applicable.

Consent for Publication Not applicable.

Competing Interests The authors declare no competing interests.

References

Ayoade, O., Rivas, P., & Orduz, J. (2022). Artificial intelligence computing at the quantum level. *Data*, (28)7, 1–12. https://doi.org/10.3390/data7030028

Bernstein, E., and Vazirani, U. (1993). "Quantum complexity theory" Proceedings of the 25th Annual ACM Symposium on Theory of Computing (STOC '93), San Diego, 16–18 May 1993, 11–20.

Boone, K., Bourgoin, J., Meyer-Scott, E., Heshami, K., Jennewein, T., & Simon, C. (2015). Entanglement over global distances via quantum repeaters with satellite links. *Physical Review A, 91*, 052325 https://journals.aps.org/pra/abstract/10.1103/PhysRevA.91.052325

Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society, 15*(5), 662–679. https://doi.org/10.1080/1369118X.2012.678878

Bozdag, E. (2013). Bias in algorithmic filtering and personalization. *Ethics and Information Technology, 15*, 209–227.

Brey, P. (2012a). Anticipating ethical issues in emerging IT. *Ethics and Information Technology, 14*, 305–317.

Brey, P. (2012b). Anticipatory ethics for emerging technologies. *NanoEthics, 6*, 1–13.

Briegel, H., Dür, W., Cirac, J., & Zoller, P. (1998). Quantum repeaters: The role of imperfect local operations in quantum communication. *Physical Review Letters, 81*, 5932 https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.81.5932

Buhmann, A., Paßmann, J., & Fieseler, C. (2019). Managing algorithmic accountability: balancing reputational concerns, engagement strategies, and the potential of rational discourse. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-019-04226-4

Burrell, J. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data and Society*, 1–12.

Carroll, S. (2020). *Something deeply hidden: Quantum world and the emergence of spacetime*. Dutton.

Coeckelbergh, M. (2021). *AI Ethics*. MIT Press.

Coenen, C., & Grunwald, A. (2017). Responsible research and innovation (RRI) in quantum technology. *Ethics and Information Technology, 19*, 277–294.

Corbett-Davies, S., & Goel, S. (2018). *The measure and mismeasure of fairness: A critical review of fair machine learning*. arXiv. https://arxiv.org/abs/1808.00023

Datta, A., & Tschantz, M. C. (2015). Automated experiments on Ad privacy settings. *Proc Priv Enhanc Technol, 1*, 92–112.

De Wolf, R. (2017). The potential impact of quantum computers on society. *Ethics and Information Technology, 19*, 271–276.

De Lima Marquezino, F., Portugal, R., & Lavor, C. (2021). *A primer on quantum computing*. Springer.

Dieks, D. (1982). Communication by EPR devices. *Physics Letters A, 92*, 271–272.

Elliott, D., & Soifer, E. (2022). AI technologies, privacy and security. *Frontiers in Artificial Intelligence*. https://doi.org/10.3389/frai.2022.826737

Feynman, R. P. (1982). Simulating physics with computers. *International Journal of Theoretical Physics, 21*(6–7), 467–488.

Floridi, L. (2016). Faultless responsibility: On the nature and allocation of moral responsibility for distributed moral actions. *Philosophical Transactions of the Royal Society A*.3742016011220160112

Floridi, L. (2022). *Etica dell'intelligenza artificiale*. Raffaello Cortina.

Floridi, L., Cowls, J., King, T. C., & Taddeo, M. (2020). How to design AI for social good: Seven essential factors. *Science and Engineering Ethics, 26*(3), 1771–1796.

Geels, F. (2005). Co-evolution of technology and society: The transition in water supply and personal hygiene in the Netherlands (1850–1930)—a case study in multi-level perspective. *Technology in Society, 27*(3), 363–397.

Grobman, S. (2020). Quantum computing's cyber-threat to national security. *PRISM, 9*(1), 52–67.

Grumbling, E., & Horowitz, M. (Eds.). (2019). *Quantum computing progress and prospects*. The National Academies Press.

Grunwald, A. (2017). Narratives of quantum theory in the age of quantum technologies. *Ethics and Information Technology, 19*, 295–306.

Gupta, D., & Rani, R. (2019). A study of big data evolution and research challenges. *Journal of Information Science, 45*(3), 322–340.

Hagar, A., & Cuffaro, M. (2022). Quantum computing. In E. N. Zalta & U. Nodelman (Eds.), *The Stanford encyclopedia of philosophy (fall 2022 edition)*.

Hayashi, M. (2006). *Quantum information: An introduction*. Springer.

Hayashi, M., Ishizaka, S., Kawachi, A., Kimura, G., & Ogawa, T. (2015). *Introduction to Quantum Information Science*. Springer.

Hoofnagle, C., & Garfinkel, S. (2022). *Law and policy for the quantum age*. Cambridge University Press.

Horodecki, R., Horodecki, P., Horodecki, M., & Horodecki, K. (1997). *Quantum entanglement*. arXiv. https://arxiv.org/abs/quantph/0702225

Hughes, C., Isaacson, J., Perry, A., Sun, R. F., & Turner, J. (2021). *Quantum computing for the quantum curious*. Springer.

Illiano, J., Caleffi, M., Manzalini, A., & Cacciapuoti, A. S. (2022). Quantum internet protocol stack: A comprehensive study. *Computer Networks* (231). https://doi.org/10.1016/j.comnet.2022.109092

Inglesant, P., Jirotka, M., & Hartswood, M. (2018). *Responsible innovation in quantum technologies applied to defence and national security*. Networked Quantum Information Technologies. https://nqit.ox.ac.uk/index.php/content/responsible-innovation-defence-briefing-note.html

Jaeger, L. (2018). *The second quantum revolution*. Springer.

Jeutner, V. (2021). The quantum imperative: Addressing the legal dimension of quantum computers. *Morals + machines* 1.

Kleinberg, J., Mullainathan, S., & Raghavan, M. (2016). *Inherent trade-offs in the fair determination of risk scores*. arXiv. https://arxiv.org/abs/1609.05807

Kop, M., & Hiscott, L. (2021). Ethics in the quantum age. *Physics World, 34*(12), 31.

Kop, M. (2022). Quantum computing and intellectual property law. *Berkeley Technology Law Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3860456

Krelina, M. (2021). Quantum technologies for military applications. *arXiv* 2103 12548.

Lele, A. (2021). *Quantum technologies and military strategy*. Springer.

Lloyd, S. (1996). Universal quantum simulators. *Science, 273*(5278), 1073–1078.

Maudlin, T. (2019). *Philosophy of physics: Quantum theory.* Princeton University Press.

McAfee, A., Saltiel, N., Rahwan, I., & Dinakar, K. (2016). Society in the loop artificial intelligence. https://joi.ito.com/weblog/2016/06/23/society-in-the-.html

McKay, E. (2022). *Keep the fight unfair: Military rhetoric in quantum technology*. arXiv. https://arxiv.org/abs/2203.01415

McNamara, D., Graham, T., Broad, E., & Ong, C. S. (2019). Trade-offs in Algorithmic risk assessment: An Australian domestic violence case study. In A. Daly, S. K. Devitt, & M. Mann (Eds.), *Good data* (pp. 96–116). Institute of Network Cultures.

Medvechy, F., & Leach, L. (2019). *An ethics of science communication*. Palgrave Macmillan.

Neumann, N., van Heesch, M., & De Graaf, P. (2020). *Quantum communication for military applications*. arXiv. https://arxiv.org/abs/2011.04989

Nielsen, M., & Chuang, I. (2011). *Quantum computation and quantum information*. Cambridge University Press.

O'Keefe, K., & O'Brien, D. (2018). *Ethical data and information management*. KoganPage.

Olson, J., Cao, Y., Romero, J., Johnson, P., Dallaire-Demers, P., Sawaya, N., Narang, P., Kivlichan, I., Wasielewski, M., & Aspuru-Guzik, A. (2017). Quantum information and computation for chemistry. *arXiv* 1706.05413.

Paperin, G. (2007). Security of communication and quantum technology. In: *Encyclopedia of Information Ethics and Security* (pp. 602–608). IGI Global.

Parker, E. (2021). *An assessment of the U.S. and Chinese industrial bases in quantum technology*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA869-1.html

Parker, E. (2022). *Commercial and military applications and timelines for quantum technologies*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1482-4.html

Perrier, E. (2021). Quantum fair machine learning. *arXiv*, arXiv 2102.00753.

Perrier, E. (2022). Ethical quantum computing: A roadmap. *arXiv*, arXiv:2102.00759.

Rawls, J. (1993). *Political liberalism*. Columbia University Press.

Rawls, J. (2001). *Justice as Fairness. A Restatement*. The Belknap Press of Harvard University Press.

Rip, A. (2018). *Futures of science and technology in society*. Springer.

Rodhe, P. (2021). *The quantum internet. The second quantum revolution*. Cambridge University Press.

Rubel, A., Castro, C., & Pham, A. (2019). Agency laundering and information technologies. *Ethical Theory and Moral Practice, 22*(4), 1017–1041. https://doi.org/10.1007/s10677-019-10030-w

Sangouard, N., Simon, C., Minář, J., Zbinden, H., De Riedmatten, H., & Gisin, N. (2007). Long-distance entanglement distribution with single-photon sources. *Physical Review A, 76*, 050301(R). https://journals.aps.org/pra/abstract/10.1103/PhysRevA.76.050301

Simon, D. R. (1997). On the power of quantum computation. *SIAM Journal on Computing, 26*(5), 1474–1483.

Smith, F. (2020). Quantum technology hype and national security. *Security and Dialogue, 51*(5), 499–516.

Susskind, L., & Friedman, A. (2014). *Quantum mechanics: The theoretical minimum*. Penguin.

Taebi, B. (2021). *Ethics and engineering*. Cambridge University Press.

Tsamados, A., Aggarwal, N., & Cowls, J. (2022). The ethics of algorithms: Key problems and solutions. *AI & Society, 37*, 215–230.

Van de Poel, I., & Royakkers, L. (2011). *Ethics, technology, and engineering*. Wiley-Blackwell.

Vermaas, P. E. (1999). *A philosopher's understanding of quantum mechanics*. Cambridge University Press.

Vermaas, P. E. (2017). The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable. *Ethics and Information Technology, 19*, 241–246.

Watene, K., & Drydyk, J. (Eds.). (2016). *Theorizing justice: Critical insights and future directions*. Rowman and Littlefield.

Weiss, D. S., & Saffman, M. (2017). Quantum computing with neutral atoms. *Physics Today, 70*(7), 44.

Wolbring, G. (2022). Auditing the social of quantum technologies A scoping review. *Societies, 12*, 41.

Wolf, S. (2019). *Overview of the status of quantum science and technology and recommendations*. Institute for Defense Analysis Document D-10709.

Zhu, H., Bowen, Y., Halfaker, A., & Terveen, L. (2018). Value-sensitive algorithm design: Method, case study, and lessons. *Proceedings of the ACM on Human-Computer Interaction, 21*(194), 1–23.

Zliobaite, I. (2017). Measuring discrimination in algorithmic decision making. *Data Mining and Knowledge Discovery, 31*(4), 1060–1089.

Zygelman, B. (2018). *A first introduction to quantum computing and information*. Dordrecht: Springer.