Digital Society (2022) 1:12
https://doi.org/10.1007/s44206-022-00012-4

ORIGINAL PAPER

Quantum Computing, Digital Constitutionalism, and the Right to Encryption: Perspectives from Brazil

Miriam Wimmer[1] · Thiago Guimarães Moraes[2]

Received: 15 February 2022 / Accepted: 14 July 2022 / Published online: 12 August 2022

Abstract

This article examines how the debates on a right to encryption, understood within the framework of digital constitutionalism, may be impacted by the development of quantum computing. An important question is how to ensure that fundamental rights and freedoms in the digital environment are adequately preserved, especially considering that the development of quantum capabilities is likely to occur in a disparate manner between developed and developing countries. For this reason, the article brings as an example the case of Brazil, a country that has a significant history of discussing digital rights and in which the issue of encryption is currently in debate before the Supreme Court. The paper is structured in three main parts, beginning with an overview of the discussions on the idea of a right to encryption within digital constitutionalism initiatives, particularly in Brazil. Next, the article examines how the development of quantum technologies may impact encryption, analyzing both technical and geopolitical repercussions of the race for quantum supremacy. Finally, it assesses the potential impacts of quantum computing on the enjoyment of fundamental rights in the digital environment and examines three different approaches: the development of post-quantum cryptography standards, the adjustment of domestic policies and further development of flexible legal and regulatory strategies, and global cooperation through binding and non-binding legal instruments. To conclude, the paper assesses the specific challenges faced by developing countries, such as Brazil, in connecting the debate on fundamental rights with the new technical and legal issues raised by emerging technologies.

Keywords Digital constitutionalism · Privacy · Security · Right to encryption · Quantum computing · Brazil

✉ Miriam Wimmer
miriam.wimmer@idp.edu.br; miriam.wimmer@yahoo.com.br

Thiago Guimarães Moraes
thiago@lapin.org.br

[1] Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP, Brasília, Brazil

[2] Laboratório de Políticas Públicas e Internet – LAPIN, Brasília, Brazil

1 Introduction

The global debate on the protection of online rights has increasingly been framed under a broader discussion of "digital constitutionalism." While there is still no universally agreed definition for this concept, it is frequently used to connect different initiatives that seek to articulate a set of political rights, governance norms, and limitations on the exercise of power on the Internet (Gill et al., 2015). One of the core themes discussed within the framework of digital constitutionalism is the use of *encryption technologies* (Yilma, 2017), often centered around the tension between the needs of law enforcement and national security agencies, on one hand, and the rights to privacy, personal data protection, and confidentiality of communications on the other.

Against this backdrop of legal discussions, we aim to examine how the debates on encryption, understood within the framework of digital constitutionalism, may be impacted by the development of *quantum computing*. It is already clear that quantum innovations may, in the future, revolutionize computing, with positive impacts on fields such as finance, drug development, defense, and health care. However, quantum computing will also severely affect some of the currently most used encryption techniques, in particular asymmetric cryptography schemes, with important consequences for data protection regulatory frameworks and digital rights. In this context, an important question is how to ensure that democratic principles and human rights and freedoms are adequately preserved. While there is ongoing research on the development of post-quantum cryptography, it is important to note that the development of quantum capabilities is likely to occur in a disparate manner between developed and developing countries.

The discussion on cryptography, fundamental rights, and quantum computing has different implications for nations who currently lead the quantum race, on one hand, and for countries of the global South, on the other. For this reason, this paper focuses on the case of Brazil, a country with an important history of discussing digital rights, as demonstrated by the pioneering Marco Civil da Internet (MCI), a civil-rights framework for the Internet enacted in 2014, and by the approval of a comprehensive data protection law, in 2018. The issue of encryption has raised heated debates and constitutional challenges in the country, and while the dispute is still far from settled, it is important to note that in concrete cases placed before the Brazilian Supreme Court, still pending final decisions, two Justices have already issued opinions connecting the use of encryption to the enjoyment of fundamental rights.

This paper does not attempt to cover all aspects of this complex discussion, but to present a preliminary assessment of the issue and to call attention to new questions for further studies, connecting legal research with computer science. The paper is structured in three main parts, beginning with an overview of how the idea of a right to encryption has been discussed within the context of digital constitutionalism initiatives, particularly in Brazil. Next, the article discusses how the development of quantum technologies may impact encryption, examining both technical and geopolitical repercussions of the race for quantum supremacy, herein understood as a milestone that will be reached when a universal quantum computer performs a computational task that is beyond the capability of any classical computer (Harrow & Montanaro, 2017). Finally, building on that analysis, the article assesses the potential impacts of quantum computing on the enjoyment of fundamental rights in the digital environment and explores three different approaches to deal with the challenges it poses: (i) the development of post-quantum cryptography standards; (ii) the adjustment of domestic policies and further development of flexible legal and regulatory strategies; and (iii) global cooperation through binding and non-binding legal instruments. To conclude, the paper assesses the specific challenges faced by developing countries in connecting the debate on fundamental rights with the new technical and legal issues raised by emerging technologies.

2 Digital Constitutionalism and a Right to Encryption

In this section, we aim to briefly examine how the claims for recognition of a right to encryption have been framed within the broader discussions on digital constitutionalism. To this end, we begin by exploring the global debates on this issue and then analyze in more detail the discussions currently underway in Brazil.

2.1 Digital Constitutionalism as a Framework to Limit Powers in the Digital Environment

The term "digital constitutionalism" has been used in connection with several initiatives, normative responses, or constitutional counteractions that seek to address the disruptive impacts of digital technologies (Celeste, 2019). Digital constitutionalism, therefore, can be described as a growing field within constitutional thinking that seeks to build a normative framework to promote the recognition, affirmation, and protection of fundamental rights in cyberspace (Mendes & Fernandes, 2020). Despite the interest that this idea has raised in legal doctrine, it is important to recognize that there is still no clear agreement on its scope and on the instruments that could promote its materialization. This terminology has often been used with contrasting meanings, and there are important differences between the initiatives that have been placed under its umbrella, ranging from mere advocacy statements to actual or proposed legislation, in the form of Internet Bills of Rights (Gill et al., 2015).

Although the concept of digital constitutionalism remains disputed and while the legislative initiatives related to Internet Bills of Rights can still be described as fragmented and piecemeal (Yilma, 2017), some key issues are present in most discussions on the issue. In general, it is possible to note a common concern related to establishing limits on the exercise of power in the digital environment. While some scholars place more emphasis on the limitation of power exercised by States (Gill et al., 2015), others point to the risks of the power exerted by private organizations, particularly online platforms (Gregorio, 2022; Suzor, 2018). In fact, as the architecture of power becomes more complex in an algorithmic society, the focus of constitutional law expands from the vertical relationship between citizens and the State towards the horizontal relationship between individuals and private organizations. This is particularly relevant in view of the widening role that non-governmental and business actors play in establishing rules and exercising functions traditionally attributed to public authorities, with limited public oversight and safeguards.

An important aspect of the current discussion on *digital* constitutionalism is its connection to the ongoing debates on *global* constitutionalism. Several authors have argued that social, economic, and political processes that place power beyond the nation-state, such as globalization and privatization, are progressively eroding central concepts of traditional constitutionalism, such as statehood and the modes of legitimation of public power (Dobner & Loughlin, 2010). One of the main challenges for contemporary constitutional theory is, therefore, the expansion of the values of constitutionalism into transnational regimes and into the private sectors of global society (Teubner, 2012).

These challenges are particularly relevant when considering the digital environment, where transnational private actors and international organizations take on increasingly broad functions in complementing or even replacing the traditional law-making activities carried out by domestic governmental institutions. For this reason, the discussions on digital constitutionalism often seek to consider the relationship and the tensions between an internal dimension of constitutionalism, driven by regional and local constitutional traditions and values connected to certain communities and territorial boundaries, and the external dimension of constitutionalism, recognizing the existence of a polycentric form of globalization beyond the traditional boundaries of political and legal constitutionalism (Gregorio, 2022).

In this sense, the framework of digital constitutionalism is particularly useful not only to discuss fundamental rights that quantum computing may affect—such as rights to privacy, security, and encryption—but also to shed light on the complex interplay between binding and non-binding, public and private, and domestic and transnational frameworks that may be developed to address these issues.

2.2 Digital Constitutionalism and the Right to Encryption

Initiatives that are described as exercises in digital constitutionalism frequently seek to promote the recognition of rights and freedoms in the digital arena, either through the reinterpretation and extension of traditional human rights, such as freedom of expression, freedom of association, and privacy, or through the identification and proposal of new rights that appear to be innate to the digital environment, such as a right to Internet access and net neutrality. It is still open to discussion if initiatives within digital constitutionalism should actually strive to identify completely new rights, or if such new rights are merely the result of reconsidering and adapting existing rights, taking into account the particularities of cyberspace (Yilma, 2017).

Rights connected to online security and privacy are an important part of the digital constitutionalism landscape. However, privacy and security are not experienced online in the same way as they are offline, and changes in certain inarticulate contextual conditions (Casacuberta & Senges, 2008) may require the identification of subsets of traditional rights that arguably serve to adapt traditional rights to online contexts. The debate on the existence of a right to encryption is an important part of discussions on Internet Bills of Rights and can be placed within this context.

Proponents of a right to encryption often discuss this idea in connection with other privacy-related rights, such as the right to protection from surveillance and the right to anonymous communication. There is currently widespread recognition that the right to privacy in the digital age relies strongly on the use of privacy-enhancing technologies, including encryption. For this reason, while still falling short of recognizing a right to encryption, several legal documents issued by organizations within the United Nations Organization (UNESCO, 2016; UNHCR, 2019, 2020) and by the OECD (1997) already mention encryption as a technology that may be instrumental towards the enjoyment of human rights, particularly privacy, freedom of expression, and freedom of assembly.

A recent example can be found in a United Nations Human Rights Council—UNHCR Resolution adopted in October 2020 on the safety of journalists that calls upon States to "…refrain from interference with the use of technologies such as encryption and anonymity tools, and from employing unlawful or arbitrary surveillance techniques, including through hacking" (UNHCR, 2020). Similar wording was also employed in the 2019 UN Resolution adopted by the Human Rights Council on the right to privacy in the digital age (UNHCR, 2019).

The 2015 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression also argues that restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality, and legitimacy, since they provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age (Kaye, 2015). Aligned with this opinion, 1 year later UNESCO published a report on human rights and encryption, in which it recognized that cryptographic methods are of particular relevance to the rights to freedom of expression and to a private life (UNESCO, 2016).

Finally, it should be mentioned that as early as 1997, the OECD adopted Guidelines for Cryptography Policy, aiming to promote the use of cryptography to foster confidence in the use of digital technologies without unduly jeopardizing public safety, law enforcement, and national security (OECD, 1997). It is interesting to note that the OECD Recommendation contains several references connecting cryptography to individual rights. The principle of "Choice of Cryptographic Methods," for instance, states that "users should have a right to choose any cryptographic method, subject to applicable law," while the principle of "Protection of Privacy and Personal Data" asserts that "the fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods."

It is still open to debate if it is necessary or useful to speak of an autonomous right to encryption, or if existing rights, such as the right to privacy and personal data protection, could afford adequate legal protections against undue interferences with the ability to deploy and enjoy the benefits of encryption. In any case, it is clear that this issue has gained prominence in domestic and international debates related to the exercise of fundamental rights.

Debates on encryption have, however, often become complex and highly contentious, polarized between privacy and law enforcement interests. On one side, the well-known “going dark” metaphor calls attention to the phenomenon in which law enforcement personnel has the legal authority to intercept and access communications and information under court orders but often lacks the technical ability to do so, due to the increased adoption of end-to-end encryption and other similar technologies (Moraes, 2020). On the other side, criticism has emerged, underlining that the “going dark” argument does not adequately reflect the complexity of the debate and the range of options available to law enforcement agencies (Walden, 2018). An alternative narrative, endorsed by a 2016 Report from an Encryption Working Group established in 2016 by the US House Judiciary Committee and House Energy and Commerce Committee, proposes the idea that the challenge for the intelligence community appears to be more akin to “going spotty” since the law enforcement and intelligence community is generally well-equipped to work around the challenges posed by the widespread adoption of encryption technologies (U.S. House Judiciary Committee and House Energy and Commerce Committee, 2016). A similar argument has been put forward by the Harvard Berkman Center for Internet and Society (2016), concluding that “communications in the future will neither be eclipsed into darkness nor illuminated without shadow.” According to the Report, “the trajectory of technological development points to a future abundant in unencrypted data, some of which can fill gaps left by the very communication channels law enforcement fears will ‘go dark’ and beyond reach.”

While the debate is far from resolved, it also seems clear that framing the discussion under a binary perspective, in the form of a trade-off between security and privacy (Solove, 2011), fails to capture several aspects that may merit more attention, such as the varied meanings that privacy and security may assume in different contexts, and the complex discussions on sovereignty and jurisdiction that emerge when national law enforcement bodies seek access to encrypted evidence held by global internet platforms.

2.3 The Case of Brazil

The discussions on encryption in Brazil to a certain extent mirror those held elsewhere on “going dark.” However, the scenario in Brazil is somewhat different because domestic debates are strongly influenced not only by the constitutional protections afforded to privacy and personal data but also by the existence of a formal and binding legal framework that establishes principles and rights for the use of the Internet in Brazil—the Marco Civil da Internet.

The Marco Civil da Internet (MCI) was approved in 2014, after lengthy consultations involving stakeholders from civil society, academia, the business community, and government, and has been internationally hailed as an example of digital constitutionalism. According to Moncau and Arguelhes (2020), the law effectively shifted the balance of power between private and state actors, by creating safeguards against intrusion on private communications by both law enforcement authorities and internet access providers. Although the Brazilian constitution already included many of the principles emphasized by the MCI, such as privacy, freedom of expression, freedom to associate, and non-discrimination, the new law translated these principles to the digital environment, bringing greater legal certainty concerning issues such as online content removal, net neutrality, data retention, ISP liability, and lawful access to metadata and private communications (Medeiros & Bygrave, 2015).

Although Marco Civil does not explicitly mention encryption, it provides rules on the secrecy of Internet-based communications, grounded on the Constitutional provision that affirms the inviolability of the secrecy of correspondence, of telegraphic communications, data, and telephone communications. In this sense, MCI states that both stored communications and communications in transit are protected and that a court order is required for investigative bodies to have access to such communications.[1]

The discussions on encryption in Brazil are currently centered around two major cases, still pending decisions by the Brazilian Supreme Court.[2] Both involve the revision of decisions issued by lower courts between 2015 and 2016 demanding the nationwide suspension of WhatsApp operations, due to non-compliance with court orders requiring the provision of digital evidence. In both cases, the discussion revolved around the proportionality of the court decisions, since the company claimed it was unable to comply with the lawful court orders to decrypt the content of messages sent using end-to-end encryption.

It is important to note that at the time that the constitutional challenges were presented, Brazil did not yet have a comprehensive data protection law. The Brazilian General Data Protection Law was approved in 2018 and entered into force in 2020, after lengthy discussions both within the government and in the National Congress. In 2021, in the wake of a 2020 Supreme Court decision recognizing the existence of a fundamental right to data protection based on informational self-determination, a constitutional amendment was approved, formally establishing a fundamental right to data protection, which can be understood as distinct and broader than the right to privacy which was already enshrined in the Federal Constitution.

As noted by Silva et al. (2021), it is clear that the new data protection legislation reshaped the debate on encryption even before entering into force, in September 2020. In fact, after a public hearing held in 2017, the Justices rapporteurs Edson Fachin and Rosa Weber issued their votes in May 2020, clearly stating that encryption is a means to ensure the protection of rights that are essential to a democratic society. Their votes also made express references to the Federal Constitution, the

[1] These provisions can be found in Article 7, items II and III of MCI: “Art. 7. Access to the internet is essential to the exercise of citizenship, and the following rights are guaranteed to the users:

II—inviolability and secrecy of the flow of users’ communications through the Internet, except by court order, as provided by law;

[2] The cases under discussion are *Ação Direta de Inconstitucionalidade 5527*, which challenges the constitutionality of certain provisions of *Marco Civil da Internet* that have been used by lower courts as grounds for blocking WhatsApp in the country, and *Arguição de Descumprimento de Preceito Fundamental 403*, which claims that WhatsApp blocks violate fundamental rights to communication and information.

MCI, and the new general data protection law, thereby placing data protection as a central pillar and building upon the country's history of protecting digital rights. The vote of Justice Edson Fachin is particularly clear in connecting the case to discussions also held under the framework of digital constitutionalism, as he states several assumptions that guide his reasoning on the case under examination:

> First: the technological impact of the changes that society is undergoing demands a permanent updating of the scope of fundamental rights and guarantees.
> Second, the rights that people have offline must also be protected online. Digital rights are fundamental rights.
> Third: the guarantee of the right to privacy and freedom of expression in communications is a condition for the full exercise of the right of access to the Internet.
> Fourth: privacy is the right to maintain control over one's own information and to determine the way to build one's own public sphere.
> Fifth: freedom of expression has prima facie primacy and constitutes an essential condition for the pluralism of ideas, a structuring vector of the democratic system of law.
> Sixth: on the Internet, encryption and anonymity are especially useful for developing and sharing opinions, which often takes place through online communications such as email, text messages, and other interactions. Cryptography, in particular, is a means of ensuring the protection of rights that, in a democratic society, are essential to public life.
> Seventh: it is contradictory that, in the name of public safety, it should be impossible to promote and seek a safer internet. A safer internet is everyone's right and the State's duty. Measures that, in the light of the best scientific evidence, make users insecure are only justified if there is certainty comparable to the gains obtained in other areas. (Brazil, 2020)

The examination of both cases was suspended at the request of justice Alexandre de Moraes. It is therefore not yet clear if the perspectives introduced by the rapporteurs will be maintained in the Supreme Court's final decision.

3 How Quantum Computing Affects Encryption: Technical and Geopolitical Aspects

As discussed in the previous section, the importance of cryptography has been extensively acknowledged, both as a technical tool for information security and a legal instrument for the protection of fundamental rights. However, technologies that may directly impact cryptography, in its current state of the art, continue to be rapidly developed. One of such technologies, which is the main focus of this paper, is quantum computing.

3.1 Quantum Computing and Encryption

Quantum computers are computers that process information based on the physical laws of quantum mechanics (European Data Protection Supervisor – EDPS, 2021). Instead of the traditional bit, a binary value which may be either 0 or 1, quantum computing employs quantum bits or qubits. A qubit is a two-state quantum system, which may simultaneously assume two independent states $|0\rangle$ and $|1\rangle$ based on a principle called superposition (Rieffel & Polak, 2011, p. 14). While the physics of quantum mechanics is beyond the scope of this paper, it is important to know that since quantum computers may carry out operations not only for a determined value $|0\rangle$ or $|1\rangle$ but also for all possible superpositions at the same time, they have better performance than binary computers for certain tasks (EDPS, 2021).

One of the mathematical operations in which quantum computers excel is the prime factorization of large numbers. The factorization problem is the basis for one of the most important public-key schemes currently used, known as RSA. This is due to a quantum computer algorithm known as Shor's algorithm, named after its author. In 1994, mathematician Peter Shor proved that factoring large integers could be reduced to a polynomial-time problem, with the use of quantum computing (Mavroeidis et al., 2018, p. 3). In short, this means that while a traditional computer could take days to solve the prime factorization of a large number, a quantum computer would take only minutes. According to a 2019 study, a 20 million qubits computer could crack a 2048-bit RSA system (the current state of the art for this cryptographic scheme) within 8 h (Gidney & Ekerå, 2021).

Shor's algorithm can also steadily solve the discrete logarithm problem faster. This problem is the basis for other important asymmetric cryptographic systems: Diffie-Hellman – DH and Elliptic Curve Cryptography – ECC (Mavroeidis et al., 2018, p. 2). Many Internet protocols use DH or ECC protocols,[3] which means that in practice, almost any digital system that processes encrypted information, such as texts, emails, credit card payment information, digital signatures, online transactions, sensitive data, and intelligence in government classified secrets, may be at risk (NIST, 2021). This scenario could potentially produce impacts not only on information security but also on online rights and freedoms related to privacy and freedom of expression.

It is important to note that in the short term, quantum computing may not be a real issue: most implementations are still at the laboratory level and do not present

[3] These include, but are not limited to: (i) Hyper Text Transfer Protocol Secure (HTTPS)/Transport Layer Security (TLS)/Secure Sockets Layer (SSL), the current protocols for providing layers of security on web browsing; (ii) Public-Key Infrastructure (PKI), which supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party; and (iii) P Security (IPSec), an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality ("Applications and Limitations of Diffie-Hellman algorithm – GeeksforGeeks", 2020). Other examples of these cryptographic systems implementations are Microsoft developer's platform, Microsoft Azure (Benari, 2014); WhatsApp's end-to-end encryption protocol (WhatsApp, 2020); and Bitcoin's authentication algorithm ("Elliptic Curve Digital Signature Algorithm – Bitcoin Wiki", 2021).

an immediate threat to deployed applications. By 2019, the most powerful quantum machine could operate only 128 qubits (Giles, 2019)—as mentioned before, a quantum computer would need to operate millions of qubits to crack state-of-the-art RSA algorithms. McKinsey estimates that by 2030 only 2000 to 5000 quantum computers will be operational (Ménard et al., 2020). Nevertheless, hybrid approaches in which parts of the problem would be handled by classical computing and parts by quantum may already be adopted by many industries, between 2022 and 2026. If and how these adoptions will have a direct impact on cybersecurity may still be not clear, but it raises an alert that some preparation for this scenario is necessary.

3.2 Geopolitical Aspects of the Adoption of Quantum Computing

The discussion on the impacts of quantum computing on encryption, cybersecurity, and the right to privacy is further complicated by the complex geopolitical dynamics surrounding the development of the technology. Kop argues that among the ten most pressing societal risks related to quantum technology identified to date is the possibility of distorted geopolitical relations, quantum arms races, cyber warfare, and altered power constellations (Kop, 2021, p. 9). In this sense, it is important to consider the likelihood that countries and regions that are already leading the way in quantum research may jump ahead in the adoption of the technology, while countries in other regions, such as Latin America and Africa, lag behind.

This disparity will probably exist not only in the field of cybersecurity but also in the context of "cyberattack power" (i.e., the ability to exploit cybersecurity vulnerabilities) since only a few countries are currently heavily investing in quantum computing: besides the USA, the EU, and Japan, other important players in quantum computing development are China and Russia (Rota, 2018).

Similar to cryptography, quantum computing is considered a dual-use technology, with both civilian and military applications (Rand & Rand, 2021, p. 16; Mancuso & Rapa, 2020). In many countries, technologies such as these may be subject to export control regimes. In the USA, while rules on controlling the exportation of dual-use technologies are commonplace, the Executive Branch's authority to regulate and enforce export controls has expanded, as a result of the Export Control Reform Act – ECRA, enacted in 2018 (Rand & Rand, 2021, p. 19). In the same year, the Bureau of Industry and Security – BIS issued an advanced notice of proposed rulemaking, identifying, at a high level, the types of emerging technologies that could eventually become subject to the mandatory ECRA controls. Not surprisingly, quantum-related technologies were included in the list. In November 2020, BIS received several comments on the list from industry and academia but has published nothing further, according to a June 2021 report from the US-China Economic and Security Review Commission (U.S-China Economic and Security Review Commission, 2021, p. 4).

According to Laurie Clarke, the race for quantum supremacy is not limited to the USA and China. In March 2021, the European Union announced that Israel, Switzerland, and the UK would no longer be able to participate in the EU's flagship Horizon Europe science program in areas that could prove sensitive to national security, including quantum computing (Clarke, 2021). The same author notes that the UK, on the other hand, has placed export controls on a range of strategic military and dual-use items, which include several quantum technologies that now must be approved before being sent abroad. Scientists can even be imprisoned if they disclose an invention without approval. The national security concerns are not unfounded, since there is a high possibility that cyber warfare may increase in the next few years (Rota, 2018). This problem may be exacerbated by the fact that there are still no clear definitions of the concepts of cyberattacks, cyberterrorism, and cyberwarfare, nor agreed-on rules to deal with such issues.

It is worth noting, however, that the concept of quantum supremacy should be used with caution: there are currently few ways to mathematically prove that a specific quantum algorithm is superior to any possible algorithm on a classical computer, such as Shor's prime factorization algorithm and methods of physics simulation. For most other applications of quantum computers, there is only some evidence that the quantum algorithm is more efficient than all known classical algorithms (OECD, 2020). According to the OECD, three milestones must be reached to advance the potential of quantum computers: first, demonstration that they can perform better in solving problems, compared to classical computers; second, achievement of commercial success, by demonstrating a quantum advantage for a task that has a practical purpose; and, finally, successful error correction for limited quantum devices. All things considered, the OECD argues that while a definite proof of quantum supremacy may require stronger evidence, it seems within reach.

In this context, the race for quantum supremacy may create a scenario where countries and organizations with mastery of quantum computing and post-quantum cryptography technologies will have a huge advantage over those who do not have access to such technologies. In this race, the ones that lag behind may have serious cybersecurity issues that will directly affect their whole infrastructure[4] and ultimately impact the enjoyment of fundamental rights and freedoms.

4 The Right to Encryption in a Post-Quantum World: Three Approaches

While it is still too soon to foresee how the debate on encryption will evolve in Brazil and elsewhere, there is no question that the development of quantum computing will produce serious repercussions.

Current discussions on a right to encryption occur in a context where end-to-end encryption is readily available to individuals and organizations—in other words,

[4] As an example, since the year 2000, the digital certification scheme in Brazil has been running under an IKE framework known as ICP-Brasil ("ICP-Brasil," 2017). It has a very large and complex ecosystem, composed of certificate and register authorities, including banks, public institutions, and universities, among others. With the digital transformation of public services, the importance of ICP-Brasil is continuously increasing. However, the cost of adapting the current IKE framework to quantum-resistant technologies may be considerable, and the lack of timely adaptation may increase its vulnerability to cyberattacks. This is a problem that may be faced both by public and private organizations, especially in developing countries.

it has become relatively easy to encrypt communications, and, conversely, it has become increasingly difficult for law enforcement and intelligence agencies to gather critical information. While there has been a public backlash against proposals of government-mandated backdoors or of prohibition of end-to-end encryption, other surveillance structures may be developed to avoid the "going dark" scenario. On the other hand, the development of quantum computing may raise difficult ethical questions, as the current balance between privacy and justified surveillance for security purposes will shift if the set of available cryptographic tools changes (de Wolf, 2017).

In the medium term, the development of quantum computing may also produce important rearrangements in existing power structures, accentuating geopolitical struggles and increasing imbalances, at the domestic level, between individuals, public authorities, and private actors (Bay, 2017). At least for some time, it is possible that some actors, such as large organizations and governments of countries that currently lead the quantum race, will have access to quantum technology, while others will not. As noted by de Wolf (2017), such a situation could not only upset the balance of power between different countries, but it could also lead to monopolies or oligopolies, increasing inequality in society.

These circumstances may also produce important effects for fundamental rights. As discussed previously, the scholarship and the legal documents built under the umbrella of digital constitutionalism share a concern on imbalanced power relations, involving not only nation-states but also private transnational corporations. They also highlight that the protection of traditional fundamental rights, such as privacy and personal data protection, may lead to the recognition of new rights, or subsets of traditional rights, that are native to the digital environment, including the right to use privacy-enhancing technologies such as encryption to protect private communications. In this sense, if nothing changes, it is possible to conceive a future scenario in which the development of quantum computing and the unequal access to secure communications could affect the existing power balance and seriously jeopardize such rights.

This important challenge to the right to privacy in the digital environment requires the consideration of different legal and policy approaches to promote equitable access to the benefits that can be created by quantum computing, limiting the capacity of States and businesses to misuse the technology and taking into account societal and group interests.

Three different approaches will be briefly discussed: (a) standardization of post-quantum cryptography; (ii) adjustment of domestic policies and further development of flexible legal and regulatory strategies related to privacy and personal data protection; and (iii) global cooperation through binding and non-binding legal instruments.

4.1 Standardization of Post-Quantum Cryptography

One approach that has been proposed to address the challenges placed by quantum computing is the development of quantum-resistant cryptography, also known as post-quantum cryptography (PQC). This is an active area of research, with its own conference series, PQCrypto, which started in 2006, and has received support from national funding agencies in Europe, Japan, and the USA, among others (NIST, 2016a, p. 7).

Mauritz Kop suggests that standardization may be a good approach to foment research and innovation on PQC (Kop, 2020, p. 18). One of the most important initiatives in this field is the one proposed by the US National Institute of Standards and Technology—NIST, which seeks to promote the development of cryptographic systems that are secure against both quantum and conventional computers and can interoperate with existing communication protocols and networks (NIST, 2016a, p. 4).

To develop its PQC standards, NIST has taken a competition-like approach, consisting of a call for submissions and several rounds of institutional and public scrutiny ("Post-Quantum Cryptography," 2017). The institute has specified a set of evaluation criteria for quantum-resistant public-key cryptography standards: (i) security; (ii) (computational) cost and performance; and (iii) algorithm and implementation characteristics (NIST, 2016b).

Security is the most important factor to be considered and is itself composed of its own factors. In short, proposed schemes are to be evaluated by the security they provide to a wide variety of Internet protocols[5] (NIST, 2016b, p. 14), as well as to Key Encapsulation Mechanisms (KEM),[6] and/or digital signatures. Considering the uncertainties related to the development of new quantum algorithms and the limited ability to predict the performance of future quantum computers (such as their cost, speed, and memory size), five security strength categories were established and listed in order of increasing strength. While the first three categories are the most important targets for NIST's evaluation, the institution has been encouraging submitters to provide at least one parameter set that meets the highest level of security strength. According to the second round report, most of the candidate algorithms have already done this (NIST, 2020, p. 12). Additionally, NIST suggested that several other properties would be desirable: (i) perfect forward secrecy[7]; (ii) resistance to side-channel attacks[8]; (iii) resistance to multi-key attacks[9]; and resistance to misuse.

[5] These include TLS, SSH, IKE, and IPsec.

[6] A KEM is a cryptographic primitive that allows anyone in possession of some party's public key to securely transmit a key to that party. A KEM can be viewed as a key-exchange protocol in which only a single message is transmitted; the main application is in combination with symmetric encryption to achieve public-key encryption of messages of arbitrary length. See Coretti et al. (2013).

[7] The term perfect forward secrecy is commonly used to denote a feature of key agreement protocols which gives assurances that past session keys will not be compromised even if the private key of the server is compromised. One example of a protocol that supposedly implements this feature is the WhatsApp end-to-end encryption mechanism. See WhatsApp (2020).

[8] Side-channel attacks gain information about the targeted cryptosystem by observing its physical processes, such as the processor's running time, electromagnetic emissions, and cryptographic hardware's power consumption. See Pfefferkorn (2017).

[9] According to NIST, "ideally an attacker should not gain an advantage by attacking multiple keys at once, whether the attacker's goal is to compromise a single key pair, or to compromise a large number of keys." See NIST (2016b, p. 19).

Computational cost is the second main factor to be considered, including computational efficiency, speed of the algorithm, memory requirements, code size, and random-access memory (RAM) requirements for software implementations, as well as gate counts for hardware implementations (NIST, 2016b, p. 20). This is an important factor since it is not enough for an algorithm to be secure, but it also needs to be able to perform well in different environments, such as computationally constrained devices (e.g., smartcards), servers dealing with a high volume of traffic, and KEM schemes used to provide perfect forward secrecy.

Finally, other algorithmic and implementation characteristics are being considered, including flexibility, design simplicity, and adoption. This last characteristic considers factors that might hinder or promote widespread adoption, including, but not limited to, intellectual property covering an algorithm or implementation and the availability and terms of licenses to interested parties (NIST, 2016b, p. 21). NIST has declared that it has a clear preference for simple and elegant designs and royalty-free algorithms to enable widespread adoption (NIST, 2020, p. 14).

While the standardization procedure is still ongoing, it seems to be reaching its final steps. In November 2017, eighty-two candidate algorithms were submitted to NIST for consideration. Currently, in its third round, only seven finalists are left, as well as eight alternate candidates (NIST, 2020, p. 15). The set of finalists is algorithms that NIST considers to be the most promising to fit the majority of use cases and most likely to be ready for standardization soon after the end of the third round. Meanwhile, the alternate candidates are regarded as potential candidates for future standardization, most likely after another round of evaluation. The report of the third round is expected to be published by early 2022 (NIST, 2020, p. 33).

Although the development of NIST standards is a US-led initiative and their adoption is not mandatory, they have ramifications at the international level, especially regarding cybersecurity (NIST, 2018). In Brazil, for example, NIST documents have inspired domestic approaches towards privacy and cybersecurity, and the National Cybersecurity Strategy, approved by Decree n. 10.222 of 2020, recommends the observance of NIST standards when appropriate, in addition to the formal rules issued by the Institutional Security Cabinet of the Presidency of the Republic. Therefore, it is very likely that initiatives such as PQC standardization will also have an impact on domestic approaches towards privacy and personal data protection in several jurisdictions.

4.2 Adjustment of Domestic Policies and Further Development of Flexible Legal and Regulatory Strategies

A second approach refers to the potential need for reassessment of domestic legal frameworks, in particular those related to privacy, security, and personal data protection, to cushion the impact of quantum computing (Bruno & Spano, 2021).

Although there is still no widespread recognition of a fundamental right to encryption, as proposed by different initiatives under the auspices of digital constitutionalism, regulation and laws increasingly point to encryption as an important tool to protect personal information online. The European General Data Protection

Regulation (GDPR), for instance, defines in Article 5(1)(f) the principle of “integrity and confidentiality,” which states that data controllers and processors must ensure that appropriate security measures are in place to prevent data from being accidentally or deliberately compromised. A similar provision can also be found in the Brazilian General Data Protection Law.

In this sense, an important question is: with the advent of quantum computing, would asymmetric encryption schemes still be considered appropriate security measures to protect privacy and personal data?

It is relevant to note that the notion of “appropriate” is impacted, among other factors, by the state-of-the-art of a given set of technologies. In the cryptographic debate, it is already clear that quantum computing, although not yet a concrete problem, will severely interfere with some of the most currently used techniques, in particular asymmetric cryptography schemes. As quantum computing develops, these traditional cryptographic protocols may be on the verge of becoming obsolete. NIST has already declared that:

> when standards for quantum-resistant public-key cryptography become available, NIST will reassess the imminence of the threat of quantum computers to existing standards and may decide to deprecate or withdraw the affected standards thereafter as a result. Agencies should therefore be prepared to transition away from these algorithms as early as 10 years from now. (NIST, 2016a, p. 12)

Therefore, it is reasonable to consider that current asymmetric cryptographic schemes, such as RSA, DH, and ECC, may cease to be considered appropriate technical measures in a post-quantum world.

While it is a fact that, in general, legislation and regulation have great difficulty in keeping up with the pace of technological evolution, it is also interesting to note that privacy and data protection frameworks have increasingly emphasized the idea of “data protection by design”,[10] thus adopting an approach that is more flexible and able to dynamically adjust to the evolving technological landscape (Bruno & Spano, 2021).

The concept of data protection by design can be found in Article 25(1) of the GDPR, which states that:

> *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data*

[10] Data Protection by Design is related to the broader concept of Privacy by Design, used at the international level since the 1990s to refer to technological measures for ensuring privacy (EDPS, 2018, p. 4). However, Data Protection by Design refers to specific legal obligations established by Article 25(1) of the GDPR.

> *minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects (emphasis added).*[11]

Similar ideas can be found in article 46 of the Brazilian General Data Protection Law, which specifies that security, technical, and administrative measures to protect personal data must be adopted from the conception phase of the product or service until its execution. The Brazilian law also defines that the National Data Protection Authority may establish minimum technical standards to this end, taking into account the nature of the processed information, the specific characteristics of the processing, and the current state of technology.

However, technical and organizational measures are not always future-proof, which is why both the GDPR and the Brazilian legislation specify that the state of the art should be taken into account when defining what appropriate security measures are. Echoing this point of view, a recent publication on anonymization by the Spanish Data Protection Agency and the European Data Protection Supervisor – EDPS states that encrypted data cannot be considered anonymized data even if the decryption key is unknown, since technological developments, such as quantum computing, may affect their confidentiality in the long term (AEPD & EDPS, 2021, p. 3). In other words, encryption techniques will only remain reliable as long as they are capable of standing the test of time.

A last aspect worth consideration is the regulation of decryption. Hoofnagle and Garfinkel suggest that regulators should consider forbidding the decryption of third parties' data, since quantum technologies will not be democratically distributed for some time (Hoofnagle & Garfinkel, 2022). The authors also highlight the importance of the limitation of the retention of personal data to mitigate the impact of data breaches due to vulnerability to quantum cryptoanalysis (Hoofnagle & Garfinkel, 2022, p. 131). This approach seems consistent with existing regulation, since principles limiting personal data collection and retention exist in several privacy regulations, such as the data minimization principle in the GDPR (Art. 5(c)) and the principle of necessity in the LGPD (art. 6º, III).

In conclusion, the development of PQC standards is a welcome development, but it is also true that the adoption of new standards may depend on further regulation and enforcement, as well as on the availability of financial resources, to be successful in maintaining the security of digital communications and keeping organizations ahead of the disruption curve (Bruno & Spano, 2021). In this sense, while many countries, such as Brazil, have enacted legislation that appears to be sufficiently flexible and abstract to respond to technological changes and prevent the law from becoming prematurely outdated, new policies and a proactive approach by regulators

[11] It is interesting to note that the provision explicitly suggests pseudonymization as an appropriate security measure to implement DPbD. In 2014, the former Article 29 Working Party presented pseudonymisation as a set of techniques that reduces the linkability of a dataset with the original identity of a data subject, highlighting secret-key encryption schemes as one of those (Article 29 Data Protection Working Party – ART29WP, 2014, p. 20).

may be necessary to minimize the risks to digital rights that may be posed by quantum computing.

4.3 Global Cooperation Through International Legal Instruments

Finally, a third approach to be examined is the feasibility of reaching a global agreement on rights, responsibilities, and safeguards for human rights through a supranational instrument, such as an international treaty on quantum computing.

This is an appealing idea for different reasons. Firstly, there is no question that global cooperation based on shared visions could help boost research efforts and the development of innovative applications, harnessing the full potential of quantum technologies. Secondly, much of the criticism directed against digital constitutionalism refers to a perceived lack of effectiveness, excessive fragmentation, and insufficient enforceability of the new rights and principles under discussion. A supranational instrument could, in theory, serve to coordinate efforts towards the development of technical and human rights standards in the field of quantum computing.

It is, however, necessary to recognize the significant hurdles that this proposal would face in practical terms.

From a geopolitical standpoint, an important aspect to be considered is that the national approaches towards quantum computing are varied: while it is possible to identify initiatives to foment the development of royalty-free post-quantum cryptography, which may increase the access to these kinds of technologies, other approaches are more geared towards tech-protectionism, through dual-use technologies export control regimes. The result of the race for quantum supremacy is far from clear, and its consequences are still difficult to envision. Therefore, although global collaboration would be the ideal solution, nationalist tech governance frameworks may be closer to reality (Kop, 2021, p. 14). While it appears that developing countries without access to the technology might have incentives to support a treaty on this subject, the power disparity presented by the control of quantum computing by a few states or sub-national actors may also lower the incentives for harmonization of international rules on quantum (Rota, 2018).

Also from a human rights point of view, the challenges are significant. Until present, despite the relevance of resolutions on the right to privacy in the digital age approved by the United Nations General Assembly, discussions on multilateral digital constitutionalism have not yet produced binding and enforceable results. Deeks (2020) notes that it seems improbable that any state would, at this point, advocate for a binding multilateral treaty on encryption, not only because the topic is quite narrow but also because many take the view that the rights that encryption protects are already recognized in existing treaties.

In this sense, an approach that may be more feasible is to initiate international discussions on quantum technology through the development of soft law instruments, geared towards the establishment of agreed-on principles and objectives. This is, in fact, the approach that can currently be observed in regard to other disruptive technologies, such as artificial intelligence, where non-binding statements and principles gradually gain maturity and become more concrete and may, in the future, lead to binding international instruments and domestic legislation.[12]

5 Conclusion

While it may be unquestionable that quantum technologies will bring several social and economic benefits, there is also widespread recognition, within the technical community, that these technological developments pose relevant risks to existing cryptographic algorithms and may consequently affect the ability of individuals and organizations to enjoy secure communications. Despite this, current legal debates on a right to encryption, within the framework of digital constitutionalism, have so far failed to significantly engage with the elephant in the room, namely, the impacts that quantum technology may have on the exercise of fundamental rights in the digital environment.

The development of quantum computing does not automatically entail the collapse of current cybersecurity and personal data protection regimes, nor does it invalidate the ongoing legal discussions on the recognition of encryption as a technology that may enable human rights in the digital age. It does, however, point to the importance of preparation for this new scenario.

One important element of preparation refers to the introduction of cryptographic schemes that are resistant to quantum computing. While post-quantum cryptography standardization is a welcome development, it is important to keep in mind the complex geopolitical dynamics related to the development of quantum technology, which may accentuate power imbalances between nations. On the other hand, domestic preparation is also required, in the form of policies to promote the adoption of quantum-resistant technologies. In some cases, it may also be necessary to update legal or regulatory requirements related to privacy and cybersecurity, considering the state of the art of the evolving technological environment.

For developing countries, such as Brazil, perhaps the first challenge to be faced is related to agenda-setting. Initiatives to promote research, development, and innovation in quantum computing in the country are still in early stages and include the creation of a national quantum-computing network connecting government agencies, research centers, businesses, and startups (Fundação Instituto de Educação de Barueri - FIEB, 2022). There is, however, no question that there is still a significant technological gap in comparison to nations currently leading the quantum race. In countries such as Brazil, with limited financial resources and urgent policy issues to

[12] Some examples are the OECD AI Principles (OECD, 2019) and the UNESCO Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021), as well as the Council of Europe Ad hoc Committee on Artificial Intelligence initiative, which was mandated to examine the feasibility of and potential elements of a legal framework for the development, design, and application of artificial intelligence (CAHAI, 2020). It should also be noted that some initiatives that started with non-binding instruments have been evolving to binding ones, such as the current debates surrounding the European proposal for an Artificial Intelligence Regulation European Commission.

be addressed, it is not easy to place a high priority on the development of capabilities in a technology that may not produce concrete effects in the short term.

In Brazil, as in other countries, there is also a significant disconnection between the technical discussions on quantum computing and the legal conversations geared towards fundamental rights in the digital environment. This disconnection between regulation and innovation is a well-known phenomenon, which is also visible in the difficulty that lawmakers and regulators, in general, have in keeping up with new technologies. In the case of quantum technologies, however, since the technological and social changes that this technology may bring will only be felt in some years' time, there is still time to make legal and regulatory preparations for a post-quantum world.

As the debates on digital rights and freedoms evolve, and as the concept of digital constitutionalism gains maturity, there is an opportunity to delve into the consequences of the development of quantum technologies and to explore what kind of legal and policy responses should be adopted at the domestic and international level to promote an equitable distribution of the benefits that this technology may bring.

Data Availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of Interest The authors declare no competing interests.

References

Agencia Española de Protección de Datos - AEPD, & European Data Protection Supervisor - EDPS. (2021). *10 misunderstandings related to anonymisation* (p. 3). Retrieved from https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en

Applications and limitations of Diffie-Hellman algorithm - GeeksforGeeks. GeeksforGeeks. (2020). Retrieved 30 December 2021, from https://www.geeksforgeeks.org/applications-and-limitations-of-diffie-hellman-algorithm/

Article 29 Data Protection Working Party. (2014). *Opinion 05/2014 on anonymisation techniques - WP216* (p. 20). Brussels: European Commission. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Bay, M. (2017). The ethics of unbreakable encryption: Rawlsian privacy and the San Bernardino iPhone. *First Monday*. https://doi.org/10.5210/fm.v22i2.7006

Benari, E. (2014). *Azure blog and updates | Microsoft Azure*. Azure.microsoft.com. Retrieved 30 Dec 2021, from https://azure.microsoft.com/en-ca/blog/tag/ecc/

Berkman Center for Internet and Society. (2016). *Don't panic: Making progress on the "Going Dark" debate*. Cambridge, Massachusetts. Retrieved from https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

Brazil. (2020). Federal Supreme Court. Vote of the Justice Rapporteur Edson Fachin. Allegation of Non-compliance with a Fundamental Precept n. 403. Retrieved 9 June 2022, from https://www.conjur.com.br/dl/fachin-suspensao-whatsapp-decisao.pdf

Bruno, L., & Spano, I. (2021). *Post-quantum encryption and privacy regulation: Can the law keep pace with technology?*. Retrieved 11 Feb 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3920272

Casacuberta, D., & Senges, M. (2008). Do we need new rights in cyberspace? Discussing the case of how to define on-line privacy in an Internet Bill of Rights. *Enrahonar. Quaderns De Filosofia*, *40*, 99. Retrieved 9 June 2022, from https://doi.org/10.5565/rev/enrahonar.306

Celeste, E. (2019). Digital constitutionalism: A new systematic theorisation. *International Review Of Law, Computers & Technology*, *33*(1), 76–99. Retrieved 30 Dec 2021, from https://doi.org/10.1080/13600869.2019.1562604

Clarke, L. (2021). *Geopolitics threat to new-era quantum computing research - Tech Monitor*. Tech Monitor. Retrieved 30 Dec 2021, from https://techmonitor.ai/technology/emerging-technology/geopolitics-protectionism-threaten-quantum-computing-research

Coretti, S., Maurer, U., & Tackmann, B. (2013). A constructive perspective on key encapsulation. *Lecture Notes In Computer Science*, 226–239. Retrieved 11 Feb 2022, from https://doi.org/10.1007/978-3-642-42001-6_16

Council of Europe Ad hoc Committee on Artificial Intelligence - CAHAI. (2020). *Feasibility study*. Retrieved from https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da

de Wolf, R. (2017). The potential impact of quantum computers on society. *Ethics and Information Technology, 19*(4), 271–276. https://doi.org/10.1007/s10676-017-9439-z

Deeks, A. (2020). The international legal dynamics of encryption. Retrieved 11 Feb 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3587438

Dobner, P., & Loughlin, M. (2010). *The twilight of constitutionalism?* New York: Oxford University Press. *Elliptic Curve Digital Signature Algorithm - Bitcoin Wiki*. En.bitcoin.it. (2021). Retrieved 30 Dec 2021, from https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm

European Commission. (2021). *Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*. Eur-lex.europa.eu. Retrieved 11 Feb 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

European Data Protection Supervisor - EDPS. (2018). *Opinion 5/2018: Preliminary opinion on privacy by design*. Brussels: EDPS. Retrieved 11 Feb 2022 from https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

European Data Protection Supervisor - EDPS. (2021). *TechDispatch #2/2020: Quantum computing and cryptography*. Brussels: EDPS. Retrieved 11 Feb 2022 from https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-22020-quantum-computing-and_en

Fundação Instituto de Educação de Barueri - FIEB. (2022). *SENAI vai coordenar Rede Nacional de Computação Quântica MCTI/SOFTEX*. Fieb.org.br. Retrieved 11 Feb 2022, from https://www.fieb.org.br/noticias/senai-vai-coordenar-rede-nacional-de-computacao-quantica-mcti-softex/

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*(433). https://doi.org/10.22331/q-2021-04-15-433

Giles, M. (2019). *Explainer: What is post-quantum cryptography?*. MIT Technology Review. Retrieved 30 Dec 2021, from https://www.technologyreview.com/2019/07/12/134211/explainer-what-is-post-quantum-cryptography

Gill, L., Redeker, D., & Gasser, U. (2015). Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights. *SSRN Electronic Journal*. Retrieved 30 Dec 2021, from https://doi.org/10.2139/ssrn.2687120

Gregorio, G. (2022). *Digital constitutionalism in Europe*. Reframing rights and powers in the algorithmic society.

Harrow, A., & Montanaro, A. (2017). Quantum computational supremacy. *Nature, 549*(7671), 203–209. https://doi.org/10.1038/nature23458

Hoofnagle, C., & Garfinkel, S. (2022). *Law and policy for the quantum age* (pp. 126–139). Cambridge University Press.

ICP-Brasil. Instituto Nacional de Tecnologia da Informação. (2017). Retrieved 30 Dec 2021, from https://www.gov.br/iti/pt-br/assuntos/icp-brasil

Kaye, D. (2015). *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*. New York: United Nations. Retrieved from https://www.undocs.org/A/HRC/29/32.

Kop, M. (2020). Regulating transformative technology in the Quantum Age: Intellectual property, standardization & sustainable innovation, 2 *TTLF Newsletter on Transatlantic Antitrust and IPR Developments Stanford-Vienna Transatlantic Technology Law Forum*, Stanford University, 18. https://law.stanford.edu/publications/regulating-transformative-technology-in-the-quantum-age-intellectual-property-standardization-sustainable-innovation/

Kop, M. (2021). Establishing a legal-ethical framework for quantum technology. *Yale Journal Of Law & Technology,* 14. https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology/

Mancuso, M., & Rapa, A. (2020). *Anticipating a turning point in US export controls for tech | Publications | Kirkland & Ellis LLP*. Kirkland.com. Retrieved 30 Dec 2021, from https://www.kirkland.com/publications/article/2020/01/anticipating-turning-point-us-export-controls-tech

Mavroeidis, V., Vishi, K., D., M., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *International Journal Of Advanced Computer Science And Applications*, *9*(3), 3. https://doi.org/10.14569/ijacsa.2018.090354

Medeiros, F., & Bygrave, L. (2015). Brazil's Marco Civil da Internet: Does it live up to the hype? *Computer Law & Security Review, 31*(1), 120–130. https://doi.org/10.1016/j.clsr.2014.12.001

Ménard, A., Ostojic, I., Patel, M., & Volz, D. (2020). *A game plan for quantum computing*. McKinsey Quarterly. Retrieved 30 Dec 2021, from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/a-game-plan-for-quantum-computing

Mendes, G. F., & Fernandes, V. O. (2020). Constitucionalismo digital e jurisdição constitucional: Uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira De Direito, Passo Fundo, 16*(1), 1–33.

Moncau, L. F. M., & Arguelhes, D. W. (2020). The Marco Civil da Internet and digital constitutionalism. In: Giancarlo Frosio. (Org.). The Oxford handbook of online intermediary liability. 1ed. *Oxford University Press*, 1, 190–214. Retrieved 11 Feb 2021, from https://doi.org/10.1093/oxfordhb/9780198837138.001.0001/oxfordhb-9780198837138-e-10

Moraes, T. (2020). Sparkling lights in the going dark: Legal safeguards for law enforcement's encryption circumvention measures. *European Data Protection Law Review*, *6*(1), 41–55. https://doi.org/10.21552/edpl/2020/1/7

National Institute of Standards and Technology - NIST. (2016a). *Report on post-quantum cryptography*. U.S. Department of Commerce. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2016a/NIST.IR.8105.pdf

National Institute of Standards and Technology - NIST. (2016b). *Submission requirements and evaluation criteria for the post-quantum cryptography standardization process*. U.S. Department of Commerce. Retrieved from https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016b.pdf

National Institute of Standards and Technology - NIST. (2020). *Status report on the second round of the NIST post-quantum cryptography standardization process*. (p. 12) U.S. Department of Commerce. Retrieved from https://doi.org/10.6028/NIST.IR.8309

National Institute of Standards and Technology - NIST. (2021). *Post-quantum cryptography: The good, the bad, and the powerful* [Video]. Retrieved 30 Dec 2021, from https://www.nist.gov/video/post-quantum-cryptography-good-bad-and-powerful

Organization for Economic Cooperation and Development - OECD. (1997). *Recommendation of the council concerning guidelines for cryptography policy*. Retrieved 24 May 2022, from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0289

Organization for Economic Cooperation and Development - OECD. (2019). The OECD artificial intelligence (AI) principles - OECD.AI. Oecd.ai. Retrieved 11 Feb 2022, from https://oecd.ai/en/ai-principles

Organization for Economic Cooperation and Development - OECD. (2020). Digital economy outlook. Retrieved 24 May 2022, from https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2020_bb167041-en

Pfefferkorn, R. (2017). Everything radiates: Does the fourth amendment regulate side-channel cryptanalysis?. *Connecticut Law Review*, *49*, 1398. Retrieved 30 Dec 2021, from https://law.stanford.edu/publications/everything-radiates-does-the-fourth-amendment-regulate-side-channel-cryptanalysis/

Post-Quantum Cryptography. NIST. (2017). Retrieved 30 Dec 2021, from https://csrc.nist.gov/projects/post-quantum-cryptography

Rand, L., & Rand, T. (2021). *The 'Prime Factors' of quantum cryptography regulation*. (p. 16) Retrieved 30 Dec 2021, from https://doi.org/10.2139/ssrn.3904342

Rieffel, E., & Polak, W. (2011). *Quantum computing: A gentle introduction* (1st ed., p. 14). The MIT Press.

Rota, D. (2018). A quantum leap in international law on cyberwarfare: An analysis of international cooperation with quantum computing on the horizon. *Harvard Law School National Security Journal*. Retrieved 30 Dec 2021, from https://harvardnsj.org/2018/11/a-quantum-leap-in-international-law-on-cyberwarfare-an-analysis-on-the-need-for-international-cooperation-with-quantum-computing-on-the-horizon/

Silva, P., Mangeth, A., & Perrone, C. (2021). The encryption debate in Brazil: 2021 update. *Carnegie Endowment for International Peace.* Retrieved 11 Feb 2022, from https://carnegieendowment.org/2021/03/31/encryption-debate-in-brazil-2021-update-pub-84238

Solove, D. (2011). Nothing to hide: The false tradeoff between privacy and security. *Yale University Press*. https://doi.org/10.5860/choice.49-2979

Suzor, N. (2018). Digital constitutionalism: Using the rule of law to evaluate the legitimacy of governance by platforms. *Social Media + Society*, *4*(3), 205630511878781. https://doi.org/10.1177/2056305118787812

Teubner, G. (2012). *Constitutional fragments: Societal constitutionalism and globalization*. Oxford University Press.

U.S-China Economic and Security Review Commission. (2021). *Unfinished business: Export control and foreign investment reforms*. Retrieved 11 Feb 2022 from https://www.uscc.gov/sites/default/files/2021-06/Unfinished_Business-Export_Control_and_Foreign_Investment_Reforms.pdf

U.S. House Judiciary Committee and House Energy and Commerce Committee. (2016). *Encryption working group year-end report*. Retrieved 11 Feb 2022 from https://www.americanbar.org/content/dam/aba/administrative/law_national_security/Encryption%20Working%20Group%20YE%20Rep.pdf

United Nations Educational, Scientific and Cultural Organization - UNESCO. (2016). *Human rights and encryption.* Paris: UNESCO. Retrieved 24 May 2022 from https://unesdoc.unesco.org/ark:/48223/pf0000246527

United Nations Educational, Scientific and Cultural Organization - UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. Retrieved 11 Feb 2022 from https://en.unesco.org/artificial-intelligence/ethics

United Nations Human Rights Council - UNHCR. (2019). *Resolution adopted by the Human Rights Council on 26 September 2019 on the right to privacy in the digital age*. Retrieved 11 Feb 2022 from https://digitallibrary.un.org/record/3837297

United Nations Human Rights Council - UNHCR. (2020). *Resolution adopted by the Human Rights Council on 6 October 2020 on the safety of journalists*. Retrieved 11 Feb 2022 from https://undocs.org/en/A/HRC/RES/45/18

Walden, I. (2018). 'The sky is falling!' – Responses to the 'Going Dark' problem. *Computer Law & Security Review, 34*(4), 901–907. https://doi.org/10.1016/j.clsr.2018.05.013

WhatsApp. (2020). *WhatsApp encryption overview: Technical white paper*. WhatsApp. Retrieved 11 Feb 2022 from https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

Yilma, K. (2017). Digital privacy and virtues of multilateral digital constitutionalism—Preliminary thoughts. *International Journal of Law and Information Technology, 25*(2), 115–138. https://doi.org/10.1093/ijlit/eax001