EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012

Post-quantum encryption and privacy regulation: Can the law keep pace with technology?

LUIGI BRUNO
Doctor of Civil Law (D.C.L.) candidate at McGill University, Faculty of Law
ISABELLA SPANO
Doctor of Civil Law (D.C.L.) candidate at McGill University, Faculty of Law

Abstract

Using an interdisciplinary law and computer science approach, this article argues that quantum computing must push lawmakers to implement more dynamic privacy regulation to cushion quantum computing's impact on data protection and privacy.

This article highlights the EU GDPR position as the global standard for data protection and privacy regulation. The GDPR has ignited a legal standardization phenomenon, whereby many jurisdictions are shaping their privacy regulation based on the GDPR. A move by EU lawmakers to amend the GDPR to embed post-quantum encryption requirements dynamically would ignite a global paradigm shift. This would result in forward-looking protection of data subjects' rights that extends beyond quantum computing perils. It would also signal that lawmakers' intention to making privacy regulation dynamic, thus enabling it to cope with future threats by being ahead of the technological disruption curve.

Keywords: Privacy Law; GDPR; Quantum Computing; Encryption; Data Protection Law; Technology Law.

Summary: Introduction. – 1. Quantum computers versus classical computers: a tale of two worlds. – 2. The relevance of quantum computing for encryption. – 3. A privacy and data protection regulatory challenge: slow regulation for fast tech. – Conclusions: Post-quantum cryptography and the future of data protection regulation.

Introduction.

Quantum computing is still far from mainstream adoption and is currently only used for scientific research purposes. Nevertheless, its impact on existing encryption algorithms and data protection and privacy regulation is already generating threats that require attention and consideration.

This novel computing paradigm came under the spotlight in 2019 when Google's AI Quantum team announced that it had achieved quantum supremacy.[1] Google announced the achievement via an article in Nature, which sparked controversy with IBM.[2] In the article, Google's team argued that their quantum processor (a 54 qubits "Sycamore") had taken about 200 seconds to perform a task that would have taken a state-of-the-art classical supercomputer approximately 10'000 years to complete. [3] A classical supercomputer is one of today's fastest high-performance systems.[4] Google's significant improvement in computational speed represents an experimental achievement of quantum supremacy, at least for the particular task tested.[5]

One year later, China's government announced that a team of its scientists had also achieved quantum supremacy. China made its announcement in an article in Science, wherein PRC's scientists declared that their achievement resulted from a quantum computer based on a different technology than Google's.[6]

These announcements are symptomatic of an ongoing race to quantum supremacy among superpowers - a race fuelled by quantum computing's promises to disrupt and improve research in chemistry, [7] biology, space exploration, artificial intelligence, and more.

Nevertheless, disruption also has side effects. Extensive research has shown that quantum computing can break modern symmetric and asymmetric

[1] Frank Arute et al., 'Quantum supremacy using a programmable superconducting processor' (2019) Nature 574, 505.
[2] Edwin Pednault et al., 'On "Quantum Supremacy"' *IBM* (21 October 2019) <https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/5>.
[3] Arute et al., 'Quantum supremacy using a programmable superconducting processor' (n 1).
[4] William L. Hosch, 'Supercomputer' *Encyclopedia Britannica* (2019) <https://www.britannica.com/technology/supercomputer> accessed 20 November 2019.
[5] *Ibid.*
[6] Han-Sen Zhong et al., 'Quantum computational advantage using photons' (2020) Science 370, 1460.
[7] Bryan Walsh, 'Why quantum computing matters' Axios (26 August 2020) <https://www.axios.com/quantum-computing-google-ibm-b0b90670-a36b-443a-b45f-eff3ceb79ec2.html> accessed 8 January 2020.

cryptography, [8] threatening current data protection and privacy practices. Regulation and laws worldwide rely on encryption as a tool to protect personal information online. The pace of development in quantum computing should inspire legislators and supervisory authorities alike to swiftly reconsider how laws and regulation can cushion quantum's impact on data protection.

This article discusses the impact of quantum computing on modern cryptographic algorithms from the interdisciplinary perspective of law and computer science. Its goal is to explore how data protection and privacy regulation need to be reimagined to keep up with technological development.

The remainder of this article is divided into four parts. The first part introduces quantum computing by showing how it differs from classical computing. The second part discusses quantum computing's impact on current encryption practices and, consequently, data protection and privacy. The third part argues that quantum computing's threats to encryption are a cautionary tale for data protection and privacy bodies, regulators and legislators, who face the challenge of technology exponentially outpacing regulation. The fourth and last part explores existing post-quantum cryptography initiatives and the future of data protection and privacy regulation.

1. Quantum computers versus classical computers: A tale of two worlds.

Quantum computers leverage quantum mechanics' laws to use quantum bits, in short *qubits*, as the basic data unit. These laws generate phenomena that enable qubits to be in multiple states of *|0⟩* and *|1⟩* simultaneously and correlate their measurement and states.[9] Qubits' very nature brings forward a new paradigm that does not map onto classical concepts. Essentially, qubits are in a linear combination of a 0 state and a 1 state, which is neither "AND" nor "OR." Therefore, through this paradigm, quantum computers perform operations so that the probabilities of reaching the right results are enhanced, while the probabilities of getting the wrong results are depressed.[10]

On the other hand, classical computers differ from quantum computers because they do not leverage quantum mechanics' properties and advantages to perform computation.[11] A classical computer—that is, one that can be modelled by a deterministic Turing machine—uses *bits* as the basic data unit. Users input instructions that are converted in binary code of 0s and 1s and are then translated into electrical signals to operate the transistors that compose the Central Processing Unit. 0 indicates "OFF," and 1 "ON." According to this logic, classical computers can only perform operations for determined values of 0 and 1.

2. The relevance of quantum computing for encryption.

[8] Vasileios Mavroeidis et al., 'The Impact of Quantum Computing on Present Cryptography' (2018) International Journal of Advanced Computer Science and Applications 9, 405.
[9] Vasileios Mavroeidis et al., 'The Impact of Quantum Computing on Present Cryptography' (n 8).
[10] National Academy of Engineering, *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2018 Symposium* (National Academies Press 2019).
[11] Jack Hidary, *Quantum Computing: An Applied Approach* (Springer 2019).

In 1982 Richard Feynman brought the idea of quantum computing to light.[12] However, the scientific community's interest in quantum computing increased sharply in 1994 when the mathematician Peter Shor developed the famous eponymous algorithm.

Shor's algorithm allows quantum computers to "*find the prime factors of large numbers efficiently*," [13] that is, "*with an exponential speed-up when compared to the best-known classical algorithm.*"[14] The problem of finding the prime factors of large numbers is the foundation of most of today's secure online communication.

The factorization problem at the heart of Shor's algorithm is vital to secure most of today's online communication. In this light, Gamble argues that the efficiency of Shor's algorithm should be seen:

[…] in a time of practical relevance, which is beyond the capability of state-of-the-art classical algorithms. […] The security of nearly every online transaction today relies on an RSA cryptosystem that hinges on the intractability of the factoring problem to classical algorithms.[15]

The RSA cryptosystem is a building block of the current internet infrastructure used to secure most online communication.[16] Its importance cannot be overstated since over 69%[17] of all websites communicate relying on the secure version of the HTTP protocol (the so-called HTTP Secure protocol), which is based on RSA encryption.[18]

The RSA algorithm's one-way function is the same integer factorization problem at the heart of Shor's algorithm. By recalling high school mathematics notions, it is easy to see that multiplying two large prime numbers is simple. However, the operation of factoring the resulting product is incredibly difficult.[19] Most of the commonly used forms of RSA encryption are currently based on the 2048 bits number factorization. Factoring any number larger than that is considered to be almost impossible for a classical computer.[20]

According to the MIT Technology Review, a team of scientists at Google and at the KTH Royal Institute of Technology has shown that a 20-million qubits quantum computer could factor 2048 RSA integers and thus break encryption in only eight hours.[21] However, a 20-million qubits processor seems a distant

---

[12] Richard P. Feynman, 'Simulating Physics with Computers' (1982) International Journal of Theoretical Physics 21, 467.
[13] Franklin de Lima Marquezino et al., 'Shor's Algorithm for Integer Factorization' in Franklin de Lima Marquezino et al. (eds), *A Primer on Quantum Computing* (Springer 2019).
[14] *Ibid.*
[15] National Academy of Engineering, *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2018 Symposium* (n 10).
[16] Christof Paar and Jan Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners* (Springer 2009).
[17] W3 Techs, 'Web Technology Surveys' <https://w3techs.com/technologies/details/ce-httpsdefault> accessed 20 January 2021.
[18] For further information on the Hyper-Text-Transfer-Protocol Secure (HTTPS) see James F Kurose and Keith W Ross, *Computer Networking: A Top-Down Approach* (Pearson 2013).
[19] Christof Paar and Jan Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners* (n 16).
[20] Emerging Technology from the arXiv, 'How a quantum computer could break 2048-bit RSA encryption in 8 hours' *MIT Technology Review* (30 May 2019) <https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/>.
[21] *Ibid.*

reality compared to the 54 qubits processor that Google used to declare quantum supremacy in 2019.

At the current pace of innovation, a 20-million qubits processor could take 25 years or more to be produced.[22] Or it could take less, much less. History is filled with failed attempts to predict the rate of innovation.[23]

This impossibility to accurately forecast when quantum computing will be capable of quickly breaking existing encryption methods prospect raises technical and regulatory questions *vis-à-vis* its critical implications for data protection and privacy. For instance, information intended to be stored for extended periods, in domains such as banking, defence, and foreign policy, should be secured with cryptographic algorithms that are quantum-proof as soon as possible. Encrypted packets of personal and sensitive information could be captured online today and be decrypted in the future, once quantum computers have become widely available and powerful enough. Although decrypting a credit card number three decades from now would probably prove unfruitful for the attackers, the same cannot be said for social security numbers and other personally identifiable information.

Therefore, quantum computers' ability to efficiently solve complex factorization problems poses a threat to current cryptographic systems and, consequently, to the data protection and privacy capabilities they offer. Mathematicians aware of these threats have launched initiatives aiming at keeping data and privacy protected in a post-quantum world. These initiatives have given rise to post-quantum encryption algorithms that leverage mathematical operations that cannot be efficiently solved using quantum computation. Many of these algorithms are freely available online.

The US National Institute of Standards and Technology (NIST) has been the first public body to acknowledge the threat that quantum computing poses to encryption. In 2017, the NIST launched a Post-Quantum Encryption Standardization project and invited mathematicians and cryptography experts to submit proposals for encryption algorithms that could withstand attacks carried using quantum computation.[24]

However, there is no doubt that standardization does not equal regulation. Data protection and privacy laws that hinge on encryption as a technical measure to prevent breaches ought to be reimagined in the face of quantum computing. NIST's standardization effort will only prove marginally successful in maintaining the security of today's internet communication unless its outcomes are swiftly absorbed by regulation and enforced by data protection authorities.

3. A privacy and data protection regulatory challenge: slow regulation for fast tech.

[22] Emerging Technology from the arXiv, 'How a quantum computer could break 2048-bit RSA encryption in 8 hours' (n 20).
[23] For a timeline of failed technology predictions see Visual Capitalist <https://www.visualcapitalist.com/a-timeline-of-failed-tech-predictions/> accessed 10 Jan 2021.
[24] NIST, 'NIST Asks Public to Help Future-Proof Electronic Information' (20 December 2016) <https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information> accessed 11 January 2021.

NIST's standardization initiative is a warning for governments and privacy and data protection bodies alike that legislative and regulatory action is needed. For instance, European lawmakers and data protection authorities are aware that personal information must be protected from quantum computing perils.[25] However, the breadth of the measures required to ensure continued and consistent protection while quantum computers are developed, become available, and are eventually adopted may not have been fully grasped yet.

This legislative inertia might rest on the assumption that it will take quantum computing a generation or more before it becomes a critical problem for data protection and privacy.[26] This assumption might be severely flawed, considered that technology forecasting rarely yields satisfying results, mainly when global superpowers are competing to be the fastest to develop the best quantum technology.[27] Therefore, it would not be surprising if quantum computing development accelerated several orders of magnitude over the next few years.

Legislators ought to consider this possibility since one of the most significant challenges that they continue facing in creating and implementing regulatory frameworks is the different pace at which technology and the law move. By its nature, the law is static and developed to respond to societal changes *a posteriori*. Norms require time to be implemented within a system, whereas technology is swift and thrives dynamically, in continuous evolution.

For instance, the European Union General Data Protection Regulation (GDPR)[28] was adopted in 2018 to replace the 1995 Data Protection Directive.[29] The latter was developed and introduced at the dawn of the internet era when all but a handful of visionaries saw the World Wide Web's potential and perils. Many technologies evolved exponentially during the six years that elapsed from the moment the European Commission proposed a reform to the 1995 Directive to adopting the GDPR. One of these technologies is Machine Learning, which, until the advent of the GDPR, was used to process personal

[25] The European Data Protection Supervisor has recognized the relevance of NIST's standardization process and stressed that the uncertainty of quantum computing development will require solutions to protect data. See Lukas Olejnik and Robert Riemann, 'TechDispatch #2/2020: Quantum Computing and Cryptography', *Eur. Data Prot. Supervisor* (7 August 2020) <https://data.europa.eu/doi/10.2804/603798> accessed 14 January 2020. In the United States, Dr. Jill Pipher of Brown University presented "No Longer Secure: Cryptography in the Quantum Era" at a Capitol Hill lunch briefing, in December 2019. In the briefing, Pipher also discussed the consequences of quantum computing on cybersecurity. See Cynthia Brumfield, 'The Race for Quantum-Proof Cryptography' *CSO* (10 December 2019) <https://www.csoonline.com/article/3488857/the-race-for-quantum-proof-cryptography.html> accessed 15 December 2020.

[26] See Olejnik and Riemann ("Based on what we know today there is no immediate threat posed by a quantum computer in the foreseeable future.").

[27] Not surprisingly, quantum computing development has been compared to the so-called "space race", with numerous superpowers investing and competing to achieve quantum supremacy. See Walter G. Johnson, 'Governance Tools for the Second Quantum Revolution' (2019) Jurimetrics 59, 490–491.

[28] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

data almost without any regulatory constraints.[30]

The natural consequence of the dynamic between law and technology is that legislative and regulatory bodies' attempts to keep technology within their grasp often fail or result unsatisfactory.[31] This outcome can be due to the inability to translate the fast-paced dynamism of technology into the law's static language. When it comes to data protection and privacy, the price for excessively static, and often late, regulation is paid directly by data subjects, whose privacy is threatened by normative gaps. Hence, to maintain adequate normative protection of privacy rights *vis-à-vis* technological innovation and disruption, a proactive, dynamic and forethinking legislative approach is required.

Such an approach can be partly identified in one of the core principles of the GDPR: Privacy by Design. The principle provides that systems processing personal data should be designed to ensure privacy protection.[32] In other words, Privacy by Design aims to integrate proactive privacy safeguards in the design phase of systems that process personal data. The idea of Privacy by Design requires dynamism of privacy safeguards' implementation, with organizations preventing risks rather than patching up damages from materialized data breaches.

In 2010, the International Conference of Data Protection and Privacy Commissioners stated that "Privacy by Design [is] an essential component of fundamental privacy protection" and encouraged lawmakers to include this principle in future privacy and data protection regulatory frameworks.[33] Privacy by Design, as embraced by Article 25 of the GDPR, represents the recognition by the EU of its foundational importance in data protection efforts.[34] This leads to questioning whether the GDPR as a whole proposes a dynamic approach that can respond to privacy risk and threats stemming from future technological innovations such as quantum computing. This question's relevance cannot be overstated, given that the GDPR has *de facto* ignited a process of global legal harmonization.[35] For instance, other jurisdictions, such as California[36] and Quebec[37], have adopted or are in the process of adopting laws that are primarily inspired by the GDPR.

---

[30] For an overview of the history of data protection and privacy regulation see European Data Protection Supervisor <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed on 11 January 2021).

[31] Mark Fenwick et al., 'Regulation Tomorrow: Strategies for Regulating New Technologies' in Toshiyuki Kono et al. (eds), *Transnational Commercial and Consumer Law* (Springer 2018) 153-155.

[32] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, para 25.

[33] Resolution on Privacy by Design, 32nd International Conference of Data Protection and Privacy Commissioners (27-29 October 2010) <https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf> accessed 16 January 2021.

[34] Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) Oslo Law Review 4, 107.

[35] On the effects of the GDPR on global data protection see Tiffany Curtiss, 'Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies' (2016) Washington Journal of Law, Technology and the Arts 12, 95; Christopher Kuner et al., 'The GDPR as a Chance to Break Down Borders' (2017) 7 International Data Privacy Law 7, 231; Dulce Lopes, 'GDPR - Main International Implications' (2020) European Journal of Privacy Law and Technology 9.

[36] California Consumer Privacy Act of 2018 (USA).

[37] Quebec Bill N.64 (CA).

Analysing the difference between the concept of Privacy by Design originally theorized by privacy scholar Ann Cavoukian and the novel iteration of the same principle within the GDPR may help answering this question. Theoretically, Privacy by Design requires a dynamic and continuously evolving approach to data protection, mirroring the dynamism of technological development. Privacy by Design aims to consistently protect personal data regardless of how and in which direction technology evolves. According to Cavoukian, "*[p]rivacy must become integral to organizational priorities, project objectives, design processes, and planning operations*."[38]

Cavoukian's theorization of Privacy by Design proposes a multidimensional approach to privacy protection for organizations. Vertically, this approach requires organizations to embed privacy in their systems and technologies by default, through privacy engineering.[39] Horizontally, it requires organizations to reimagine their business under the overarching theme of privacy. Overall, Cavoukian's approach aims to ensure that organizations anticipate and prevent privacy-invasive events before they happen.[40]

The current approach to Privacy by Design proposed by Article 25 of the GDPR greatly emphasizes the principle's vertical dimension rather than its multidimensionality. However, the horizontal dimension would ensure threats like the one posed by quantum computing to be anticipated and dealt with swiftly, without requiring additional legislation or continuous reforms.

The limitation of the reach of the principle of Privacy by Design in the GDPR seems based on risk analysis. The more dynamic a law, the more it will inevitably encounter feasibility and continuous compliance issues. Hence, the EU lawmakers faced the risk of creating an unenforceable soft law instrument had it excessively and unclearly generalized the norm's content. On the other hand, the opposite would have led to an impossibly demanding framework that would have unfairly disadvantaged small businesses over Big Tech companies, with the latter having the resources to ensure compliance.[41]

It is necessary for the GDPR and, by extension, GDPR-inspired regulation worldwide to provide a more encompassing and dynamic privacy governance framework. One that would require little to no amendments to the regulation, to ensure that forthcoming privacy risks and threats such as quantum computing are minimized seamlessly and consistently over time. Dynamic privacy and data protection regulation should favour proactive wording to push organizations to stay ahead of the disruption curve. In the case of quantum computing, this means requiring organizations to implement the forthcoming NIST post-quantum encryption standards without waiting for the adoption of additional legislation.

---

[38] Ann Cavoukian, 'Privacy by Design: the 7 Foundational Principles' *Privacy Security Academy* (August 2020) <https://www.privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf> accessed 8 December 2020.

[39] Sean Brooks et al., 'An Introduction to Privacy Engineering and Risk Management' *NIST* (7 January 2017) <https://doi.org/10.6028/NIST.IR.8062> accessed 11 December 2020.

[40] Ann Cavoukian, 'Privacy by Design: the 7 Foundational Principles' (n 38).

[41] Even in the GDPR's current form, the EU has registered hardships in GDPR compliance for small businesses. On the matter see the '2019 GDPR Small Business Survey', GDPR.eu (May 2019) <https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf> accessed 14 January 2021.

4. Conclusions: Post-quantum cryptography and the future of data protection regulation.

Quantum computing must start the conversation on the implementation of more dynamic privacy and data protection regulation. NIST's effort to reach a standardized set of post-quantum encryption algorithms should inspire legislators and privacy authorities worldwide to start the necessary process of reforming existing and introducing new regulatory frameworks.

NIST has explicitly warned organizations about the threats that quantum computing presents already today to encrypted data and what risks this entails for data subjects. NIST's recommendation is unequivocal: prepare today for the privacy breach of tomorrow. Lawmakers should embrace this proactive and forward-thinking approach and embed it in data protection and privacy regulation. Without it, it will be difficult to achieve regulatory dynamism and cope with forthcoming technological changes that may affect data protection and privacy.

NIST's Post-Quantum Cryptography Standardization project aims to standardize a set of the most effective quantum-resistant cryptographic algorithms. Its goal is to solicit, evaluate and select quantum-resistant public-key cryptographic algorithms devised by mathematicians and cryptography experts worldwide.[42] Public-key algorithms, such as RSA, underpin today's infrastructure that allows us to communicate online securely. Therefore, NIST has chosen to limit its standardization efforts only to these algorithms, at least for the time being.

NIST has announced the beginning of its third selection round on July 22, 2020.[43] The expectation is that by the end of this phase, NIST will shortlist one or two quantum-resistant encryption algorithms that will ultimately compose its standard. The current deadline for the publication of the first official standard is 2022, even when considering potential pandemic-related slowdowns. At the same time, NIST will provide organizations with technical guidance on implementing the standardized algorithms.

In the meantime, to ease the transition, NIST has recently published a whitepaper in which it first paints the picture of the impact of quantum computing on existing – or classical – encryption. It then brings forward the challenges linked with implementing post-quantum encryption once the standardization process will have been concluded.[44]

Lawmakers and privacy authorities outside of the US should closely monitor NIST's standardization project's outcome, [45] as the EU Agency for Cybersecurity

---

[42] NIST, 'Post-Quantum Cryptography' *NIST* (6 January 2017) <https://csrc.nist.gov/projects/post-quantum-cryptography> accessed 19 January 2021.

[43] NIST, 'NIST's Post-Quantum Cryptography Program Enters "Selection Round"' *NIST* (22 July 2020) <https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round> accessed 4 January 2021.

[44] NIST, 'Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms' NIST (28 April 2021) <https://csrc.nist.gov/publications/detail/white-paper/2021/04/28/getting-ready-for-post-quantum-cryptography/final> accessed 28 June 2021.

[45] NIST's efforts have already been recognized by agencies such as the French *Agence National de la Sécurité des Systèmes d'Information* (ANSSI), which published a paper on Quantum Key Distribution. In its paper, ANSSI

(ENISA) is already doing. The GDPR has de facto become the global gold standard for data protection and privacy regulation. An increasing number of jurisdictions are shaping their privacy regulation based on the GDPR, mainly to ensure adequate data protection to transfer data from and to the EU. Providing free and secure data transfer with the EU is a priority for states and organizations alike, given the single EU market's economic relevance. [46] Therefore, a potential move by Brussels' lawmakers to prescribe the implementation of NIST's post-quantum encryption standard, at least to those organizations potentially impacted by the technology, would ignite a paradigm shift. It would not only project international data protection into its post-quantum future, but it would also signal that data protection and privacy regulation are most effective when they look at the future of technology. In such a case, foreign jurisdiction would inevitably follow the EU's lead, thus setting up a new global standard for privacy protection while renewing the conversation on how regulation ought to be designed and implemented.

Doing so would not require much regulatory effort from the EU. For what concerns explicitly encryption, the GDPR indicates in its article 32 the obligation for organizations to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk".[47] In this light, ENISA has recently released a study examining the current state of the standardization process of post-quantum encryption, including describing the finalist algorithms chosen by NIST. [48] The study has a forward-looking approach, taking into consideration the time that will be required for NIST to complete its standardization process. It also offers organizations two proposals for implementing immediate solutions that could already protect the confidentiality of their data against quantum-enabled attacks.[49] Hence, the European Data Protection Board (EDPB) could release additional guidelines clarifying quantum computing's impact on encryption a legal perspective and requiring organizations to follow ENISA's proposals and then implement NIST's standard to ensure compliance with the GDPR.

On the one hand, this would result in a stronger, more encompassing, and forward-looking protection of data subjects' privacy rights. On the other hand, it would signal that lawmakers and supervisory authorities are keen to make privacy regulation dynamic. A dynamic regulatory framework would ultimately be capable of coping with forthcoming threats by relying on additional sources, such as standards and soft-law instruments, without needing constant amendments or reforms.

---

advises caution in the application of NIST's algorithms, and suggests "combin[ing] them with current mechanisms in order to avoid any security regression linked to immature designs." ANSSI, 'Should Quantum Key Distribution Be Used for Secure Communications' *ANSSI* (4 May 2020) <https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/> accessed 16 January 2021.

[46] Dulce Lopes, 'GDPR - Main International Implications' (2020) European Journal of Privacy Law and Technology 9, 14.

[47] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, para 32.

[48] ENISA, 'Post-Quantum Cryptography: Current state and quantum mitigation' ENISA (3 May 2021) <https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation> accessed 24 June 2021.

[49] *Ibid.*