Quantum Preparedness as a Constitutional Obligation for the European Union*

Davide Clementi

Table of contents

1. Introduction

The necessity of preparing for the quantum era represents not merely a technological challenge but a legal duty for the European Union (EU).[1] In order to understand why this duty arises, it is first necessary to clarify what is meant by quantum computing. Contemporary technologies are undergoing what several authors have described as a second quantum revolution,[2] in which the principles of quantum mechanics are no longer only the object of theoretical description but become the operating core of new devices capable of processing, transmitting and securing information in ways that classical electronics cannot achieve. Quantum computing belongs to this family: it is a form of computation that no longer relies on the traditional bit, which can take only the value 0 or 1, but on the

* Peer-reviewed article.

[1] R. De Wolf, *The Potential Impact of Quantum Computers on Society*, in *Ethics and Information Technology*, 19, 2017, 271 ff.; C. Bush, *Quantum Computing and Digital Payments: Opportunities, Threats, and the Path toward Regulation*, in *International Review of Law, Computers and Technology*, 2026, 1 ff.; N. Bindel – M. Mosca – B. Munson, *The Quantum Threat to Cybersecurity and Privacy*, in *The Boundaries of Data*, 2024, 35 ff.

[2] J.P. Dowling – G.J. Milburn, *Quantum Technology: the Second Quantum Revolution*, in *Philosophical Transactions of the Royal Society of London*, 2003, 1655 ff.; I.H. Deutsch, *Harnessing the Power of the Second Quantum Revolution*, in *PRX Quantum*, 1, 2020, 020101; K. Intonti et al., *The Second Quantum Revolution: Unexplored Facts and Latest News*, in *Encyclopedia*, 4, 2024, 630 ff.; A. Ferreira – V. Lipiäinen – C. Polito, *Quantum Technologies and Cybersecurity*, CEPS Research Paper, Brussels, 2023.

quantum bit (qubit), a physical system governed by quantum laws that can be prepared in a superposition of states, so that, before measurement, it can encode simultaneously the information corresponding to 0 and to 1. This property of superposition, to which one may add the possibility of correlating qubits through entanglement – a phenomenon in which two or more qubits become linked in such a way that the quantum state of each cannot be described independently of the others, even when separated by large distances – allows a quantum processor to explore in parallel portions of the computational space that a classical machine could reach only through sequential or exponentially costly steps. It was precisely this insight, already noted by Feynman in the early 1980s, that suggested that certain phenomena described by quantum physics cannot be efficiently simulated by classical computers, and that, conversely, a computer built according to quantum rules could solve specific classes of problems with far superior efficiency. The decisive confirmation came in 1994 with Shor's algorithm,[3] which showed that a sufficiently powerful quantum computer would be able to factor large integers in polynomial time, thus attacking the mathematical problems on which today's most widespread public key cryptographic schemes are based. From that moment it became evident that quantum information and quantum computers were not only a theoretical exercise, but a technology with concrete and disruptive applications in cryptography, optimization, simulation of materials and chemical processes, and even in the acceleration of certain artificial intelligence tasks. Precisely because they are able to manage information in a way that exploits the laws of the subatomic world, quantum machines can produce benefits of extraordinary scope, but they can also generate risks of the same magnitude, including risks for cybersecurity, national security and the protection of personal and strategic data.

Seen in this light, quantum computing, while promising revolutionary advances in computation, simulation, and cryptographic analysis, simultaneously introduces a class of risks unprecedented in both scale and systemic impact. The capacity of quantum machines to disrupt current public key encryption schemes threatens the confidentiality of communications, the

[3] Shor's algorithm and Grover's algorithm are two landmark quantum-computing algorithms. Shor's algorithm allows a quantum computer to factor large composite integers in time that is polynomial in the logarithm of the integer, thereby achieving an exponential speed-up over the best-known classical factoring methods, and raising critical implications for cryptographic systems based on integer-factorisation hardness (such as RSA). Grover's algorithm is tailored to the "unstructured search" problem (i.e., finding a target entry in an unsorted database of size N) and achieves a quantum quadratic speed-up (roughly $O(\sqrt{N})$ queries, where N denotes the size of the database and O denotes standard asymptotic complexity notation) compared to the classical O(N) brute-force search; while not exponential, the quadratic improvement remains widely significant, especially for cryptographic brute-force attacks on symmetric-key systems.

protection of data, and, by extension, the foundational values of the European Union's legal order.[4] At stake are the effectiveness of fundamental rights, the credibility of digital governance, and the preservation of the Union's autonomy.

Within the European legal framework, stretching from primary law to the extensive body of secondary legislation, the institutions of the Union and Member States bear positive obligations to ensure that freedoms and rights remain effective within the digital environment. This includes the duty to maintain the technological conditions necessary for the exercise of those rights. The security and reliability of cryptographic infrastructures are therefore not merely technical matters, but legal preconditions for the continued validity of arts. 7 and 8 of the Charter of Fundamental Rights of the European Union, which guarantee the confidentiality of communications and the protection of personal data. In this sense, quantum preparedness designates the legal and institutional capacity to anticipate, absorb, and mitigate the disruptive effects of quantum technologies while ensuring their responsible incorporation into the Union's regulatory ecosystem, embodying a legal obligation of foresight in the form of a duty of technological diligence flowing from art. 2 TEU and the principle of sincere cooperation enshrined in art. 4(3) TEU.

This obligation has already begun to acquire operational relevance. The EU Cybersecurity Strategy and the 2030 Digital Compass identify the transition to post-quantum cryptography as a strategic priority, while the Cybersecurity Act (Regulation 2019/881) mandates the European Union Agency for Cybersecurity (ENISA) to monitor emerging threats and to promote crypto-agility, as the ability to adapt swiftly to new encryption standards. Recent analyses, including the RAND report *The Quantum Age and Its Impacts on Civil Justice System*,[5] warn that persisting in reliance on classical encryption without structural adaptation amounts to the accumulation of deferred vulnerabilities: a latent erosion of trust that will mature precisely when the technological asymmetry becomes irreversible. To neglect this trajectory would be to compromise, in advance, the Union's

[4] Cf. A. Castiglione – J.G. Esposito – V. Loia – M. Nappi – C. Pero – M. Polsinelli, *Integrating Post-Quantum Cryptography and Blockchain to Secure Low-Cost IoT Devices*, in *IEEE Transactions on Industrial Informatics*, 2024, 1674 ff.; A. Castiglione – J.G. Esposito – V. Loia – M. Nappi – C. Pero – M. Polsinelli, *Enhancing Trust of Deep Learning Models with Post-Quantum Digital Signatures*, in *Journal of Supercomputing*, 81, 2025, 1191 ff.; F.J. Zuiderveen Borgesius et al., *The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust*, in *Theoretical Inquiries in Law*, 2019, 291 ff.

[5] J. Dimarogonas – M. Grisé – M. Buenaventura – E. Silfversten – A.J. Lohn – J.M. Anderson – B. Saunders-Medina, *The Quantum Age and Its Impacts on the Civil Justice System*, RAND Corporation, RR-A1020-1, 2025, in *rand.org*.

promise of security and privacy.[6]

Yet, the problem transcends the technical dimension and strikes at the legal and geopolitical core of digital governance. Quantum computing compels a re-examination of the balance between innovation, freedom, and sovereignty in the digital order.[7] The values proclaimed in art. 2 TEU – respect for human dignity, freedom, democracy, equality, and the rule of law – require not only passive respect but active protection through legal measures capable of anticipating technological disruption. The Court of Justice of the European Union has consistently held that the rights of the Charter impose duties of action on public authorities whenever necessary to secure their effectiveness. From *Digital Rights Ireland* (C-293/12) to *Schrems II* (C-311/18),[8] the Court has clarified – in particular, in §§ 39–42 of the former and §§ 176–177 of the latter – that data protection entails a continuous responsibility to adapt safeguards to evolving risks. Quantum preparedness can thus be conceived as the next expression of this jurisprudential line: an obligation to preserve the material conditions under which digital rights can exist.

Several jurisdictions have already begun to articulate different models of quantum governance.[9] The United States has opted for security-oriented

---

[6] F. Fabbrini – E. Celeste – J. Quinn (eds.), *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Hart, 2021.

[7] Cf. F. Fabbrini – E. Celeste – J. Quinn (eds.), *Data Protection beyond Borders*, cit.

[8] ECJ, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* (2014), §§ 39–42; ECJ, C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* ("Schrems II") (2020), §§ 174–177. See also T. Ojanen, *Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance*, in *European Constitutional Law Review*, 10, 2014, 528 ff.

[9] R. Courtland, *China's 2,000-km Quantum Link Is Almost Complete*, in *spectrum.ieee.org*, 26 October 2016; E. Parker et al., *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*, RAND Corporation, February 2022, in *rand.org*; United States House Committee on Science, Space, and Technology, *Full Committee Hearing: Advancing American Leadership in Quantum Technology*, 118th Cong., 7 June 2023 (Statement of C. Merzbacher, Executive Director of Quantum Economic Development Consortium), in *democrats-science.house.gov;* University of Science and Technology of China (USTC), 中国科学技术大学成功实现最大规模的51比特量子纠缠态制备 *(USTC Successfully Realises the World's Largest 51-Qubit Entangled State Preparation)*, in 信息网络安全 *(Information Network Security)*, 23, 2023, 129; B.K. Williams, *The Innovation Race: US-China Science and Technology Competition and the Quantum Revolution*, Wilson Centre, in *wilsoncenter.org*, 25 October 2023; Z. Weilan, *US Blockades Won't Hinder China's Quantum Computing Technology Development: Leading Scientist*, in globaltimes.cn, 26 July 2024; University of Science and Technology of China (USTC), 中国科学技术大学构建国际首个基于纠缠的城域量子网络 *(USTC Builds the World's First Entanglement-Based Metropolitan Quantum Network)*, in 信息网络安全 *(Information Network Security)*, 24, 2024, 981; M. Wimmer – T.G. Moraes, *Quantum Computing, Digital Constitutionalism, and the Right to Encryption: Perspectives from Brazil*, in *Digital Society*, 1, 2, 2022, 12 ff.; A. Zornetta, *Quantum-safe Global Encryption Policy*, in *International Journal of*

pragmatism, as illustrated by the *Quantum Computing Cybersecurity Preparedness Act* (2022),[10] which instructs federal agencies to map and replace cryptographic infrastructures that will become vulnerable to quantum attacks. China, by contrast, is advancing a state-led project of technological sovereignty, combining substantial public investment with the creation of national standards in quantum communications and post-quantum encryption. Both approaches generate extraterritorial effects, often described as the *Washington effect* and the *Beijing effect*,[11] which influence how trust, interoperability and technical benchmarks are defined at the global level. Within this increasingly binary context, the European Union must articulate a path of its own, one that aligns scientific competitiveness with legal and fundamental rights safeguards, so that technological development is integrated into the rule of law rather than absorbed entirely by logics of national security or administrative control.

For the European Union, quantum preparedness therefore has a dual orientation. On the internal side, it means guaranteeing that the concrete enjoyment of rights and freedoms remains protected from the disruptive potential of quantum computing. On the external side, it means preserving strategic autonomy in setting the legal, ethical and technical parameters of the quantum era. Part of the recent doctrine has referred to this project as a *Quantum Acquis Planétaire,*[12] that is, a body of cooperative norms for quantum technologies built on principles of ethical universality and reciprocal limitation of power. This remains an aspirational construct, yet it indicates the possibility of a global governance arrangement that, in spirit, would resemble the 1968 Nuclear Non-Proliferation Treaty, converting technological rivalry into a more orderly and mutually comprehensible form of coexistence.

A comprehensive treatment of the legal and policy challenges posed by the quantum age, including the implications for intellectual property, national security, and civil liberties, is offered by Hoofnagle and Garfinkel.[13] The most systematic analysis to date of the relationship between information

Law and Information Technology, 32(1) 2024, art. eaae020.

[10] H.R. 7535 – *Quantum Computing Cybersecurity Preparedness Act*, 117th Cong., 2022, in *congress.gov*.

[11] V. Weber, *The Diffusion of Cyber Norms: Technospheres, Sovereignty, and Power*, DPhil thesis, University of Oxford, 2021, in *ora.ox.ac.uk*.

[12] M. Kop, *Establishing a Legal-Ethical Framework for Quantum Technology*, in *yjolt.org*, 30 March 2021; J. Mökander – P. Juneja – D. Watson – L. Floridi, *The US Algorithmic Accountability Act of 2022 vs the EU Artificial Intelligence Act: What Can They Learn from Each Other?*, in *Minds and Machines*, 32, 2022, 751 ff.; M. Kop, *Towards an Atomic Agency for Quantum-AI*, arXiv:2505.11515, 2025, 87 ff.

[13] C.J. Hoofnagle – S.L. Garfinkel, *Law and Policy for the Quantum Age*, Cambridge, 2022

security governance and human rights, encompassing both encryption and quantum computing, is provided by Van Daalen,[14] whose monograph develops a normative framework centred on the ECHR and the Charter, analysing the duties of States within what he terms the *information security cycle* – the continuous dynamic of *making and breaking* security measures. While that work focuses primarily on the assessment of existing governance through the lens of human rights compatibility, the present article adopts a complementary and *propositional* perspective, advancing concrete institutional proposals – the European Digital Code and the QSDP – designed to operationalise the Union's legal duty of quantum preparedness. The analysis that follows proceeds from this premise. It interprets quantum preparedness not as a speculative and captivating metaphor, but as a concrete manifestation of the Union's duty of foresight, interpreted as an obligation to preserve, within the quantum horizon, the unity between freedom, security, and technological progress that defines the European project. The following sections will demonstrate how this duty can be articulated through existing legal frameworks, from data protection and cybersecurity to digital services and market governance, and how it may culminate in the proposal of an integrated European Digital Code designed to ensure that the law itself becomes quantum-ready.

2. Legal Foundations: From Cryptographic Vulnerability to a Right to Adequate Encryption

2.1. Quantum Threats and Legal Responsibility

Quantum computing constitutes a stress test for the European Union. By undermining the technical foundations upon which data protection, privacy, and digital trust depend, it challenges the effectiveness of rights guaranteed under arts. 7 and 8 of the Charter of Fundamental Rights, ensured not only by the GDPR,[15] but also by the ePrivacy Directive (Directive 2002/58/EC), the Law Enforcement Directive (Directive 2016/680), and the Regulation applicable to EU institutions and bodies (Regulation 2018/1725). The duty to preserve these rights cannot be discharged merely through abstract recognition of the forthcoming adoption of quantum technologies; rather, it entails the proactive maintenance of the technical

[14] O. van Daalen, *From Encryption to Quantum Computing: The Governance of Information Security and Human Rights*, Springer Nature, 2024.

[15] Regulation (EU) 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, OJ L 119/1 (hereinafter "GDPR").

means that make them operational. In the digital environment, cryptography constitutes one essential dimension of the material substratum upon which legal guarantees and obligations rest. To be sure, privacy and data protection encompass a range of principles far broader than confidentiality alone, including transparency, purpose limitation, data minimisation, and accountability. Yet, without adequate encryption, even these broader safeguards lose much of their practical efficacy: a transparent and fair processing framework provides scant protection if the data it governs can be accessed through cryptanalysis. When the cryptographic substratum becomes obsolete, the rights it supports risk becoming nominal.

The capacity of quantum computers to execute Shor's and Grover's algorithms will render today's dominant public-key systems – RSA and elliptic-curve cryptography – computationally vulnerable. Long-lived or high-sensitivity datasets,[16] including genomic archives, diplomatic correspondence, and intellectual property registries, are particularly exposed to the so-called *harvest now, decrypt later* strategy, whereby adversaries intercept and store encrypted data today to decrypt them once quantum capability becomes available. Continued reliance on classical encryption effectively accumulates latent vulnerabilities whose consequences will materialize once the technological asymmetry becomes irreversible. The risk of unlawful access has been identified as a central factor in any measure affecting encryption;[17] by extension, the foreseeable erosion of classical encryption intensifies this obligation, since the risk of unlawful access is no longer hypothetical but structurally embedded in the current technological trajectory.

From a legal standpoint, this prospect gives rise to a positive obligation of foresight. Art. 2 TEU commits the Union to respect for human dignity, freedom, and the rule of law; those values are not static ideals but operative principles that impose duties of protection. The Court of Justice has repeatedly confirmed that where the effectiveness of a Charter right depends on technical safeguards, public authorities must act to ensure their adequacy. In *Digital Rights Ireland* (C-293/12, §§ 39-41) and *Tele2 Sverige* (C-

[16] P. Quinn – L. Quinn, *Big Genetic Data and Its Big Data Protection Challenges*, in *Computer Law and Security Review*, 34, 2018, 1000 ff.; M. Shabani – P. Borry, *Rules for Processing Genetic Data for Research Purposes in View of the New EU General Data Protection Regulation*, in *European Journal of Human Genetics*, 26, 2018, 149 ff.; P. Parmar et al., *A Review of DNA Cryptography: From a Data Protection Perspective*, in *Proceedings of the 2023 16th International Conference on Security of Information and Networks (SIN)*, IEEE, November 2023, 1 ff.

[17] O.L. Van Daalen, *The Right to Encryption: Privacy as Preventing Unlawful Access*, in *Computer Law & Security Review*, 49, 2023, 105804, 8 ff.; M. Mladenov – M. Galetin, *The Unbreakable Code Shaping Digital Resistance: A Right to Encryption in the Jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union*, in *Juridical Tribune – Review of Comparative and International* Law, 2025, 578 ff.

203/15, §§ 100-107), the Court invalidated data-retention regimes primarily because indiscriminate and general retention of data, without sufficient safeguards such as purpose limitation, oversight, and security guarantees, undermined the substance of the right to privacy and data protection. In *Schrems II* (C-311/18, §§ 176-177), it extended this logic to transatlantic data transfers, emphasizing the obligation to maintain an "essentially equivalent" level of protection.[18]

Similarly, the foreseeable breakdown of current encryption systems gives rise to a legal duty to adapt the protective infrastructure of the Union. Failure to act would amount to a structural omission in fulfilling the Union's mandate to safeguard the integrity and reliability of information. In this sense, quantum preparedness should be read as a responsibility to prevent the gradual weakening of fundamental rights caused by technological obsolescence, reframing what could be seen merely as technological updating into a problem of legal continuity and effectiveness.

2.2. Evolving Accountability and Technological Diligence

The principle of accountability, central to the GDPR and to the Union's data-governance architecture, requires that controllers and processors be able to demonstrate compliance with applicable standards of protection. Yet accountability cannot remain static while the threat landscape evolves. A dynamic accountability model must ensure that responsibilities – whether of public authorities, corporations, or professionals – evolve in parallel with technological progress.[19] This imperative is reinforced by the conceptualisation of information security as a continuous cycle of *making and breaking*: security measures are taken, circumvented, and then replaced by new measures, in an ongoing dynamic that renders any static notion of adequacy inherently insufficient.[20] If, as recent scholarship concludes, 'doing nothing to develop and adopt quantum-resistant encryption technologies would be quite likely to be a violation of Convention and the Charter',[21] the principle of dynamic accountability acquires immediate

[18] C. (J.) Li, *The Legal Implications for International Data Transfers in the Outsourcing Contracts following the CJEU's Schrems II Decision*, in *ssrn.com*,

[19] P.G. Thomas, *The Changing Nature of Accountability*, in *Taking Stock: Assessing Public Sector Reforms*, 2, 1998, 348 ff.; P.T.J. Wolters, *The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility?*, in *International Data Privacy Law*, 7, 2017, 165 ff.; R. Baldwin – M. Cave – M. Lodge, *Understanding Regulation: Theory, Strategy, and Practice*, Oxford, 2021.

[20] *Ibid.,* 1-3 and 346.

[21] *Ibid.*, 338.

urgency. In this respect, arts. 24, 25 and 32 GDPR – mandating, respectively, the responsibility of the controller, data protection by design and by default, and "appropriate technical and organizational measures" in light of the state of the art – already anticipates a regime of continual adaptation.[22] This same logic extends to quantum vulnerability: regulatory inertia would constitute a culpable omission of the State's duty of care toward citizens' informational integrity. An additional and complementary strategy is data minimisation: eliminating data that is no longer necessary constitutes a direct means of protection against quantum attacks,[23] since data that no longer exists cannot be decrypted. The GDPR's principles of purpose limitation and storage limitation (arts. 5(1)(b) and (e)) thus acquire renewed significance in the quantum horizon, operating as an independent safeguard alongside cryptographic resilience. The Union must therefore guarantee a timely transition to post-quantum cryptography (PQC) and to quantum-secure solutions such as quantum key distribution (QKD). Only through such adaptation can the present standard of protection avoid abrupt obsolescence once quantum computation becomes operational reality.

The dynamic interpretation of "appropriate" security measures already reflects an established regulatory understanding: the standard is not frozen in time but evolves with the state of the art. As quantum computing approaches operational maturity, this existing principle acquires new urgency, since what counts as a reasonable safeguard today will no longer be defensible once quantum computation becomes operational. Security agencies and research institutions, including ENISA, have emphasized that information intended to remain confidential for decades must already be protected by quantum-resistant algorithms. Failing to account for this time horizon would amount to negligence. Within the logic of risk-based regulation, proportionality is not a static balance but a moving equilibrium between evolving capabilities and foreseeable harms.

Comparable reasoning is emerging in other jurisdictions. In the United States, the *Quantum Computing Cybersecurity Preparedness Act 2022* obliges federal agencies to inventory and replace vulnerable cryptographic systems. The American Bar Association has further clarified that lawyers' ethical duties of competence and confidentiality include keeping abreast

[22] G. Almeida Teixeira – M. Mira da Silva – R. Pereira, *The Critical Success Factors of GDPR Implementation: A Systematic Literature Review*, in *Digital Policy, Regulation and Governance*, 21, 2019, 402 ff.; A. Selzer – D. Woods – R. Böhme, *An Economic Analysis of Appropriateness under Article 32 GDPR*, in *European Data Protection Law Review*, 7, 2021, 456 ff.; A. Selzer, *The Appropriateness of Technical and Organisational Measures under Article 32 GDPR*, in *European Data Protection Law Review*, 7, 2021, 120 ff.

[23] O. van Daalen, *From Encryption to Quantum Computing*, cit., 339.

of technological change relevant to client data protection.[24] Over forty State Bars have incorporated a "technology-competence" requirement into their codes of professional conduct, obliging practitioners to remain aware of both the benefits and the risks of emerging technologies.[25] By extension, failing to consider the quantum threat could soon amount to professional negligence.

These trajectories illustrate a common normative insight: accountability evolves as knowledge advances. The European Union should articulate its own conception of technological diligence, combining anticipatory pragmatism with the rights-oriented ethos of its legal order. Pursuant to art. 2 TEU, the Union's foundational values entail not only a duty to respect fundamental rights but also an obligation of due care in the face of foreseeable technological disruption.

2.3. From Technical Safeguards to a Right to Adequate Encryption

At the intersection of these developments lies the conceptual emergence of a right to adequate encryption. This right is not a new fundamental entitlement, but a corollary of the existing right to data protection under art. 8 of the Charter and the operational obligations of art. 32 GDPR. It denotes the individual's legitimate expectation that personal information be protected through cryptographic means proportionate to the technological state of the art, including quantum-resistant standards once these become available. Such a right would articulate, in legal form, the requirement that technological adequacy evolve with foreseeable threats. The scholarly foundations for this claim have been developed, in particular, by Van Daalen, who conceptualises the right to encryption as an expression

[24] American Bar Association, *Formal Opinion 498: Virtual Practice*, Standing Committee on Ethics and Professional Responsibility, 10 March 2021, in *lawnext.com;* American Bar Association, *Model Rules of Professional Conduct – Table of Contents*, 2025, in *americanbar.org.*

[25] R. Ambrogi, *Tech Competence: 40 States Have Adopted the Duty of Technology Competence*, in *lawnext.com,* 2021; R. Ambrogi, *N.J. Supreme Court Adopts Tech CLE Requirement But Declines to Adopt Duty of Tech Competence*, in *lawnext.com*, 16 April 2025. The New Jersey Supreme Court, in April 2025, adopted a mandatory continuing legal education (CLE) requirement obliging lawyers to complete at least one hour of technology-related training every two years, while expressly declining to amend Rule 1.1 of the Rules of Professional Conduct to incorporate a "duty of technology competence". This makes New Jersey the first state to impose a tech CLE requirement without formally recognising a duty of technological competence, diverging from over forty states that have followed the American Bar Association's Comment 8 to Rule 1.1.

of the right to privacy understood as the prevention of *unlawful access*,[26] and who, in a subsequent monograph, situates the governance of encryption within the broader trajectory from classical information security to quantum computing and human rights.[27] Van Daalen's framework, centred on the ECHR and the Charter, demonstrates that States bear positive obligations to safeguard a *vibrant encryption landscape* – one in which a wide range of cryptographic technologies, including user-controlled encryption, are available and actively promoted.[28] Within this framework, the risk of unlawful access operates as a central criterion for assessing the proportionality of any measure that restricts or weakens encryption. The quantum threat radicalises this logic: if current cryptographic schemes become vulnerable, the risk of unlawful access becomes not merely individual and contingent but systemic and foreseeable. It follows that the positive obligation to protect encryption must extend, a fortiori, to the obligation to anticipate and prevent cryptographic obsolescence through the timely adoption of quantum-resistant standards. The right to adequate encryption proposed here can thus be understood as the EU-law expression of the same normative imperative that Van Daalen articulates through the ECHR: a duty to ensure that the material conditions for the prevention of unlawful access remain effective in the quantum horizon.

The logic underpinning this right finds support in the Court's jurisprudence on positive obligations.[29] In *La Quadrature du Net* (Joined Cases C-511/18 and others, §§ 129-133),[30] the Court confirmed that ensuring the effectiveness of rights under arts. 7 and 8 entails not only refraining from interference but also maintaining sufficient guarantees against external intrusion. By extension, where the collapse of cryptographic security would nullify those guarantees, public inaction would itself constitute a breach.[31] The principle of technological equivalence – that protection must remain commensurate with risk – becomes an operational criterion of legal com-

[26] O.L. Van Daalen, *The Right to Encryption*, cit.; P.A.E. Davis, *A Right to Encryption in the European Union's Charter of Fundamental Rights*, in *Columbia Journal of European Law*, 30, 2024, 52 ff.

[27] O. van Daalen, *From Encryption to Quantum Computing*, cit.; O. van Daalen, *Developing a Human Rights Compatible Governance Framework for Quantum Computing*, in *Research Directions: Quantum Technologies*, 2024.

[28] O. van Daalen, *From Encryption to Quantum Computing*, cit., 325-326.

[29] ECJ, C-300/21, *Österreichische Post AG* (2023); ECJ, C-687/21, *MediaMarktSaturn* (2024), §§ 36–42; ECJ, C-340/21, *Natsionalna agentsia za prihodite (NAP)* (2023), §§ 26–30 and 42–46; ECJ, C-683/21, *Nacionalinis visuomenės sveikatos centras* (2025).

[30] ECJ, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others v Premier ministre and Others*, §§ 123–133.

[31] ECJ, C-470/21, *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* (2024); ECJ, C-129/21, *Proximus NV v. Gegevensbeschermingsautoriteit* (2022).

pliance. Recognizing a right to adequate encryption would have two major implications. First, it would guide regulatory interpretation: the adequacy of technical measures would be assessed not only ex post, by reference to current practice, but also ex ante, against foreseeable quantum capabilities. Second, it would establish a normative benchmark for institutional conduct: the Union and the Member States would be bound to ensure a timely migration toward post-quantum cryptography within their administrative systems and critical infrastructures.

This evolution is already implicit in policy instruments and binding norms, such as the Cybersecurity Act,[32] the NIS2 Directive (Directive 2022/2555), which imposes cybersecurity risk-management measures and reporting obligations across essential and important entities, and the Cyber Resilience Act (Regulation 2024/2847), which establishes horizontal cybersecurity requirements for products with digital elements. The EU Cybersecurity Strategy (2020) and the 2030 Digital Compass identify crypto-agility as a dimension of resilience, while ENISA's *Advancing Cryptographic Agility* report (2024) recommends that regulatory bodies incorporate transition planning into compliance obligations (see further infra, note 55). The recognition of a right to adequate encryption would simply render explicit what these instruments presuppose: that the protection of digital rights is inseparable from the capacity of law to evolve with technology.[33]

From a comparative perspective, the transatlantic and Chinese experiences expose divergent articulations of the same underlying principle.[34] In

[32] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, OJ L 151/15; ENISA, *Post-Quantum Cryptography: Current State and Quantum Mitigation*, in *enisa.europa.eu*, 3 May 2021; European Commission, *EU Reinforces Its Cybersecurity with Post-Quantum Cryptography*, in *digital-strategy.ec.europa.eu,* 23 June 2025.

[33] Cf. ECJ, C-817/19, *Ligue des droits humains ASBL v Conseil des ministres* (2022), where the CJEU reaffirmed that data processing systems for the purposes of preventing and suppressing crime must ensure effective protection of the fundamental rights enshrined in arts. 7 and 8 of the Charter of Fundamental Rights of the EU, in particular against interference resulting from the automated collection, evaluation, and retention of PNR data. Such systems must adopt appropriate technical and organisational measures to protect the security, confidentiality, and integrity of the data, ensuring transparency, human oversight, non-discrimination, and allowing the effective exercise of the right to a judicial remedy. The Court emphasised the need for these safeguards to be constantly updated in light of technical developments and emerging risks, but did not explicitly mention the principle of future-proof protection nor make a direct reference to quantum-resilient infrastructures; instead, it emphasised that the safeguards must be interpreted in light of current and future risks and technologies in the protection of data processed for public security purposes.

[34] Cf. G. Resta – V. Zeno-Zencovich (eds.), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, 5, Rome, 2016; B. Bessone, *Oltre le censure della*

the United States, even in the absence of an explicit right to privacy and personal data protection, the awareness of quantum risk has prompted executive action: the 2022 Presidential Memorandum on National Security instructed federal agencies to identify vulnerable cryptographic systems and to plan their substitution.[35] Professional sectors, from law to healthcare, will incorporate quantum-readiness into their technological due diligence. The United States has increasingly subjected quantum technologies to export controls, including through the Commerce Control List and the Wassenaar Arrangement, reflecting the strategic significance attributed to quantum computing as a foundational technology for national security. China, by contrast, interprets the challenge as a vector of strategic assertion.[36] Through massive public investment in quantum technologies and

CGUE: il Data Privacy Framework e la nuova decisione di adeguatezza per il trasferimento dei dati personali verso gli Stati Uniti, in *Rivista di Diritto dei Media*, 2, 2024, 62 ff.

[35] The White House, *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems* (NSM-10), in *bidenwhitehouse.archives.gov*, 4 May 2022.

[36] State Council, *National Medium- and Long-Term Science and Technology Development Plan (2006–2020)*, in gov.cn, 2006; Geng Xi, *Interview with Chen Zenghing of the University of Science and Technology of China: Interpretation of Quantum Communication That "Will Not Be Stolen"*, in *Beijing Science and Technology Daily*, 11 November 2008; State Council, *Medium- and Long-Term Plan for the Construction of Major National S&T Infrastructure*, in gov.cn, 23 February 2013; Xi Jinping, *Deepen the Reform of the Science and Technology System and Enhance the Vitality of Scientific and Technological Innovation*, in *Xinhua*, 17 July 2013; *Xi Jinping Hosted the Ninth Study Session of the Politburo of the Central Committee*, in *People's Daily*, 1 November 2013; *The Wall Has Ears: Eavesdropping, Invisible Radio Waves*, in *People's Daily*, 8 November 2013; Xi Jinping, *Explanation of the Recommendations Provided by the Central Committee of the CCP on the Formulation of the 13th Five-Year Plan on the National Economic and Social Development*, in *Xinhua*, 3 November 2015; *Outline of the 13th Five-Year Plan for National Economic and Social Development*, in *Xinhua*, 17 March 2016; *The Launch of Quantum Satellites Will Give Birth to a Market of 100 Billion in the Communication Industry Chain*, in *People's Daily*, 16 August 2016; V. Zhou, *China's Orbiting Quantum Satellite Links with Ground Stations*, in *South China Morning Post*, 24 September 2016; State Council, *Outline of the National Information Technology Development Strategy*, in gov.cn, 19 December 2016; Chinese Academy of Sciences, *13th FYP for the Development of the Chinese Academy of Sciences*, 2016; Ministry of Science and Technology, *13th FYP for National Key Basic Research and Development Program*, in *most.gov.cn*, 8 June 2017; S. Chen, *Chinese Satellite Makes Breakthrough in Quantum Communication*, in *South China Morning Post*, 16 June 2017; University of Science and Technology of China, *The National Quantum Confidential Communication "Beijing–Shanghai Trunk Line" Project Passed the General Technical Acceptance*, in *quantum.ustc.edu.cn*, 4 September 2017; E.B. Kania – J.K. Costello, *Quantum Hegemony? China's Ambitions and the Challenge to US Innovation Leadership*, Center for a New American Security, in *cnas.org*, 12 September 2018; J. Whalen, *China's Top Quantum Scientist Has Ties to the Country's Defense Companies*, in *The Washington Post*, 26 December 2019; S. Chen, *Chinese Scientists Develop Portable Quantum Satellite Communication Device*, in *South China Morning Post*, 3 January 2020; S. Chen, *China Is Developing Drones That Use Quantum Physics to Send Unhackable Messages*, in *South China Morning Post*, 10 January 2020; *During the 24th Study Session of the Politburo of the Central*

the deployment of pilot quantum-communication networks such as the Beijing–Shanghai backbone, the Chinese state promotes quantum cryptography as a sovereign capability and a means of consolidating national control. This approach elevates technological mastery over the protection of individual rights.

The European Union must instead articulate a third path: adopting the foresight and decisiveness of the American model while orienting it toward the protection of rights rather than mere securitization – understood, in the sense developed by the Copenhagen School, as the discursive process through which an issue is framed as an existential threat warranting exceptional measures[37] – and investing in quantum technologies with the ambition of the Chinese strategy yet for the purpose of enhancing freedom, not control. Accordingly, the evolution of cybersecurity obligations under art. 32 GDPR and related jurisprudence points toward the crystallization of a right to adequate encryption,[38] a right inherent in, and derivative from, the right to data protection itself. Citizens and enterprises could claim that their data be protected through cryptographic means commensurate with the technological state of the art. It signifies the individual's legitimate expectation that personal information be secured through cryptographic means proportionate to the technological state of

Committee, Xi Jinping Emphasized the Importance of Promoting the Development of Quantum Technology, in *Xinhua*, 17 October 2020; C. Feng, *China Telecom Launches Quantum Encrypted Phone Calls on Smartphones in a New Pilot Programme*, in *South China Morning Post*, 7 January 2021; L. Zhen, *China's Experiment in Quantum Communication Brings Beijing Closer to Creating a Hack-Proof Network*, in *South China Morning Post*, 9 January 2021; State Council, *Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035*, in gov.cn, 13 March 2021; S. Chen, *China Launches New Satellite in "Important Step" towards Global Quantum Communications Network*, in *South China Morning Post*, 27 July 2022; E. Parker et al., *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*, RAND Corporation, RR-A869-1, 2022, in *rand.org*; A. Shalal – D. Brunnstrom, *US and China Diplomats Communicating, But Not Militaries*, in *Reuters*, 17 February 2023; Qian Tongxin, *China Is Developing Medium-High Orbit Quantum Satellites*, in *Yicai*, 4 March 2023; US Department of Energy Office of Science Advanced Scientific Computing Research, *Scientific Enablers of Scalable Quantum Communications*, in *science.osti.gov*, 18 April 2023; National Institute of Standards and Technology, *Quantum Communications and Networks*, in *nist.gov*; National Institute of Standards and Technology, *Post-Quantum Cryptography*, in *csrc.nist.gov*; R. Lemos, *Satellite Hacking*, in *Defense One*; National Security Agency, *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*, in *nsa.gov*.

[37] B. Buzan – O. Wæver – J. de Wilde, *Security: A New Framework for Analysis*, Boulder, 1998.

[38] O.L. Van Daalen, *The Right to Encryption*, cit.; O. van Daalen, *From Encryption to Quantum Computing*, cit. See also V. Ciriani et al., *Fragmentation and Encryption to Enforce Privacy in Data Storage*, in *Proceedings of the European Symposium on Research in Computer Security*, Springer, 2007; S. Bellamkonda, *Securing Data with Encryption: A Comprehensive Guide*, in *International Journal of Communication Networks and Security*, 11, 2019, 248 ff.

the art, including quantum-resistant standards.

3. Toward an Integrated Framework for the EU Digital Acquis in the Quantum Age

3.1. The Need for Regulatory Integration

The growing complexity of the European digital acquis has generated an increasingly fragmented legal landscape. Over the past decade, the Union has adopted a series of major legislative instruments – the General Data Protection Regulation (GDPR), the Digital Services Act (DSA),[39] the Digital Markets Act (DMA),[40] the Data Governance Act (DGA),[41] the NIS2 Directive,[42] the Cyber Resilience Act (CRA),[43] and the eIDAS2 Regulation,[44] *inter alia* – each addressing discrete aspects of the digital ecosystem. While these frameworks collectively advance the Union's strategic goal of technological sovereignty, their proliferation risks undermining coherence, accessibility, and legal certainty.[45] The Union's quest for digital sovereignty

[39] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277/1.

[40] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act), OJ L 265/1.

[41] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152/1.

[42] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), OJ L 333/80.

[43] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L 307/23.

[44] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2 Regulation), see G. Comandé – M. Varilek, *The Many Features Which Make the eIDAS 2 Digital Wallet either Risky or the Ideal Vehicle for the Transition to Post-Quantum Encryption*, in *Computer Law and Security Review*, 54, 2024, art. 106022.

[45] *Ex multis, V. Zeno-Zencovich, Artificial Intelligence, Natural Stupidity and Other Legal Idiocies,* in *Rivista di Diritto dei Media,* 1, 2024, 9 ff.; M. Pathak*, Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act,* in *European Data Protection Law Review,* 10, 2024, 43 ff.

is itself increasingly intertwined with the capacity to govern quantum innovation in a manner consistent with its legal identity.[46]

This dispersion is particularly problematic when emerging technologies such as quantum computing introduce systemic risks that cut across regulatory domains. Quantum vulnerability, for instance, simultaneously affects data protection, cybersecurity, digital identity, and trust services. Addressing it through isolated amendments or ad hoc instruments would multiply overlaps and inconsistencies. The problem is therefore not the absence of legislation but its compartmentalization.

To meet this challenge, the Union should pursue a process of principled coordination aimed at ensuring, at a minimum, the internal coherence and forward compatibility of its digital legislation. The objective need not be the wholesale merger of disparate regulatory domains – whose subject matters, from competition law to cybersecurity to digital identity, are legitimately diverse and respond to distinct policy rationales – but rather the alignment of shared horizontal principles, particularly those relating to quantum preparedness and cryptographic security.[47] Such a process of normative alignment would be grounded in the Treaties and aimed at rationalizing the interfaces between existing instruments. The objective is not expansion but alignment: ensuring that the legal architecture of the internal market remains functional, intelligible, and technologically adaptive.[48]

3.2. A European Digital Code: Legal Foundations and Design

Within the framework of the Digital Package on Simplification, a European Digital Code should be conceived as a *consolidating framework*, not as an additional layer of regulation. Its legal feasibility rests upon two complementary treaty bases.

First, art. 114 TFEU empowers the Union to adopt measures for the

[46] P. Vogiatzoglou, *The EU's Quest for Digital Sovereignty: A Matter of Quantum Innovation?*, in *Digital Society*, 4, 2025, 16.

[47] European Commission, *Simplification: Digital Package and Omnibus*, Better Regulation Portal, Initiative 14855, in *ec.europa.eu*.

[48] Typical examples include medical and biometric records, genetic profiles, long-term financial or legal data, and information concerning minors preserved until adulthood. For such data, the ordinary safeguards of Article 32 are insufficient; a differentiated regime of obligations is required to ensure continuity of protection across technological paradigms, see L. Jančiūtė, *Cybersecurity in the Financial Sector and the Quantum-safe Cryptography Transition: In Search of a Precautionary Approach in the EU Digital Operational Resilience Act Framework*, in *International Cybersecurity Law Review*, 6, 2025, 145 ff.

approximation of laws to ensure the establishment and functioning of the internal market, particularly where regulatory fragmentation impedes cross-border digital services. Second, art. 16 TFEU provides the competence to regulate the protection of personal data. Together, these provisions supply a robust foundation for a codified instrument harmonizing the principles, definitions, and enforcement mechanisms of the Union's digital legislation.

A Digital Code established under these competences would not supersede existing acts but *restructure* them into a coherent framework. Each major regulation or directive (GDPR, DSA, DGA, NIS2, CRA, and eIDAS2) would retain its specific material scope but operate within a unified conceptual and terminological grammar. Common definitions (e.g., of "data," "controller," "digital service") would be aligned where genuine interpretive inconsistencies undermine legal certainty, while recognising that some definitional variations across instruments are contextually justified: for instance, the notion of "significant incident" under the NIS2 Directive appropriately reflects risk-management concerns specific to critical infrastructure, which differ from the product-safety logic that governs the same concept under the Cyber Resilience Act. Cross-references between acts would be rationalized, and overlapping obligations would be harmonized through a single interpretative matrix.

From an institutional perspective, the Code could be established through a two-tier legislative instrument: a first tier would define a framework regulation codifying shared principles and horizontal obligations (privacy-by-design, cybersecurity-by-design, algorithmic transparency, quantum safety); and a second one would set up series of sectoral annexes corresponding to existing instruments, to be progressively aligned and updated through delegated acts under art. 290 TFEU and, where uniform conditions of implementation are required, through implementing acts under art. 291 TFEU. Such a structure would preserve the autonomy of sector-specific regimes while introducing legal interoperability among them. It would also enable future integration of emergent fields – quantum communication, artificial intelligence, or digital identity – without requiring new legislative packages.

It must be acknowledged that the feasibility of such a comprehensive codification is open to legitimate objection. The legislative instruments encompassed by the proposed Digital Code address materially heterogeneous domains – from competition and platform governance to data protection and cybersecurity – and the very notion of "digital law" as a unitary analytical category remains contested. Nevertheless, the category retains an operative function for the purposes of codification insofar as it identifies a corpus of legislative instruments that share specific structural features – obligations of algorithmic transparency, data protection by

design, interoperability, and now crypto-agility – which functionally distinguish them from non-digital legislation. The European Commission's Digital Package on Simplification itself employs this very category as an operational tool, confirming that, however contested in theoretical terms, "digital law" serves a concrete regulatory purpose. To address these legitimate concerns, the present proposal adopts a two-stage architecture. The first stage (de lege ferenda) is immediately practicable and independent of codification: it encompasses the adoption of a dedicated Quantum Act, or the insertion of horizontal obligations of crypto-agility into each existing instrument through targeted revisions during their scheduled review cycles. Either approach could deliver substantial gains in quantum preparedness without requiring the political and institutional effort of a full-scale codification, and both can proceed autonomously from – and in advance of – any codification process. This article does not conceive codification as a precondition for its operative recommendations; the Quantum Act and the sectoral interventions proposed herein retain their full validity regardless of whether the broader codification project materialises. The second stage is prospective: the progressive codification of the digital acquis into a coherent framework, toward which the process of sectoral alignment tends as a regulatory horizon. The institutional design outlined above – the framework regulation, the sectoral annexes, the mechanisms of delegated and implementing acts under arts. 290 and 291 TFEU – pertains to this second stage. It constitutes a reference architecture whose value lies not in its immediate enactability but in the discipline it imposes on the incremental process of legislative adaptation: each sectoral revision, each delegated act, each new standard would be assessed for its contribution to overall coherence, guided by the Code's underlying logic of principled integration. The normative case for this horizon rests on the observation that quantum vulnerability is inherently cross-cutting: it simultaneously affects data protection, cybersecurity, digital identity, and trust services, so that a purely sectoral approach – however effective within each domain – risks reproducing the very incoherences and gaps that the paper identifies. Crucially, the Code would embody the Union's duty of legislative coherence, an expression of the general principle of good administration under art. 41 of the Charter. By providing a single, systematic framework for digital regulation, the EU could enhance legal certainty for economic actors and the intelligibility of digital rights for citizens, echoing the logic of previous codifications, such as the Consumer Code and the Customs Code, which have transformed dispersed legislation into accessible and coherent normative systems.

3.3. Anticipatory Governance: Operational Mechanisms for Quantum Readiness

The integration of quantum preparedness into the Digital Code would translate the obligation of technological foresight into a concrete legal mechanism. Whether through a dedicated Quantum Act – which, as argued above, represents an immediately viable first stage – or through the incorporation of quantum-safe requirements into the Code's horizontal provisions, the Union would ensure that existing rights and obligations evolve in synchrony with scientific progress.

Under the GDPR component and via interpretative guidance or delegated regulation, for example, art. 32 on "security of processing" could be clarified to specify that adequacy of technical measures includes resistance to foreseeable quantum attacks. The NIS2 and CRA segments could adopt consistent definitions of quantum risk and crypto-agility, establishing common assessment methodologies across sectors. The eIDAS2 and trust-services components could mandate the recognition of post-quantum signature algorithms such as CRYSTALS-Dilithium, CRYSTALS-Kyber,[49] SPHINCS+, and XMSS.

This anticipatory capacity could be operationalized through a European Committee for Quantum Security and Technological Standards, coordinated by ENISA and reporting annually to the Commission and Parliament. The Committee would maintain a unified repository of quantum-safe algorithms, certification benchmarks, and transition guidelines applicable across the Code's domains. This mechanism would embed *technological vigilance* within the law, ensuring that regulatory obsolescence does not undermine the Union's values.

The integration of such a system within the Digital Code would also satisfy the requirements of proportionality and subsidiarity under art. 5 TEU. Member States would retain primary responsibility for implementation and enforcement, while the Union would ensure coherence, interoperability, and minimum harmonization standards. The aim is a federalized model of digital governance, in which the Union defines common safeguards and methodologies, leaving operational details to national authorities within a harmonized framework.

[49] E.g. CRYSTALS-Kyber for encryption and CRYSTALS-Dilithium for digital signatures. See J.W. Bos – L. Ducas – E. Kiltz – T. Lepoint – V. Lyubashevsky – J.M. Schanck – P. Schwabe – G. Seiler, *CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM*, in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 2018, 353 ff.; L. Ducas et al., *CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme*, in *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018, 1, 238 ff.; J. Shurson, *A European Right to End-to-End Encryption?*, in *Computer Law and Security Review*, 55, 2024, art. 106063

4. The Quantum Secure Data Protocol: Legal Design and Institutional Architecture

4.1. Quantum-Secure Adequacy: Foundations and Normative Design

Within the framework of the proposed European Digital Code, the Quantum Secure Data Protocol (QSDP) – a legally binding procedural framework designed to establish, validate and periodically update quantum-secure cryptographic standards applicable across the Union's digital legislation – should not be envisaged as a stand-alone regulatory instrument, but rather as an annexed and harmonized component that operationalizes the Union's duty to preserve the integrity of digital infrastructures in the quantum era. [50] Its function would be to translate the principle of technological foresight into a normative architecture capable of ensuring coherence, interoperability, and resilience across the Union's digital legislation.

The legal foundation of the QSDP may be found in the combined reading of arts. 114, 16 and 290 of the Treaty on the Functioning of the European Union. art. 114 provides the competence to approximate laws in order to secure the functioning of the internal market, a competence that naturally encompasses the harmonization of cryptographic standards whenever fragmentation jeopardizes the circulation of data or the provision of cross-border digital services. Art. 16, by contrast, anchors the entire operation in the dimension of data protection, ensuring that the regulatory pursuit of interoperability does not come at the expense of individual rights. arts. 290 and 291 TFEU enable the Commission, respectively, to adopt delegated acts supplementing or amending non-essential elements of legislative instruments, and implementing acts where uniform conditions of implementation are required; through these mechanisms, the QSDP could be periodically updated to reflect the evolving state of scientific knowledge without requiring new legislative procedures.

The normative design of the QSDP should avoid the technocratic temptation to legislate algorithms. The goal is not to prescribe a specific cryptographic formula but to establish a legally binding procedure through which certain standards acquire the status of quantum-secure adequacy within the Union. Compliance with the Protocol would constitute prima facie evidence that the relevant entity has satisfied the cryptographic

[50] M. Taleby Ahvanooey et al., *Future of Cyberspace: A Critical Review of Standard Security Protocols in the Post-Quantum Era*, in *Computer Science Review*, 57, 2025, art. 100738; K. Csenkey – N. Bindel, *Post-quantum Cryptographic Assemblages and the Governance of the Quantum Threat*, in *Journal of Cybersecurity*, 9(1) 2023, art. tyad001.

component of the "appropriate technical and organisational measures" required under the applicable sectoral legislation – from data protection to cybersecurity, trust services, and digital platforms. The presumption is thus circumscribed to the cryptographic dimension of sectoral obligations, not to their entirety: it does not discharge the entity from its broader duties of data protection or cybersecurity, but establishes that the specific requirements of quantum-secure encryption have been met. Such a presumption would, at the same time, foster market confidence and reduce administrative complexity by providing a single European benchmark for encryption adequacy.

At the technical level, the Protocol would refer to families of post-quantum cryptographic algorithms, such as those standardized by NIST and evaluated within ETSI's Quantum-Safe Cryptography Group, [51] but it would do so only by reference and without embedding them directly into the text of the law. These design choices find independent support in the emerging literature on human-rights-compatible quantum computing governance, which emphasises the need to mandate the adoption of PQC through regulation, to require its use in public procurement, to eliminate intellectual property barriers that hinder the diffusion of quantum-resistant standards, and to promote adoption through education and standardisation campaigns. This approach preserves technological neutrality and ensures that the Union's regulatory order remains adaptable to scientific progress. A clarification is in order regarding the scope and ambition of the Protocol. The QSDP is not conceived as a single monolithic standard that absorbs or replaces the multiplicity of sectoral standards already in existence or under development – a task that would be neither practicable nor desirable, given that the Cyber Resilience Act alone has generated over forty separate standardisation requests, each addressing distinct product categories and risk profiles. Rather, the Protocol operates on a different plane: it defines a horizontal layer of minimum cryptographic requirements – principally, reference families of quantum-resistant algorithms, mandatory crypto-agility obligations, and key-management principles – that cut across and complement the sectoral standards without pretending to subsume them. The complexity of the current standardisation landscape is, in this perspective, an argument *in favour of* a coordinating framework rather than against it. Precisely because dozens of sectoral standards coexist, a transversal cryptographic baseline is needed to ensure that quantum-readiness requirements are coherent across domains, avoiding the

[51] Commission mandates to ETSI and CEN/CENELEC issued under the European standardisation framework, pursuant to Regulation (EU) No 1025/2012. ETSI: European Telecommunications Standards Institute; CEN: European Committee for Standardization; CENELEC: European Committee for Electrotechnical Standardization.

risk that different sectors adopt incompatible or inconsistent post-quantum transition paths. The QSDP thus functions as the connective tissue between sectoral standards, not as their replacement: a modular family of quantum-related harmonised principles, organised around shared security objectives, that reduces fragmentation while respecting the autonomy of each regulatory domain.

A clarification of institutional design is warranted at this juncture. The QSDP is conceptually and operationally independent of the codification project outlined in the preceding section. The Protocol could be adopted as a free-standing instrument – a regulation on quantum-secure cryptographic standards founded upon arts. 114 and 16 TFEU – or as an annex inserted into each of the existing sectoral instruments (GDPR, NIS2, CRA, eIDAS2) through targeted legislative revisions. Its placement within the European Digital Code represents the optimal solution from the standpoint of normative coherence, but it is not a precondition for its effectiveness. This institutional modularity is a deliberate feature of the proposal, not a weakness: it ensures that the transition to quantum-safe cryptography can proceed regardless of the political trajectory of the broader codification process, while preserving the option of subsequent integration into a unified framework.

At the organizational level, the Protocol would require entities subject to the Code (controllers, processors, service providers, and public authorities) to maintain documented policies for algorithmic transition, key management, and cryptographic renewal, in accordance with the principle of crypto-agility already endorsed by ENISA in its 2024 report *Advancing Cryptographic Agility*.[52] At the institutional level, a European Committee for Quantum Security Standards, coordinated by ENISA and composed of representatives from the Commission, the Member States, and recognized standardization bodies, would be entrusted with maintaining the QSDP annex, approving updates, and advising supervisory authorities on its interpretation. In this way, the Protocol would embody a model of delegated self-correction, ensuring that the legal order evolves in synchrony with technological change.

The QSDP would operate horizontally within the European Digital Code, serving as a common reference for the interpretation and implementation of sector-specific obligations. In the domain of data protection, compliance with the Protocol would constitute prima facie evidence that the controller or processor has implemented "appropriate technical and organisational measures" within the meaning of art. 32 GDPR. In cybersecurity and product-security regulation, adherence to the QSDP would demonstrate conformity with the cybersecurity risk-management meas-

[52] ENISA, *Advancing Cryptographic Agility*, 2024.

ures and incident-reporting obligations imposed by the NIS2 Directive and the Cyber Resilience Act, while in the context of trust services, it would define the quantum-secure parameters applicable to qualified electronic signatures and identity credentials pursuant to eIDAS2. The same logic could extend to data-sharing and platform-governance frameworks, such as the DGA and DSA, where the Protocol would establish a baseline for encryption, key management, and risk assessment.

Rather than multiplying certifications and overlapping conformity assessments, the QSDP would aim at rationalising them. Its adoption would promote a modular family of quantum-related harmonised standards, organised around shared security principles, which could reduce fragmentation without requiring a single monolithic standard purporting to cover all essential cybersecurity requirements across all sectors.[53] Such a modular approach would acknowledge that quantum-secure adequacy may differ in its technical parameters depending on the sectoral context, while ensuring that the underlying principles of cryptographic resilience and transition planning remain uniform. The distinction between harmonised standards and certification schemes is crucial: the former define the technical specifications against which compliance is assessed, while the latter establish the procedures through which conformity with those specifications is verified. The QSDP would operate primarily at the level of standards-setting, while leveraging existing certification frameworks – such as those established under the Cybersecurity Act – to verify compliance. This system would significantly enhance legal certainty for operators while reducing regulatory costs and strengthening the internal market's technological coherence. Public authorities and critical infrastructures could, in turn, incorporate QSDP conformity into public procurement procedures, thereby aligning market incentives with the Union's obligation to safeguard technological sovereignty.

The Protocol's international dimension would be equally essential. As an annex of the European Digital Code – or, in its absence, as a free-standing instrument or as an annex to existing sectoral legislation – the QSDP would articulate a European profile of global interoperability. It would build upon existing cooperation within international standardization fora, including ISO/IEC JTC 1/SC 27, ITU-T, and ETSI, while promoting reciprocal recognition of quantum-secure profiles with strategic partners such as the United States and Japan. By doing so, the Union would avoid the formation of competing "quantum blocs" characterized by incom-

[53] Cf. P.G. Chiara, *Towards a Right to Cybersecurity in EU Law? The Challenges Ahead*, in *Computer Law and Security Review*, 53, 2024, 1 ff.; V. Papakonstantinou, *Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?*, in *Computer Law and Security Review*, 44, 2022.

patible standards, and at the same time it would assert its capacity to project normative influence into the governance of emerging technologies. Cooperation with non-European actors would thus coexist with a strong commitment to autonomy, particularly in the promotion of open-source, verifiable implementations developed within the Union and the cultivation of a domestic industrial base for cryptographic hardware and random-number generation.

The legal meaning of the QSDP ultimately lies in its ability to translate values into infrastructure. By embedding quantum preparedness within the European Digital Code, the Union would render tangible its duty to act with foresight in the face of technological transformation. The Protocol would guarantee that the rights protected by arts. 7 and 8 of the Charter remain materially effective even when the computational paradigms that sustain them evolve. It would also reaffirm the Union's vocation to govern technology through law, demonstrating that legality and innovation are not opposing forces but complementary expressions of the same project. In this perspective, the QSDP becomes not only an annex of the Digital Code, but an emblem of the European commitment to a lawful digital future, one in which the endurance of rights depends on the adaptability of the legal order itself.

4.2. Normative Coherence in the EU Digital Acquis

The integration of quantum preparedness within the European Digital Code requires that the normative principles underlying the Digital Services Act and the Data Governance Act be interpreted and, where necessary, progressively adapted in light of the QSDP. Both instruments were conceived as pillars of the Union's emerging regulatory framework for the digital environment[54] – a framework that some scholars have begun to analyse through the lens of "digital constitutionalism":[55] the DSA governing the accountability of platforms and intermediaries in the digital public sphere, the DGA establishing the conditions for trustworthy data sharing and intermediation. Yet neither instrument, in its current formulation, addresses the implications of quantum computing for the confidentiality, integrity, and authenticity of information flows on which their respective architectures depend.

By incorporating the QSDP into their operative logic, these frameworks

[54] On the principle of technological foresight, see the Commission's Communication *Shaping Europe's Digital Future*, COM(2020) 67 final.

[55] G. De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022.

can evolve from static regulatory instruments into dynamic systems of technological due diligence. The premise is simple but profound: if encryption, authentication, and key management are the infrastructural foundations of trust, then the obsolescence of these mechanisms – foreseeable in the quantum horizon – entails not merely a technical deficiency but a potential breach of the legal duties of care that these Acts impose on their subjects.

Within the DSA, the embedding of quantum preparedness manifests itself primarily through the principle of platform accountability. [56] Art. 34 of the Regulation obliges very large online platforms and search engines to identify and mitigate systemic risks, including those that affect the integrity of the information environment and the protection of fundamental rights. Although the provision was drafted with disinformation and algorithmic opacity in mind, its underlying logic applies equally to technological vulnerabilities capable of compromising data integrity and user security. The capacity of a platform to ensure that user communications remain confidential and authentic against foreseeable quantum attacks constitutes, in this sense, a dimension of systemic risk management. Interpreting the DSA in coherence with the Digital Code and the QSDP would therefore entail recognizing that the implementation of quantum-secure encryption and verification mechanisms is part of the due diligence obligations incumbent upon intermediaries. The Commission, acting under art. 87 DSA, could adopt delegated acts or guidelines clarifying that adherence to the QSDP constitutes a presumption of compliance with the systemic-risk mitigation duties established by the Regulation.

The same reasoning applies, *mutatis mutandis*, to the Data Governance Act. The DGA's central aim is to foster trust in data intermediaries by ensuring that data sharing occurs under conditions of neutrality, security, and transparency. This architecture presupposes the reliability of the cryptographic and authentication processes that protect both personal and industrial data. Quantum vulnerability directly undermines these premises, exposing data intermediation to risks of unauthorized access, manipulation, or decryption. Embedding the QSDP into the DGA would thus amount to safeguarding the very condition of possibility of data governance: the credibility of the technological infrastructure that sustains it.

In practical terms, data intermediaries registered under the DGA could be required to demonstrate conformity with the QSDP as part of their technical compliance assessments. Such conformity would evidence that their

[56] Regulation (EU) 2022/2065 (Digital Services Act), cit., recital 3. The DSA imposes obligations on providers of digital services — particularly Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) — to identify, assess, and mitigate systemic risks associated with their operations.

systems incorporate encryption schemes resilient to foreseeable quantum attacks and that they maintain algorithmic transition plans consistent with the principle of crypto-agility. This would not impose new obligations but rather specify the existing duty – already implicit in art. 12 DGA – to implement adequate technical and organizational measures ensuring the protection and confidentiality of data.

This imperative is textually reinforced elsewhere in the Act. Art. 12(j) DGA requires data intermediation services providers to put in place "adequate technical, legal and organisational measures" to prevent the transfer of or access to non-personal data that is unlawful under Union or national law, while art. 12(l) DGA obliges them to take necessary measures to ensure "an appropriate level of security for the storage, processing and transmission of non-personal data," and the highest level of security for competitively sensitive information.[57] In the quantum horizon, however, even these techniques depend upon key-exchange systems that must evolve toward quantum-resilient configurations. Beyond the DGA's regime for data intermediation, business-to-government (B2G) data sharing is governed by Chapter V (arts. 14–22) of the Data Act (Regulation (EU) 2023/2854), which obliges data holders to make data available to public sector bodies, the Commission, the ECB and Union bodies on the basis of an exceptional need – whether arising from public emergencies such as natural disasters, pandemics or major cybersecurity incidents, or from specified tasks of public interest that cannot otherwise be discharged. The two instruments form complementary components of the European data strategy, with the European Data Innovation Board – established under art. 29 DGA – contributing cross-cutting interpretative guidance on the governance of the Union's data economy. Within this architecture, the integration of the QSDP would supply a uniform framework for secure key exchange and data transmission between data holders and the public authorities acting as trusted custodians. Emerging technologies such as quantum key distribution (QKD) offer paradigmatic examples of how cryptographic innovation can be channeled into compliance architectures rather than remaining confined to research laboratories.

The normative coherence achieved through the QSDP thus ensures that the infrastructures of trust envisioned by the DSA and DGA remain operational in the quantum age. It also reinforces the legal foundations of data altruism, [58] understood as the voluntary sharing of personal informa-

[57] Regulation (EU) 2022/868 (Data Governance Act), cit., art. 12, letts. (j) and (l). Advanced cryptographic mechanisms include homomorphic encryption, secure enclaves, and multi-party computation.

[58] M. Christofidou et al., *Data Altruism and the "Consent" Question: A Study into the "Consent" Models Used under the GDPR and How the Data Altruism Mechanism Can Act as a Potential*

tion for purposes of public interest, research, and innovation. The capacity to guarantee confidentiality and authenticity through quantum-secure infrastructures strengthens the ethical and juridical legitimacy of such mechanisms, ensuring that altruistic data sharing remains compatible with the Charter's requirements of consent, autonomy, and proportionality.

At a systemic level, the alignment of the DSA and DGA with the QSDP within the Digital Code would realize the principle of normative coherence that underpins the entire digital *acquis*. Both instruments were drafted to promote trust in the digital economy through transparency and accountability; quantum preparedness gives concrete content to those abstract values by ensuring that the infrastructures of trust remain technically sound. The QSDP thereby becomes the connective tissue of European digital governance, translating legal foresight into operational certainty.

The incorporation of the QSDP would also enhance institutional coordination. Supervisory and enforcement authorities (ranging from data protection agencies to the Digital Services Coordinators) would operate within a shared technological vocabulary and a common evaluative framework. This would mitigate the fragmentation that currently characterizes European enforcement in the digital domain, where overlapping competences often produce inconsistent interpretations. The convergence around the QSDP would promote uniformity without sacrificing flexibility, as updates to the Protocol through delegated acts under art. 290 TFEU would automatically propagate across all relevant sectors of the Digital Code, maintaining coherence between its components.

In a comparative perspective, this approach situates the Union midway between the American and Chinese regulatory philosophies. The United States has pursued a pragmatic, security-oriented model of quantum readiness, focusing on federal migration to post-quantum cryptography through administrative orders and agency guidelines. China, conversely, has developed a sovereignty-based model centered on state-controlled certification and standardization. The European path, as embodied in the QSDP and its embedding within the DSA and DGA, articulates a distinct legal philosophy: one of constitutional interoperability. It seeks neither unilateral control nor *laissez-faire* adaptation, but rather the institutionalization of technological foresight within the normative fabric of the Union, ensuring that the evolution of technology remains governed by law and oriented toward the protection of rights.

Solution for the Research Community in the Reuse of Health Data, in *Frontiers in Medicine*, 11, 2025, art. 1489925.

5. Quantum Sovereignty as Constitutional Vigilance

The emergence of quantum technologies marks a decisive turning point in the evolution of the Union's relationship with science, innovation, and the market. What is at stake is not merely the regulation of a new technological field but the redefinition of Europe's capacity to govern the infrastructures upon which its normative order depends. Quantum computing, quantum communication, and post-quantum cryptography collectively form what may be described as critical infrastructures:[59] systems whose control determines the Union's ability to safeguard its autonomy, enforce its law, and protect the rights of its citizens.

The legal basis of this project can be traced to art. 173 TFEU, which mandates the Union and the Member States to ensure that "the conditions necessary for the competitiveness of the Union's industry exist." This provision, initially conceived for the industrial policies of the single market, has gradually assumed a constitutional dimension as technology itself has become a precondition for the exercise of sovereignty.[60] In the context of digital transformation, competitiveness is no longer reducible to productivity or innovation metrics: it encompasses the Union's capacity to preserve normative independence in the face of global technological asymmetries. When the means of encryption, computation, or standardization are controlled externally, the autonomy of European law becomes contingent upon foreign infrastructures. The constitutionalization of industrial policy under art. 173 TFEU thus expresses a functional equivalence between technological capability and legal self-determination.

This logic is further tested by the tension between export controls on quantum technologies and the right to science. While the Dual-Use Regulation and the Wassenaar Arrangement increasingly restrict the export of quantum-related components, such controls must be balanced against the imperative of international scientific cooperation, which the right to science under the Charter and the International Covenant on Economic, Social and Cultural Rights protects.[61] In the quantum domain, where active international cooperation and open exchanges remain "imperative" for technological progress,[62] the governance of export controls becomes a test of the Union's capacity to reconcile sovereignty with openness. This logic underlies the European Commission's Communication "Shaping Europe's

[59] M. Ivezic, *Quantum Technology Initiatives in Europe and EU*, in *postquantum.com*, 20 November 2024.

[60] O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road towards Digital Constitutionalism?*, Oxford, 2021.

[61] *Ibid.*, 339-340.

[62] C.J. Hoofnagle – S.L. Garfinkel, *Law and Policy for the Quantum Age*, cit., 408.

Digital Future", which identifies technological sovereignty as a structural objective of the Union's digital policy. The document defines sovereignty not as autarky or isolation, but as the ability to make independent technological choices and to shape global standards in line with European values. The growing body of literature on European digital sovereignty and strategic autonomy – encompassing both the conceptual foundations of digital self-determination and the global contest over regulatory models for technology – has increasingly recognised that this capacity is tested, above all, by emerging technologies whose governance implications cut across established regulatory boundaries.[63] An empirical analysis of over thirty EU policy documents demonstrates that the Union's discourse on digital sovereignty is increasingly intertwined with quantum innovation, as illustrated by the *Digital Decade Policy Programme 2030*, which sets the target of a first European quantum computer by 2025 as a milestone of strategic autonomy. Yet this convergence also carries risks: the rhetorical association of quantum technologies with sovereignty may generate unrealistic expectations if not accompanied by robust scientific evidence and proportionate regulatory responses.[64] This formulation is of constitutional significance: it situates sovereignty within the normative order of the Treaties, connecting it to the Union's founding principles of human dignity, democracy, and the rule of law. Sovereignty, in this perspective, is a derivative of legality. It does not consist in exercising control for its own sake, but in preserving the integrity of the legal and ethical foundations that enable technological innovation to remain compatible with the Union's fundamental rights architecture.

The integration of quantum technologies into this framework demands a reconsideration of how sovereignty is operationalized. The Union's traditional instruments of market regulation and competition law are insufficient to secure control over infrastructures characterized by cumulative technological complexity and strategic dependency. Quantum computing epitomizes this challenge: it is both a scientific frontier and a potential vector of asymmetry in the distribution of computational power, with implications that reach far beyond economics. Four possible scenarios for the quantum future have been mapped – *state takes all*, *corporation takes all*, *public-private development*, and *quantum winter* – each carrying distinct implications for the distribution of decryption power and, consequently, for the

[63] *Ibid.*; see also O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet*, cit. For the broader theoretical framework on digital sovereignty, see L. Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Philosophy & Technology*, 33, 2020, 369 ff.; A. Bradford, *Digital Empires*, cit.; E. Celeste, *Digital Constitutionalism: The Role of Internet Bills of Rights*, Routledge, 2023; P. Timmers, *Strategic Autonomy and Cybersecurity*, EU Cyber Direct, 2019.

[64] P. Vogiatzoglou, *The EU's Quest for Digital Sovereignty*, cit., 12-15.

protection of fundamental rights.[65] In all scenarios except quantum winter, the prospect of quantum decryption entails significant risks for privacy and communications freedom, reinforcing the argument for pre-emptive governance. If the capacity to decrypt, simulate, or optimize becomes monopolized by a limited number of actors – whether corporate or state – the informational balance underpinning the rule of law risks being destabilized.[66] The Union's constitutional duty, therefore, extends to the prevention of *technological dependency* in critical quantum sectors.

This duty finds institutional articulation in the principle of strategic autonomy, which has evolved from a primarily foreign-policy concept into a transversal criterion of Union governance. In the digital domain, strategic autonomy denotes the ability of the Union to maintain sovereign control over essential technologies, data infrastructures, and standardization processes while remaining open to international cooperation. The principle implies a balance between openness and resilience: Europe seeks to remain integrated into the global scientific community but under conditions that preserve its regulatory capacity. The European Quantum Communication Infrastructure (EuroQCI)[67] and the Quantum Flagship programme exemplify this dual logic of autonomy through cooperation. [68] Both initiatives pursue interoperability with international partners while maintaining independent development of secure quantum networks and post-quantum cryptography.

The notion of quantum sovereignty thus encapsulates a juridical synthesis: it unites the industrial rationale of art. 173 TFEU with the constitutional imperatives of art. 2 TEU. By investing in quantum infrastructures, the Union not only promotes industrial competitiveness but also upholds the conditions of its legal system. This is why the governance of quantum technologies cannot be relegated to the domain of research policy; it constitutes a form of constitutional governance, concerned with preserving the material preconditions for legality itself. The security and integrity of

---

[65] *Ibid.*, 305-372 (Chapter 8).

[66] Cf. M.V. Vargas – G. De Gregorio, *The Transformation of European Risk Regulation: Managing Uncertainty and Powers in the Digital Age*, in *European Journal of Risk Regulation*, 2026, 1-17.

[67] European Commission, *Call for Proposals CEF-DIG-2024-EUROQCI-WORKS: European Quantum Communication Infrastructure – The EuroQCI Initiative*, version 2.0, 14 January 2025; European Commission, *European Quantum Communication Infrastructure – EuroQCI*, in *digital-strategy.ec.europa.eu*; European Space Agency – European Commission, *ESA and European Commission Partner to Develop Secure Quantum Communication Infrastructure*, in *connectivity.esa.int*, 30 January 2025.

[68] ICFO, *MWC Quantum Projects*, ICFO, February 2024; European Commission – Quantum Flagship, *Strategic Research and Industry Agenda 2030: Roadmap and Quantum Ambitions over the Decade*, European Quantum Flagship, February 2024.

the Union's information infrastructures have become, in effect, components of legal identity.[69]

From this perspective, the integration of the QSDP within the European Digital Code acquires broader significance. It does not merely establish a standard for cryptographic adequacy; it operationalizes the Union's commitment to strategic autonomy. The QSDP ensures that the technical standards governing encryption and data integrity remain under democratic supervision, subject to the normative oversight of the Union's institutions rather than external certification authorities. In doing so, it bridges the gap between industrial policy and fundamental rights, between standardization and sovereignty. The capacity to define and maintain a European profile of quantum security thus becomes a function of the Union itself.

Comparatively, the European model distinguishes itself from both the United States and the People's Republic of China. The American approach to quantum innovation is market-driven and security-oriented: it relies on decentralized standardization led by NIST, framed within a logic of technological pragmatism. The Chinese approach, conversely, is state-centred and sovereignty-driven: [70] it subordinates technological development to political imperatives of control and self-reliance. [71] The European trajectory seeks a third path, grounded in constitutional pluralism:

---

[69] M.G. Porcedda, *The Recrudescence of "Security v. Privacy" after the 2015 Terrorist Attacks, and the Value of "Privacy Rights" in the European Union*, in E. Orrú et al. (eds), *Rethinking Surveillance and Control: Beyond the "Security versus Privacy" Debate*, Berling, 2017, 137 ff.

[70] Huang Zhaolong – Han Zhaoying, *Sviluppo delle tecnologie dell'informazione quantistica e sicurezza nazionale* (Liangzi xinxi jishu fazhan yu guojia anquan 量子信息技术发展与国家安全), in *Wuhan daxue xuebao (zhexue shehui kexue ban)* 武汉大学学报（哲学社会科学版）, 77, 2, 2024, 51 ff.; Song Shanshan – Zhong Yongheng – Liu Jia et al., *Analisi della configurazione strategica nazionale e delle tendenze di R&S nel settore dell'informazione quantistica* (Liangzi xinxi lingyu de guojia zhanlüe buju yu yanfa taishi fenxi 量子信息领域的国家战略布局与研发态势分析), in *Shijie keji yanjiu yu fazhan* 世界科技研究与发展, 46, 1, 2024; Liu Qingling – Cai Yiran – Zeng Li, *Confronto internazionale delle strategie di sviluppo delle tecnologie dell'informazione quantistica in prospettiva di intelligence* (Qingbao shijiao xia de liangzi xinxi jishu fazhan zhanlüe guoji bijiao 情报视角下的量子信息技术发展战略国际比较), in *Guofang keji* 国防科技, 46, 3, 2025, 108 ff.

[71] Zou Lixue – Liu Yanli, *Ricerca sulla strategia UE per le tecnologie quantistiche e implicazioni* (Oumeng liangzi jishu zhanlüe yanjiu ji qishi 欧盟量子技术战略研究及启示), in *Shijie keji yanjiu yu fazhan* 世界科技研究与发展, 44, 1, 2022, 25 ff.; Fang Wei – Feng Gaoyang, *Strategia e tendenze di sviluppo delle tecnologie quantistiche nel Regno Unito* (Yingguo liangzi keji fazhan zhanlüe ji qushi yanjiu 英国量子科技发展战略及趋势研究), in *Quanqiu keji jingji liaowang* 全球科技经济瞭望, 39, 3, 2024, 20 ff.; Liu Jicheng, *L'UE pubblica il rapporto "Dare forma a una strategia europea per le tecnologie quantistiche"* (Oumeng fabu «Suzao Ouzhou liangzi jishu zhanlüe» baogao 欧盟发布〈塑造欧洲量子技术战略〉报告), in *Keji Zhongguo* 科技中国, 8, 2025, 106.

it reconciles sovereignty with openness, industrial coordination with rights protection, and competitiveness with legality. In this respect, technological sovereignty is not the negation of globalization but its juridical modulation for ensuring that the conditions of participation in global technological exchange remain consistent with the Union's values. [72]

The constitutionalization of technological sovereignty entails, finally, a transformation of the relationship between law and time. Classical constitutional theory conceived sovereignty as a static principle; in the digital age, it becomes temporal, expressed through the continuous adaptation of legal frameworks to technological change. The Union's ability to foresee and regulate emerging technologies before they crystallize into dependencies becomes a test of constitutional vitality. Quantum preparedness, understood as the institutionalization of this capacity for foresight, thus represents the juridical culmination of the Union's strategic autonomy: a form of vigilance oriented not toward the preservation of power, but toward the preservation of the conditions under which power remains legitimate.

The present contribution situates itself within an emerging body of scholarship that addresses the governance of quantum technologies through the lens of law and rights. Where Van Daalen's monograph provides the most comprehensive assessment to date of the human-rights compatibility of existing encryption and quantum computing governance,[73] and where Vogiatzoglou's empirical work exposes the discursive construction of digital sovereignty in EU quantum policy,[74] the present article advances a propositional argument: not merely that the Union's governance must be rights-compatible, but that it must be constitutionally anticipatory, translating the duty of foresight into concrete institutional architectures – the European Digital Code and its annexed Quantum Secure Data Protocol – capable of ensuring that the law itself remains quantum-ready.

[72] L. Moccia, *La cittadinanza nella prospettiva della federazione europea*, in *La cittadinanza europea*, 2, 2011.

[73] *Ibid.*, 39-68.

[74] *Ibid.*

Abstract

This article argues that preparing the European Union for the advent of quantum computing constitutes a constitutional obligation rooted in art. 2 TEU and in the duty to preserve the effectiveness of fundamental rights enshrined in arts. 7 and 8 of the Charter. By demonstrating that quantum machines will render current public-key cryptographic schemes obsolete, the paper identifies a positive obligation of technological foresight incumbent upon the Union's institutions and Member States. Building on the jurisprudence of the Court of Justice and on the emerging scholarship on encryption governance and human rights, the article conceptualises a right to adequate encryption as a corollary of the right to data protection. It then advances two institutional proposals. The first is a two-stage process of normative integration of the EU digital acquis, ranging from immediately practicable sectoral interventions to the prospective horizon of a European Digital Code. The second is a Quantum Secure Data Protocol (QSDP), conceived as a modular, horizontal framework of minimum cryptographic requirements capable of operating either within the Code or as a free-standing instrument. The article concludes by situating quantum preparedness within the broader discourse on European digital sovereignty, reconceived as a form of constitutional vigilance.

Keywords

quantum computing – post-quantum cryptography – EU digital law – right to encryption – digital sovereignty