

FOROEUROPA N.1/2026
ISSN 2038-5161

**EUROPEAN CHALLENGES IN THE RIGHT TO ONLINE SECURITY: THE
IMPACT OF QUANTUM TECHNOLOGY**

Autore: Dott. Alessandro Tacente e Luca Barbieri*

Abstract: In an era of accelerated digital transition, marked by the advent of quantum technologies, online security acquires a distinctly European dimension. The shift to a post-quantum paradigm is not merely a technical development; it affects the legal foundations of digital trust and calls for a reassessment of the European Union's regulatory architecture in the field of cybersecurity.

Adopting a comparative public law perspective and placing supranational regulation at the core of the analysis, this contribution reconstructs, in systemic terms, the evolution of the European framework, assessing its coherence, integration, and adaptive capacity also in light of the safeguards provided by the European Convention on Human Rights, with particular regard to the secrecy of digital communications.

The central argument advanced is that online security is consolidating as a structural dimension of European digital constitutionalism: no longer a sectoral policy, but a supranational public function and a legal precondition for stability and trust within the digital sphere. Quantum technologies thus emerge as a crucial test for the constitutional maturity of the Union, which is called upon to balance security imperatives, the effective protection of fundamental rights, and guarantees of democratic oversight in a context of heightened technological complexity.

Table of Contents: **1** – Preliminary Considerations – **2.** The European Security Architecture in the Age of Quantum Innovation – **3.** The Legal Governance of Online Security in a Transforming Technological Landscape – **3.1.** Cryptography as a Structural Safeguard of Fundamental Rights in the European Digital Order – **4.** Concluding Reflections: Quantum Technology and the Future of European Digital Constitutionalism.

KEYWORDS (EN): Right to Online Security – *Digital Constitutionalism* – *Cybersecurity* – *Quantum Technology*

1. Preliminary Considerations

In an era marked by profound digital transformation and escalating technological disruption, the right to online security can no longer be confined to technical or policy-oriented discourse. It has progressively assumed a distinctly European and

constitutional dimension, emerging as a field of interdisciplinary inquiry of direct relevance to legal scholarship, particularly within comparative public law.

The development of quantum technologies (QT)[\[1\]](#) constitutes one of the most significant drivers of transformation within the contemporary digital ecosystem and raises, with particular intensity, questions concerning the normative resilience of the European legal order. [\[2\]](#)

Constitutional scholarship tends to situate the rights exercised in the digital sphere within the category of so-called fourth-generation rights[\[3\]](#), in light of the new and specific challenges that the technological dimension of security and information poses to the effective exercise and protection of fundamental rights[\[4\]](#), including beyond traditional state boundaries.

In this perspective, the digital environment does not merely constitute a new space for the exercise of already established rights, but requires – if their effective protection is to be ensured – a digital rearticulation of traditional legal categories and constitutional protection mechanisms.

Unlike many digital innovations that merely bring about incremental improvements to existing technologies, quantum technologies entail a genuine paradigm shift, making it possible to process, transmit, and measure information through the direct application of the principles of quantum mechanics[\[5\]](#), thereby overcoming the limitations inherent in classical electronics.

In particular, the prospect of **quantum computing**[\[6\]](#) – understood as the set of computational systems that exploit phenomena intrinsic to quantum mechanics, such as **state superposition** and **entanglement**[\[7\]](#), in order to process information with computational capabilities significantly exceeding those of classical computers – directly affects the **technological foundations upon which the current security of digital networks is based**[\[8\]](#).

The most notable implication of quantum computing is to asymmetric cryptography[\[9\]](#), which is extensively employed to guarantee the confidentiality of digital communications, user authentication, and data integrity. Conventional cryptography algorithms depend on the computational intractability of particular mathematical problems, an intractability that quantum computers may surmount in far shorter durations[\[10\]](#).

The potential vulnerability of such algorithms to quantum attacks therefore introduces a **systemic risk** to the security of communications, the protection of **critical digital infrastructures**[\[11\]](#), and, more broadly, to the reliability of the European digital space. These risks manifest with particular intensity in sensitive domains such as **military defence, government communications**, the functioning of **digital justice systems**, and **electoral processes**.

Within this framework, the **post-quantum paradigm**[\[12\]](#) refers to the set of **technological, organisational, and regulatory strategies** aimed at ensuring the security of networks and information systems even in the presence of advanced quantum computing capabilities. This paradigm includes, in particular, the development of **post-quantum cryptographic algorithms**[\[13\]](#) designed to

withstand attacks based on quantum technologies, as well as the adoption of **hybrid architectures** combining classical and quantum cryptographic solutions. However, the transition towards post-quantum security[14] cannot be reduced to a merely technical adjustment of digital infrastructures, as it affects the **structural foundations of the legal order** and the **allocation of powers within the digital space**.

From the perspective of **European public law**, this transition constitutes a critical **testing ground for the resilience of digital constitutionalism**[15] **in Europe**. This notion refers to the set of principles, limits, and safeguards governing the exercise of public power online[16], within a context characterised by a plurality of normative levels, the coexistence of public and private actors, and an increasing opacity of technical decision-making processes.

From this standpoint, **digital constitutionalism**[17] is called upon to preserve the **primacy of law** and the **protection of fundamental rights**, even in the face of technological innovations that structurally affect both the conditions under which freedoms are exercised and the organisation of public powers.

Online security thus acquires a significance that goes beyond a merely technical dimension, assuming a **genuinely constitutional relevance within the digital sphere**[18].

In this sense, the protection of digital networks and communications does not merely affect the efficiency of information systems, but directly concerns the continuity of essential public functions, the reliability of democratic processes, and public trust in institutions. The potential of quantum technologies to overcome current asymmetric cryptographic techniques makes it clear that the security of communications, the resilience of critical digital infrastructures, the integrity of electoral systems, and the proper functioning of digital justice are structurally interconnected elements.

From this perspective, **cybersecurity** acquires a fully **infrastructural and geopolitical dimension**[19], closely linked to the stability of democratic legal orders and to the prevention of **hybrid conflicts** within the digital space. Network security therefore emerges as a **legal safeguard of peace**[20] in the European context, understood not merely as the absence of armed conflict, but as a condition of **institutional stability, predictability of public action, continuity of essential functions**, and **effective protection of fundamental rights** in the digital environment.

In this scenario, the **European Union** occupies a position of particular complexity. On the one hand, it has progressively strengthened its regulatory framework on **cybersecurity**, qualifying the security of networks and information systems as a **primary public interest** and imposing obligations relating to risk prevention and management[21]. On the other hand, this regulatory framework was conceived within a **pre-quantum technological context** and is now required to confront a **structural shift in the technical foundations of digital security**. Added to this is the need to coordinate European security policies with the constraints arising from the **multilevel system of fundamental rights protection**, in particular those enshrined in the **Charter of Fundamental Rights of the European Union** and the **European Convention on Human Rights**.

It is within this framework that the present article adopts the lens of comparative constitutional law[22], understood as an analytical tool for examining the multilevel interactions between European Union law, the conventional human rights system, and national legal orders. Ultimately, the aim is to assess whether and to what extent the current European governance of quantum technologies is capable of reconciling and balancing the requirements of infrastructural security and strategic autonomy with the protection of fundamental rights, while preserving the role of law as a means of conflict prevention and as a guarantor of peace within the European digital space.

2. The European Security Architecture in the Age of Quantum Innovation

In the context of rapid technological advancements in the twenty-first century, quantum technologies are progressively transitioning from experimental phases to comprehensive industrial implementation, thereby acquiring direct strategic importance for European security and policies aimed at protecting critical digital infrastructures[23].

Recent experimental advances in superconducting[24] qubits[25], trapped ions[26], integrated photonics, and diamond defect centres have made it possible to achieve coherent control of systems comprising tens or hundreds of qubits, although such systems still operate in environments characterised by high noise levels and significant limitations in terms of stability and scalability. Nevertheless, these developments position quantum technologies among the emerging factors likely to exert a significant impact on security balances, on the protection of strategic communications, and, more broadly, on the capacity of European state legal orders to effectively govern and secure the digital space.

The first quantum revolution, which occurred in the early twentieth century, resulted in the establishment of quantum mechanics as the foundational theory of microscopic physics.

It introduced a profound revision of classical concepts such as determinism, causality, and continuity, establishing a probabilistic paradigm grounded in phenomena including energy quantisation, wave–particle duality, and the uncertainty principle. The technological innovations arising from this initial period, including semiconductors, transistors, and lasers, established the groundwork for modern electronics and current information technology.

The second quantum revolution[27], which began in the 1980s, is instead characterised by the transition from the mere theoretical description of quantum phenomena to their controlled manipulation and engineering for practical applications. In this phase, fundamental quantum properties—such as superposition and entanglement—are employed as operational resources for the processing, transmission, and protection of information, giving rise to new fields such as quantum computing[28], quantum communication[29], and quantum cryptography[30]. This evolution marks a technological paradigm shift, in which the laws of quantum mechanics are no longer merely objects of scientific inquiry but become direct tools of technological design.

Quantum technologies exhibit an intrinsically dual-use character, positioning themselves structurally at the intersection of civil and military applications and exerting a direct impact on security and defence policies.

Within the European context, this dual-use character acquires particular significance with regard to the protection of strategic communications, the development of advanced intelligence^[31] capabilities, and the safeguarding of critical digital infrastructures, as it unfolds within a global technological competition that has assumed an explicitly geopolitical dimension.

Quantum supremacy thus emerges as one of the central nodes of international technological rivalry, with direct repercussions on security balances and on the capacity of legal orders to preserve the reliability of their information systems.

Within this framework, quantum technologies are increasingly situated at the intersection of cybersecurity and European security in a broader sense, affecting areas that fall, directly or indirectly, within the scope of the Common Security and Defence Policy.

The prospect that quantum computing may undermine mechanisms for the protection of communications and data introduces a factor of systemic vulnerability that does not concern isolated sectors, but rather affects the continuity of essential public functions and the overall resilience of strategic infrastructures. In this sense, digital security acquires a strategic significance that transcends the technical-administrative dimension, emerging as a structural element of the capacity of the Union and its Member States to operate within a context of growing instability and technological competition.

It is from this perspective that the notion of digital sovereignty^[32] must be understood, as the capacity of legal orders to regulate the development, use, and governance of digital technologies, with a view to preserving security, the protection of fundamental rights, and strategic autonomy within the European digital space.

In the post-quantum supremacy era, digital sovereignty cannot be understood as a reassertion of exclusive state power over the digital space, as such an approach would be incompatible with the open and multilevel structure of the European legal order and with the constraints deriving from the system of fundamental rights protection. Rather, digital sovereignty may be conceived as the functional capacity of European legal orders to ensure the control, security, and reliability of critical technological infrastructures, while reducing strategic dependencies and systemic vulnerabilities within a context of global interdependence.

In the field of quantum technologies, this capacity translates into the ability to secure sensitive technological supply chains, to ensure the security of public and strategic communications, and to protect essential state functions from external interference or forms of technological pressure. Digital sovereignty thus assumes a predominantly infrastructural and preventive dimension, oriented not toward the expansion of public power, but toward the preservation of the stability of the legal order and the continuity of institutional action within the European digital space.

However, digital sovereignty[33] can be incorporated into legal discourse only on the condition of its constitutionalisation within domestic legal orders. It cannot legitimise spaces of exception nor justify structural restrictions of fundamental rights in the name of technological security. On the contrary, security becomes a legally relevant component of sovereignty only insofar as it is exercised in compliance with the principles of legality, necessity, and proportionality, and remains subject to effective democratic and judicial oversight.

From this perspective, the multilevel system of fundamental rights protection operates as a structural limit on digital sovereignty. European case law[34] has clarified that national security and the protection of critical infrastructures do not constitute domains immune from legal scrutiny, but instead require a particularly rigorous balancing whenever they affect the sphere of communications and personal data. When applied to post-quantum technologies, these principles require the exclusion of regulatory solutions that introduce generalised vulnerabilities or systemic weakening of security architectures, as such measures would ultimately undermine the very security they purport to pursue.

Ultimately, quantum technologies bring to light a structural tension between security, sovereignty, and fundamental rights. The response of the European legal order cannot consist either in a renunciation of security or in its absolutisation. Rather, post-quantum security must be integrated into a constitutionally oriented conception of digital sovereignty[35], in which the protection of critical infrastructures and strategic communications is conceived as an instrument of stability and conflict prevention, rather than as a factor of permanent exception within the European digital space.

3. The Legal Governance of Online Security in a Transforming Technological Landscape

Over the past decade, the security of networks and information systems within the European Union has evolved into an autonomous legal domain, transcending its original technical connotation to become a structured field governed by binding obligations and clearly defined public responsibilities.

This evolution reflects the recognition of online security as an essential condition for the functioning of the internal market, the continuity of public services, and the stability of democratic legal orders, thereby situating cybersecurity within the realm of European public law.[36].

Within this framework, the European Union occupies a position of particular complexity and ambivalence. On the one hand, it seeks to consolidate its role as a regulatory power also in the domain of emerging technologies, and in particular in the quantum sector, through long-term strategies, investment programmes, coordination initiatives, and instruments of soft law[37].

The announced prospect of a future EU Quantum Act[38] fits within this trajectory as a potential instrument aimed at strengthening European strategic autonomy, reducing technological dependencies, and ensuring public oversight over next-generation critical digital infrastructures[39]. At the same time, however, the existing

cybersecurity regulatory framework—although significantly reinforced in recent years—remains structurally anchored to a pre-quantum technological context.

The main regulatory innovations – namely Directive (EU) 2022/2555 (NIS 2)[\[40\]](#), Directive (EU) 2022/2557[\[41\]](#) on the resilience of critical entities (CER), Regulation (EU) 2019/881 (Cybersecurity Act) [\[42\]](#), and Regulation (EU) 2024/2690[\[43\]](#) – have undoubtedly expanded and strengthened obligations relating to risk prevention, incident management, and institutional cooperation, by extending the scope of obligated entities and introducing more stringent mechanisms of accountability[\[44\]](#).

However, this regulatory framework remains fragmented and only partially equipped to address in a systematic manner the constitutional implications of the post-quantum transition, which calls into question the technological assumptions underlying current security architectures.

In this context, cryptography, traditionally understood as an essential tool for the protection of communications and data, becomes a focal point for growing tensions between security requirements, the protection of public order, and the safeguarding of fundamental rights.

European Union law and the European conventional system for the protection of fundamental rights operate jointly as structural constraints on public interferences with the communicative sphere, even where such interferences are justified by security or public order concerns.

In this respect, Article 7 of the Charter of Fundamental Rights of the European Union [\[45\]](#) and Article 8 of the European Convention on Human Rights[\[46\]](#) recognise the secrecy of communications and the respect for private life as fundamental rights, the restriction of which is admissible only under strictly defined conditions.

In particular, the case law of the European Court of Human Rights[\[47\]](#) has consistently held that any measure interfering with the communicative sphere must be based on an accessible and foreseeable legal basis, pursue a legitimate aim, and be necessary in a democratic society, in accordance with a strict proportionality test.

Accordingly, the case law of the European Court of Human Rights has held that national security cannot justify forms of surveillance amounting to generalised and insufficiently circumscribed control of communications. In *Roman Zakharov v. Russia*[\[48\]](#), *Szabó and Vissy v. Hungary*[\[49\]](#), and *Big Brother Watch and Others v. the United Kingdom*[\[50\]](#), the Court has emphasised the need for substantive and effective safeguards against the risk of arbitrariness, thereby reinforcing the view that the protection of communications does not constitute an obstacle to security, but rather an essential component of security in a democratic society.

These requirements are accompanied by the need for effective procedural safeguards, such as the clear delimitation of surveillance powers, the provision for independent *ex ante* and *ex post* oversight, and the availability of effective judicial review[\[51\]](#) of the measures adopted. Comparable principles have been incorporated and further developed within the European Union legal order, where respect for the rights enshrined in the Charter of Fundamental Rights constitutes a binding

parameter for the action of both EU institutions and Member States when implementing Union law.

Within this framework, the conventional system performs an essential function as an external constraint on digital security policies, requiring that technological innovation and the deployment of advanced protection or surveillance tools do not result in a structural lowering of fundamental rights protection standards. In the absence of such safeguards, there is a risk of the progressive normalisation of exceptional measures adopted in the name of security, capable of permanently affecting the balance between public powers and individual rights and of undermining the democratic legitimacy of security policies within the European digital space.

Overall, the European regulatory framework reflects a conception of online security as an infrastructural dimension of public law, grounded in obligations of prevention, organisational responsibility, and multilevel cooperation among public authorities, private actors, and European institutions. Network security is no longer entrusted exclusively to the technical capabilities of operators, but is instead constructed as the outcome of a system of legal duties and governance mechanisms involving the entire digital ecosystem.

Accordingly, the emergence of quantum technologies affects this framework in a structural manner. The prospect of quantum computing capable of undermining the cryptographic algorithms currently in use calls into question one of the implicit foundations of the entire European digital security architecture: the reliability of classical cryptography. The risk does not concern isolated or contingent vulnerabilities, but rather the possibility of a generalised and retroactive compromise of digital communications, with systemic effects on critical infrastructures and on essential public functions[52].

Within this scenario, online security can no longer be conceived merely as a technical domain of administrative action or as a sector-specific field of regulation[53], but rather acquires a genuinely constitutional significance, insofar as it is directly connected to the capacity of the European legal order to ensure stability, trust, and continuity of public functions within the digital space. The post-quantum transition therefore calls for a reflection on security governance capable of reconciling technological innovation, the protection of fundamental rights, and democratic oversight, so as to prevent responses to emerging threats from resulting in a structural erosion of the principles of the – *now digital*[54] – rule of law.

3.1. Cryptography as a Structural Safeguard of Fundamental Rights in the European Digital Order

Cryptography constitutes a structural safeguard through which the effective protection of private life and the secrecy of communications is ensured within the digital environment. In contemporary networked societies—where interactions are predominantly mediated by electronic communications—encryption is not merely a technical tool of data protection, but a legal precondition for the effective exercise of the rights enshrined in Article 7 of the Charter of Fundamental Rights of the European Union and Article 8 of the European Convention on Human Rights. From a constitutional perspective, encryption operates as a legal infrastructure of

confidentiality: it translates normative guarantees into concrete protection against unlawful access, disproportionate surveillance, and systemic vulnerabilities.

From this perspective, cryptography operates as a legal infrastructure of confidentiality, contributing to the practical effectiveness of constitutional guarantees in a context characterised by the pervasiveness of electronic communications.

In the post-quantum context, the potential vulnerability of traditional cryptographic algorithms raises an issue that transcends the technological plane and directly engages the responsibility of European legal orders in safeguarding fundamental rights.

The ability to ensure effective and durable protection of digital communications cannot rely on solutions that entail a structural weakening of cryptography or the introduction of generalised access mechanisms to encrypted communications. Such approaches would risk transforming security into a factor of systemic vulnerability, undermining the overall reliability of the digital environment and producing disproportionate interferences with fundamental rights.

From the perspective of European Union law, the case law of the Court of Justice has made clear that measures entailing extensive interferences with the confidentiality of communications and personal data must be subject to particularly strict scrutiny.

In the judgments *Digital Rights Ireland*[\[55\]](#), *Tele2 Sverige/Watson*[\[56\]](#), and *La Quadrature du Net*[\[57\]](#), the Court of Justice of the European Union ruled out the compatibility with EU law of data retention regimes characterised by generalised and indiscriminate scope, holding that even national security considerations cannot justify serious and disproportionate interferences with the rights to private life and personal data protection, as guaranteed by Articles 7 and 8 of the Charter, read in conjunction with Article 52(1) thereof.

These rulings delineate a framework in which the cryptographic protection of communications does not constitute a mere technical option, but rather emerges as a structural component of the level of protection required by the EU legal order, insofar as it functions as a safeguard against forms of generalised access to data incompatible with the principles of necessity, proportionality, and effective oversight.

When applied to the post-quantum domain, the principles developed by European and conventional case law require a reassessment of cryptography as both a legal and technical prerequisite of constitutionally oriented security, capable of reconciling the effective protection of fundamental rights with the need to safeguard the digital space.

The protection of digital communications does not stand in opposition to security requirements, but rather constitutes a structural precondition thereof, insofar as it contributes to preserving public trust, the reliability of digital infrastructures, and the democratic legitimacy of security policies. In light of this, the right to online security may be understood as a right to a reliable and legally protected digital environment, in which technological innovation does not result in a regression of fundamental rights protection standards.

4. Concluding Reflections: Quantum Technology and the Future of European Digital Constitutionalism.

The emergence of quantum technologies within the European security landscape compels a constitutional reassessment of the foundations of digital governance. Their impact cannot be confined to a mere technical upgrading of digital infrastructures or to a simple extension of existing cybersecurity policies[58]. Rather, the post-quantum transition exposes structural tensions within the European legal order, requiring a recalibration of the balance between technological innovation, strategic autonomy, fundamental rights protection, and democratic oversight.

The transition to a post-quantum framework directly influences the legal underpinnings of security, significantly altering the dynamics among public authority, technology, and fundamental rights, necessitating an evaluation of the ability of digital constitutionalism in Europe to manage structural technological transformations while maintaining its regulatory role.

Quantum technologies introduce a dimension of systemic instability that directly impacts public law. The potential to compromise established cryptographic systems while concurrently affecting communication security, the robustness of essential infrastructures, and the strategic capabilities of nations underscores that internet security must transcend sector-specific boundaries. It arises as a comprehensive legal category, intersecting the safeguarding of fundamental rights, institutional stability, and conflict prevention in the digital realm.

In this light, and consistently with the analysis developed above, online security may be understood as a strategic asset for peace, conceived as a condition of legal reliability and continuity of essential public functions.

The European Union has increasingly recognized the strategic importance of network and information systems security through regulation enhancement, culminating in the passage of the NIS 2 Directive, the CER Directive, and the Cybersecurity Act. Nonetheless, this evolution is primarily rooted in a pre-quantum technology framework and is defined by a fundamentally technical and sector-specific governance model, heavily dependent on soft-law tools. This results in a deficit of constitutionalisation of digital security, which risks obscuring issues of fundamental rights protection and democratic oversight in the governance of emerging technologies.

Within this framework, the prospect of an EU Quantum Act acquires a significance that transcends the sphere of industrial policy and technological competitiveness. Such a legislative initiative could provide a forum for the emergence of a constitutionally oriented regulatory framework for quantum technologies, capable of integrating security concerns, fundamental rights, and public responsibility. Its legitimacy, however, will ultimately depend on its compliance with the constraints deriving from European Union law and the European conventional human rights system.

Moreover, the case law of the European Court of Human Rights, although developed in a technological context predating the full maturity of quantum computing, provides interpretative criteria that are equally applicable within the post-quantum

domain. The principles of legality, necessity, and proportionality, together with the requirement of substantive and effective safeguards against the risk of arbitrariness in surveillance activities, constitute indispensable parameters for preventing technological security from evolving into a permanent state of exception.

As clarified by the European courts, national security cannot be construed as a zone of exemption from the protection of fundamental rights.

Finally, an interdisciplinary and comparative approach^[59] makes it possible to highlight how quantum technologies intensify the structural tensions between security and democratic control within the European legal space. The inherently dual-use nature of quantum technologies, their growing integration into defence and intelligence policies, and the increasing technocratisation of security-related decision-making expose the legal order to the risk of a progressive withdrawal of fundamental choices from the sphere of constitutional guarantees. It is precisely within this space of tension that the stakes of European digital constitutionalism are ultimately played out^[60].

In conclusion, cyber security in the era for quantum technology challenges the future of European public law^[61].

The approach of the European legal order in handling the post-quantum transition will be a crucial indicator of its constitutional development. If security imperatives are permitted to solidify into a permanent condition of exception, the fundamental principles of digital constitutionalism would be jeopardized. The critical examination, consequently, resides in regulating technological disruption through legislation to maintain peace, liberty, and human dignity in the digital realm.^[62]

While the article is grounded in a shared conceptual and methodological framework, for the purposes of academic authorship attribution Sections 1 and 3 are to be attributed to Alessandro Tacente, whereas Sections 2 and 3.1 are to be attributed to Luca Barbieri. Section 4 (Conclusions) is the result of joint research and collective scholarly deliberation by the Authors.

*Alessandro Tacente holds a PhD in Comparative Constitutional Law from LUMSA University of Rome. Luca Barbieri is a PhD candidate in Security, Risk and Vulnerability at the University of Genoa.

^[1] The origins of quantum theory are conventionally situated at the turn of the twentieth century, when Max Planck (1900–1901), in addressing the black-body radiation problem, introduced the revolutionary hypothesis of discrete energy “quanta,” thereby breaking with the classical notion of continuity. This foundational insight was soon expanded by Albert Einstein (1905) through his explanation of the photoelectric effect and was further systematised in Niels Bohr’s atomic model (1913). In the 1920s, the seminal contributions of Louis de Broglie, Erwin Schrödinger, and Werner Heisenberg culminated in the formal consolidation of quantum mechanics, marking a decisive shift from classical determinism to a fundamentally probabilistic understanding of physical reality.

[2] See A. ACÍN et al., The Quantum Technologies Roadmap: A European Community View, in *New Journal of Physics*, vol. 20, n. 8, 2018, 080201.

[3] On this point, see L. Pegoraro, A. Rinella, *Sistemi costituzionali*, Giappichelli, Turin, 2024, at 199, who argue that “the fourth generation of rights originates from the new technological dimension of information and communication and refers to the so-called rights of the technological society. Science and technology have developed at such a rapid pace as to encounter ever fewer obstacles in the sphere of life and its various expressions. Technosciences directly interfere with the configuration of new rights and new claims, while at the same time creating a bridge towards future generations. As a result of the scientific and technological revolution, the value framework that long constituted the reference basis for fundamental rights and freedoms undergoes a profound identity crisis, to which political communities respond by attempting to reconstruct a new fabric of legitimacy.” See also L. Bruscutta, R. Romboli (eds.), *Diritto pubblico e diritto privato nella rete delle nuove tecnologie*, Pisa University Press, Pisa, 2010; T.E. Frosini, *Liberté Égalité Internet*, Editoriale Scientifica, Naples, 2015; J.J. FERNÁNDEZ RODRÍGUEZ, *Gobierno electrónico*, Fundap, Querétaro, 2004; F.J. DÍAZ REVORIO, *Los Derechos Humanos ante los nuevos avances*

Científicos y Tecnológicos, Tirant lo Blanch, Valencia, 2009.

[4] With regard to the protection of human rights on the Internet, the United Nations Human Rights Council adopted Resolution 20/8, “The promotion, protection and enjoyment of human rights on the Internet” (A/HRC/RES/20/8, 2012), which affirms that the same rights that people have offline must also be protected online, thereby recognising the Internet as a space subject to international human rights law.

[5] C Cohen-Tannoudji, B Diu and F Laloë, *Quantum Mechanics*, vol. 1: Basic Concepts, Tools, and Applications, 2nd edn, Wiley-VCH, Weinheim, 2019.

[6] On the theoretical foundations of quantum computing, see R. P. Feynman, *Simulating Physics with Computers*, *International Journal of Theoretical Physics*, vol. 21, nos. 6–7, 1982, pp. 467 ff., where the author highlights the inadequacy of classical computational models for simulating complex quantum physical systems and introduces the idea of computation based on quantum principles as a conceptually necessary tool for the efficient simulation of natural phenomena.

[7] Entanglement is a phenomenon of quantum mechanics whereby the state of a system composed of multiple particles cannot be described as the sum of the states of its individual components, but only in a holistic and unitary manner. This form of non-local correlation implies that a measurement performed on one particle instantaneously affects the state of the other, regardless of spatial distance, and constitutes an essential technological resource for applications such as quantum computing and quantum cryptography, thereby impacting the technical foundations of communications security.

[8] See M. D. Rahman, *Cryptography in Digital Security: Foundations, Applications, and Emerging Challenges*, CRC Press, Boca Raton, 2023, which provides a structured overview highlighting that cryptography constitutes a core component of digital

security and plays a critical role in protecting data, communications, and digital identities in contemporary information systems.

[9] Asymmetric cryptography is an encryption system that employs a pair of mathematically related keys, namely a public key and a private key, where the former is used to encrypt the message and the latter to decrypt it. The security of the system is based on the high computational complexity of specific mathematical problems, which makes the reconstruction of the private key from the public key computationally infeasible.

[10] Shor, P. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS). IEEE

[11] Within European Union law, the protection of critical infrastructures is now governed by Directive (EU) 2022/2557 (Critical Entities Resilience – CER), which replaces Directive 2008/114/EC and introduces a reinforced resilience framework for critical entities operating in essential sectors. The Directive imposes obligations relating to risk assessment, preventive measures, and operational continuity, as well as mechanisms of cooperation among Member States, with a view to ensuring the functioning of essential services and the security of the Union; Reference may be made to NIST, Post-Quantum Cryptography Standards, Washington, D.C., 2023; NIST, Post-Quantum Cryptography Standardization: Finalist Algorithms, Gaithersburg, MD, 2022; as well as E. Grumbling, M. Horowitz, Quantum Computing: Progress and Prospects, National Academies Press, Washington, D.C., 2019, which provides a systematic overview of the state of the art and the prospective developments of quantum computing, together with an analysis of its implications for the security of digital communications.

[12] See D. J. Bernstein, J. Buchmann, E. Dahmen, Post-Quantum Cryptography, Nature, vol. 549, 2017, pp. 188–194, which conceptualises the post-quantum paradigm as a structural shift in digital security, requiring cryptographic systems resilient to quantum-enabled attacks.

[13] That is, the set of cryptographic algorithms specifically designed to remain secure even in the presence of advanced quantum computing capabilities, as they are based on mathematical problems for which, according to the current state of knowledge, no efficient quantum algorithms are known.

[14] From a comparative perspective, reference may be made to the United States, where the National Institute of Standards and Technology (NIST) has initiated and conducted a comprehensive post-quantum cryptography standardisation process, culminating in the adoption of new federal standards aimed at ensuring the security of public and private communications in a context of the progressive vulnerability of classical cryptographic algorithms. This process reflects a highly centralised and anticipatory model of technical-scientific governance.

[15] On this point, see O. Pollicino, Di cosa parliamo quando parliamo di costituzionalismo digitale?, Quaderni Costituzionali, no. 3, 2023.

[16] L. TORCHIA, *Poteri pubblici e poteri privati nel mondo digitale*, Il Mulino, no. 1, 2024, page 28.

[17] E. CELESTE, *Digital constitutionalism: a new systematic theorisation*, in *International Review of Law, Computers & Technology*, 2019.

[18] On this issue, see P. Passaglia, *Liber Amicorum per Pasquale Costanzo. Ancora sul fondamento costituzionale di Internet. Con un ripensamento*, ConsultaOnLine, 26 June 2019; P. Costanzo, *Internet (diritto pubblico)*, ad vocem, in *Digesto delle Discipline Pubblicistiche*, Appendix, 2000, pp. 347 ff.

[19] See European Policy Centre (EPC), *Quantum Technologies and Value Chains*, Discussion Paper, Brussels, 2023, analysing the strategic configuration of quantum value chains and related dependencies; European Centre for International Political Economy (ECIPE), *Quantum Technology: A Policy Primer for EU Policymakers*, Policy Brief, Brussels, 2022, outlining the policy and regulatory implications of quantum technologies for the EU's strategic autonomy.

[20] *Ex multis*, see J. Boeken, *In Between Digital War and Peace*, *Journal of Military Ethics*, 2024; ICT4PEACE, *Information and Communication Technology for Peace: the Role of ICTs in Preventing, Responding to and Recovering from Conflict*, New York, 2005.

[21] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge University Press, Cambridge, 2010.

[22] Comparative analysis, which the present contribution modestly seeks to offer, serves as both a compass and a "shortcut to understanding the world" within the kaleidoscope and eclecticism of legal systems, preventing scholars from remaining confined to "... the theories and categories learned at home (or in the basement), attributing to them a [scientifically incorrect] universal value ...". This reflection is drawn from L. Pegoraro – A. Rinella, op. cit., esp. pp. 1 ff., as well as from Id., *Introduzione al diritto pubblico comparato. Metodologie di ricerca*, Cedam, Padova, 2002. The same concept is also taken up by D. Amirante, *Metodo comparativo, ambiente e dinamiche costituzionali*, in *DPCE online*, 2023, special issue no. 2, p. 19.

[23] J. Preskill, *Quantum Computing in the NISQ Era and Beyond*, *Quantum*, vol. 2, 2018, Art. 79.

[24] F. Arute et al., *Quantum Supremacy Using a Programmable Superconducting Processor*, *Nature*, vol. 574, no. 7779, 2019, pp. 505–510.

[25] A qubit (quantum bit) constitutes the fundamental unit of quantum information and is characterised by the ability to exist in a superposition of the logical states 0 and 1. Unlike the classical bit, which assumes a single definite value at any given time, the qubit enables information processing according to the principles of quantum mechanics, thereby underpinning computational paradigms capable of exceeding the limits of classical information processing.

[26] Trapped ions are electrically charged atoms confined in space by means of electromagnetic fields (such as Paul or Penning traps) and employed as controllable

quantum systems. In the quantum domain, they enable the realisation of highly stable qubits, primarily used in quantum computing and quantum simulation.

[27] J. P. Dowling, G. J. Milburn, Quantum technology: The second quantum revolution, *Philosophical Transactions of the Royal Society A*, vol. 361, no. 1809, 2003, pp. 1655–1674, introducing the conceptual framework of the second quantum revolution based on controlled manipulation of quantum states.

[28] A. Acín et al., The European Quantum Technologies Roadmap, *npj Quantum Information*, 2018, which provides a scientifically grounded overview of European initiatives in the field of quantum technologies, including quantum computing.

[29] See further B. Kubala et al., Advanced Quantum Communication and Quantum Networks – From basic research to future applications, *arXiv*, 2024, which provides a systematic account of the theoretical foundations, technological architectures, and prospective applications of quantum communication, with particular attention to the transition from basic research to large-scale infrastructural implementation.

[30] See A. Broadbent, C. Schaffner, Quantum Cryptography Beyond Quantum Key Distribution, *Designs, Codes and Cryptography*, vol. 78, 2016, pp. 351 ff., where the Authors provide a systematic reconstruction of quantum cryptography understood no longer as a field limited to Quantum Key Distribution alone, but rather as an articulated set of primitives and protocols grounded in the principles of quantum mechanics, examining both its practical potential—particularly in terms of information-theoretic security—and the structural limitations and theoretical challenges arising from the extension of classical cryptographic models to the quantum domain.

[31] Within European Union law, intelligence activities remain primarily attributed to the Member States, as national security “remains the sole responsibility of each Member State” (Article 4(2) TEU). Nevertheless, a progressive level of cooperation and information support has developed at the European level, in particular through the EU Intelligence and Situation Centre (INTCEN), an internal structure of the European External Action Service (EEAS), within the organisational framework established by Council Decision 2010/427/EU; With regard to the prevention and countering of security threats, Europol operates as a platform for analysis and information exchange pursuant to Regulation (EU) 2016/794. In the literature, see R.A. Wessel, V. Szép, Towards Intelligence Cooperation in the EU?, *European Foreign Affairs Review*, 27(3), 2022, pp. 307 ff.; D. Curtin, *Overseeing Secrets in the EU: A Democratic Perspective*, 2014.

[32] See A. Venanzoni, L’ordine costituzionale della cybersecurity, *Forum di Quaderni Costituzionali*, no. 4, 2024, pp. 39–43, where the Author observes that digital sovereignty may alternatively denote either a reassertion of the State within the digital domain, in response to the almost genetic transformations of society and state forms driven by globalisation and digitalisation, or a form of sovereignty that is self-determined by the technical and organisational rules of the digital environment itself.

[33] See R. Bellamy, A European republic of sovereign States: sovereignty, republicanism and the European Union, *European Journal of Political Theory*, vol. 16, 2016; R. Bifulco, A. Nato, The concept of sovereignty in the European Union: past,

present and the future, Brussels, European Union's Horizon 2020 Research and Innovation Programme, 2020; C. Bjola, *The European Union's quest for digital sovereignty and its implications for the transatlantic relationship*, Oxford, Oxford Department of International Development, 2021; M. Robles Carrillo, *La articulación de la soberanía digital en el marco de la Unión europea*, *Revista de Derecho Comunitario Europeo*, no. 75, 2023.

[34] As will be examined in greater detail in the following section.

[35] See M. Santaniello, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, *Rivista italiana di informatica e diritto*, no. 1, 2022, p. 48.

[36] Lewis, A., Scudo, P., Cerutti, I., Travagnin, M., Marcantonini, C. et al., *Future directions for quantum technology in Europe – an analysis of policy questions*, Publications Office of the European Union, Luxembourg, 2025.

[37] *European Quantum Flagship, Strategic research agenda*, European Commission, Brussels, 2020.

[38] The expression EU Quantum Act refers to the announced regulatory initiative of the European Union aimed at providing quantum technologies with a unified legal framework, designed to strengthen the Union's technological sovereignty and industrial competitiveness. As outlined by the European Commission within the Quantum Europe Strategy, the proposed act is intended to address issues of governance, investment coordination, the security of quantum infrastructures, and the resilience of supply chains in a sector characterised by high strategic relevance and potential implications for security and fundamental rights. Although no formal legislative proposal has yet been adopted, the Quantum Act forms part of the broader process of the European constitutionalisation of emerging technologies, alongside instruments such as the Chips Act and the Cybersecurity Act, marking a further step towards the public regulation of enabling technologies with high systemic impact.

[39] Riedel, M. F., Bloch, I., Debuisschert, T., Wilhelm-Mauch, F., Pruneri, V., Vitanov, N. V., Wehner, S. & Calarco, T., *Europe's Quantum Flagship is taking off*, *Europhysics News*, vol. 49, no. 5-6, pp. 30–34, 2018.

[40] Directive (EU) 2022/2555 (NIS 2) strengthens and harmonises the European cybersecurity framework by extending risk-management, incident-reporting and supervisory obligations to a broader range of public and private entities operating in critical sectors, with the aim of enhancing the resilience of essential infrastructures and digital services within the Union.

[41] European Union, Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive), Brussels, 2022. The CER Directive establishes a common EU framework to enhance the resilience of critical entities by imposing risk assessment, prevention and incident-response obligations, complementing the NIS 2 Directive in the protection of essential infrastructures against physical and hybrid threats.

[42] Regulation (EU) 2019/881 (the Cybersecurity Act) establishes a European cybersecurity certification framework for ICT products, services and processes, and

strengthens the mandate of ENISA, thereby contributing to a higher common level of cybersecurity and trust in the Union's digital single market.

[43] Regulation (EU) 2024/2690 introduces horizontal cyber-resilience requirements for products with digital elements by imposing security-by-design and security-by-default obligations throughout the entire product life cycle, with the aim of strengthening the protection of the internal market and the security of European digital infrastructures.

[44] In this regard, reference should also be made to the principle of accountability enshrined in Regulation (EU) 2016/679 (GDPR), pursuant to which data controllers—including digital platforms—are required not only to comply with personal data protection requirements, but also to be able to demonstrate such compliance through appropriate technical and organisational measures, risk assessment systems, and mechanisms of accountability both *ex ante* and *ex post* (Articles 5(2), 24 and 25 GDPR).

[45] Article 7 of the Charter of Fundamental Rights of the European Union provides that "everyone has the right to respect for his or her private and family life, home and communications", recognising a fundamental right aimed at protecting personal autonomy and the intimate sphere from arbitrary interference by public authorities. This provision is conceived in continuity with Article 8 of the European Convention on Human Rights and is binding on the EU institutions and the Member States when implementing Union law, allowing for limitations only where they are provided for by law and are necessary in a democratic society, *inter alia*, for reasons of national security or for the protection of the rights of others.

[46] Article 8 of the European Convention on Human Rights enshrines the right of everyone to respect for his or her private and family life, home and correspondence, binding the Contracting States to refrain from interference with this right except where such interference is in accordance with the law and necessary in a democratic society for legitimate aims such as national security, public safety, the protection of order and the rights of others, as well as the prevention of crime; the case law of the European Court of Human Rights has further clarified that Article 8 entails both negative and positive obligations to ensure effective respect for private and family life.

[47] A central reference is provided by the judgment of the European Court of Human Rights, Grand Chamber, *Roman Zakharov v. Russia* of 4 December 2015, in which the Court held that measures of communications surveillance are compatible with Article 8 ECHR only where they are based on a legal framework meeting the required quality of law, understood in terms of accessibility, foreseeability and the existence of effective safeguards against the risk of abuse, and where they comply with the requirements of necessity and proportionality in a democratic society. In the same vein, see *Malone v. the United Kingdom*, 2 August 1984, in which the Court denied compliance with Article 8 ECHR to interception powers lacking a sufficiently clear statutory basis as regards the scope, modalities and limits of the interference.

[48] See ECtHR, GC, *Roman Zakharov v. Russia*, 4 December 2015, where the Court held that systems of secret surveillance are compatible with Article 8 ECHR only if based on an accessible and foreseeable legal framework providing effective and

adequate safeguards against arbitrariness, reaffirming that national security cannot justify generalised and uncontrolled interception of communications.

[49] See ECtHR, Szabó and Vissy v. Hungary, 12 January 2016, where the Court found a violation of Article 8 ECHR, reaffirming that national security surveillance measures must meet the standard of strict necessity, be circumscribed by clear legal limits, and be subject to independent oversight to ensure effective protection in a democratic society.

[50] See ECtHR, GC, Big Brother Watch and Others v. the United Kingdom, 25 May 2021, where the Court held that bulk interception regimes are not per se incompatible with Article 8 ECHR, provided that they are accompanied by robust end-to-end safeguards, including clear legal limits, independent authorisation and supervision, and effective oversight mechanisms capable of preventing abuse and arbitrariness.

[51] On the principle of effective judicial review as a structural component of the rule of law and an indispensable safeguard against the arbitrary exercise of public power, see K. Lenaerts, *The Rule of Law and the Coherence of the Judicial System of the European Union*, *Common Market Law Review*, vol. 44, 2007, pp. 1625 ff., where it is emphasised that the effectiveness of judicial protection constitutes an essential condition for the legitimacy of public action, particularly in fields characterised by a high degree of technical complexity and broad margins of administrative discretion.

[52] Renn, O. (2020). *Risk Governance: Coping with Uncertainty in a Complex World*. Earthscan.

[53] *Ex multis*, C. Cennamo, T. Kretschmer, P. Constantinides, C. Alaimo, J. Santalò, *Digital Platforms Regulation: An Innovation-Centric View of the EU's Digital Markets Act*, in *Journal of European Competition Law & Practice*, 2023, n. 1, pp. 44 ss.

[54] Amplius, L. TORCHIA, *Lo Stato digitale. Una introduzione*, il Mulino, Bologna, 2023, p. 77.

[55] See CJEU, *Digital Rights Ireland and Seitlinger and Others* (Joined Cases C-293/12 and C-594/12), 8 April 2014, where the Court annulled the Data Retention Directive for violating Articles 7 and 8, read in conjunction with Article 52(1) of the Charter, holding that generalised and indiscriminate retention of communications data, lacking clear limits, strict necessity, and effective safeguards, constitutes a disproportionate interference with fundamental rights.

[56] See CJEU, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Watson and Others* (Joined Cases C-203/15 and C-698/15), 21 December 2016, where the Court held that EU law precludes general and indiscriminate retention of traffic and location data, allowing data retention only where strictly necessary, targeted, time-limited, and accompanied by effective safeguards and independent review, in accordance with Articles 7, 8 and 52(1) of the Charter.

[57] See CJEU, *La Quadrature du Net and Others* (Joined Cases C-511/18, C-512/18 and C-520/18), 6 October 2020, where the Court clarified that, as a rule, Member

States may not impose generalised and indiscriminate data retention regimes, even where justified by national security considerations. The Court nevertheless held that exceptional and temporary measures of general retention may be permissible only in the presence of a serious, genuine and present or foreseeable threat to national security, provided that such measures are strictly limited in time, subject to prior or ex post review by a court or an independent administrative body, and accompanied by robust safeguards against abuse, in accordance with Articles 7, 8 and 52(1) of the Charter.

[58] M. Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Routledge, London–New York, 2008, analysing the securitisation of cyberspace and the political construction of cyber threats in the United States.

[59] According to authoritative scholarship, the comparatist is inherently attentive to cultural pluralism and to insights drawn from other disciplines, as comparative law is not a merely descriptive exercise but a methodological approach aimed at uncovering the interrelations between legal systems, institutions, and their broader socio-economic contexts. See L. Pegoraro, A. Rinella, *Sistemi costituzionali comparati*, Giappichelli, Turin, 2017, at 2.

[60] L. Collingwood, 'Privacy in Cyberworld: Why Lock the Gate After the Horse Has Bolted?' (2012) 3(1) *European Journal of Law and Technology*.

[61] See M. Mosca, *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?*, *IEEE Security & Privacy*, vol. 16, no. 5, 2018, pp. 38–41.

[62] On this issue, see Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022).