

A Proportional Approach to Cybersecurity Challenges in the Financial Sector: Ideas from Post-Quantum Cryptography Legal Analysis*

Maria Gagliardi^{1,*} and Chiara D'Elia^{1,†}

¹ Sant'Anna School of Advanced Studies, Piazza Martiri della Libertà 33, 56127 Pisa, Italy

Abstract

This preliminary analysis examines the evolution of the cybersecurity regulatory framework, with particular emphasis on the delicate balance between ensuring systemic resilience and protecting individuals, using the financial sector as a test case. The dual imperatives of regulation – namely, the maintenance of systemic stability and the protection of individual rights – present significant challenges in terms of practical implementation, especially considering emerging threats such as quantum computing. The absence of clear and detailed legislative guidance exacerbates the complexity involved in selecting appropriate technical measures. The analysis advocates for a more nuanced and proportional approach to cybersecurity, emphasizing the need for a diverse array of solutions, including post-quantum cryptography, to address both collective and sector-specific security requirements. To this end, it calls for the evolution of regulatory frameworks that provide greater clarity in harmonizing these two essential objectives.

Keywords

proportionality, security, post-quantum cryptography, risk assessment, law, financial sector

1. Introduction: Security in the Age of Quantum (Computing) and Cryptography. Legal Requirements Depending on the Level of Risk

The ongoing research on quantum computing and its legal consequences urges the consideration of the level of security which can be granted in the near future by existing cryptographic solutions.


From a technical standpoint, it is evident that the cryptographic algorithms currently in use are rapidly approaching obsolescence, as their security will soon be compromised by advancements in quantum computing. This is the reason why many standardisation institutions are trying to identify some quantum safe algorithms. At the same time, hybrid

**Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), February 03-8, 2025, Bologna, IT

* Corresponding Author.

† These authors contributed equally.

✉ maria.gagliardi@santannapisa.it (M. Gagliardi); chiara.delia@santannapisa.it (C. D'Elia)

 [0000-0003-4783-2480](https://orcid.org/0000-0003-4783-2480) (M. Gagliardi); [0009-0000-0211-7753](https://orcid.org/0009-0000-0211-7753) (C. D'Elia)



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

solutions are being imagined and tested, with the objective not only of ensuring the robustness of cryptographic protocols but also of securing quantum key distribution mechanisms.

In this context / on this background, it is necessary to consider the legal implications of the transition from a traditional to a post-quantum cryptography. Indeed, cryptography is explicitly used or implicitly considered by regulatory documents and legislative acts to achieve different goals of security and of protection of selected interests.

Of course, legislation refers to technical solutions as they are constructed and designed, as they are available. Sometimes, on the contrary there are specific solutions or specific requirements or standards referred to, because of the indication of a higher level of security or of warranty that is expected by some actors or by some measures. Where different levels of security are stipulated, it is crucial to delineate the corresponding legal requirements for cryptography across the spectrum, from traditional methodologies to quantum-safe cryptographic mechanisms. This ensures compliance with regulatory expectations while maintaining the integrity and confidentiality of protected information in the evolving landscape of cybersecurity.

Any assessment of the transition to post-quantum cryptography must be conducted with full awareness of both legal and technical constraints. In fact, the securest solutions are often also the most difficult to implement, sometimes expansive, sometimes energy consuming, sometimes requiring a great computing capacity difficult to manage in mobile devices, for instance. Therefore, it is important to understand the different domains in which a legal requirement should be applied, so that it is possible to interpret it considering all the constraints, also including the possible stronger need to protect some rights and liberties more than others. From a (cyber)security point of view, the transition to a post quantum cryptography environment can be governed and addressed also considering different levels of risks and different levels of urgency in the need or opportunity to protect information available in different contexts. It seems that security of Critical Infrastructures guides the most recent initiatives at national and European level, while other sectors are not at the centre of the strategies in the field of cryptography. While collective cybersecurity concerns are undeniably paramount in shaping policies surrounding the adoption of post-quantum cryptography, the protection of individual rights and liberties must not be overlooked. The foundational principles enshrined in international treaties, national constitutions, and corresponding legislative instruments provide essential guidance in determining which domains should be prioritized in the transition to higher levels of cryptographic security. These legal frameworks serve as a cornerstone in identifying those areas where heightened protections are most urgently required, ensuring a balanced approach that safeguards both public security interests and individual freedoms.

The research – of which this paper is a very provisional part – is ongoing, and we have not yet reached any absolute conclusions. Nevertheless, some interesting facts can be identified and used to show how it can be possible to clarify in which cases legislation gives

us evidence of the need to use the strongest tools of security. An example comes from the financial sector.

2. Evolution of EU Cybersecurity Regulation: Ensuring Resilience and Security in a Digital Financial Landscape

The global financial landscape has undergone a profound transformation in recent decades, driven by the rapid advancement of digital technologies. The widespread adoption of FinTech solutions, the proliferation of electronic payment systems, and the ascent of cryptocurrencies have fundamentally reshaped the interactions between financial institutions and consumers. These innovations have introduced unprecedented efficiencies and opportunities; however, they have also given rise to significant challenges concerning consumer protection, market integrity, and the security and continuity of financial operations. In this evolving context, regulatory frameworks assume a pivotal role in ensuring both the safeguarding of users and the stability of financial markets.

The evolution of EU regulations on cybersecurity, particularly with the transition from Directive (EU) 2016/1148 (NIS 1) to Directive (EU) 2022/2555 (NIS 2), has marked a substantial paradigm shift in the legal approach to protecting critical infrastructures and essential services. This transformation has been further reinforced by the introduction of the Digital Finance Package – and, in particular, Regulation (EU) 2022/2554 on Digital Operational Resilience Act (DORA) and Regulation (EU) 2023/1114 on Markets in Crypto-Assets Regulation (MiCAR) – has further integrated this transformation, expanding the focus from merely protecting individual actors to pursuing the so-called operational resilience of entire economic sectors. This evolution reflects the growing interdependence of modern economies and societies, where the secure and continuous operation of strategic sectors is crucial for ensuring overall stability.

From a legal standpoint, this shift signifies a transition from a protection model centered on individual operators – such as financial service consumers – to a systemic framework that prioritizes the resilience of interconnected actors within the financial and digital ecosystem. The overarching objective is to preserve market continuity and safeguard the broader societal and economic order.

This regulatory progression carries profound implications not only for the protection of infrastructures but also for the formulation of technical standards, security protocols, and contingency planning measures. These must be dynamically adapted to an ever-evolving regulatory landscape to ensure the continued efficacy and robustness of cybersecurity governance within the European Union.

More specifically, Directive NIS 1 introduced the first comprehensive European legal framework for the security of networks and information systems, focusing on the protection of essential services such as energy, transportation, healthcare, and digital infrastructures. The goal of NIS 1 was twofold: first, to ensure the resilience and security of individual

providers of critical services, and second, to achieve a broader protective effect by reinforcing the stability of the entire sector through the resilience of its constituent entities. In this context, the legal approach was primarily focused on the individual responsibility of service providers, who were required to adopt appropriate security measures to ensure operational continuity and reduce the risk of disruption to essential services. At the regulatory level, NIS 1 set requirements for the adoption of cybersecurity measures, the management of cyber risks, and the reporting of significant incidents. The regulatory incentive was designed to establish a minimum threshold of technical and organizational security standards for individual entities, thereby fostering a preventive approach aimed at minimizing the risk of cascading failures across the broader ecosystem. However, this individualistic approach proved insufficient in addressing the growing interconnectivity of systems and the increasing complexity of supply chains. The evolving cybersecurity landscape necessitated a paradigm shift, extending protection beyond isolated entities to a collective and systemic level, ensuring that the security and resilience of the entire digital and operational infrastructure could be effectively safeguarded against emerging threats.

With Directive NIS 2, a paradigm shift occurred, with the goal of strengthening operational resilience and cybersecurity at the systemic level. Unlike its predecessor, NIS 2 adopts a more comprehensive and inclusive framework, recognizing that cybersecurity cannot be effectively ensured by focusing solely on individual operators. Protection is no longer focused solely on the individual operator, but on the entire sector or market, and includes entities that, while not traditionally considered “essential” have a significant impact on economic and social stability. Stricter obligations are imposed in terms of cybersecurity governance and risk management, aiming to reduce vulnerabilities at the system level and ensure operational continuity even in the case of cyberattacks or incidents. The required security measures are detailed and include the protection of digital infrastructures, the adoption of incident response plans, the management of third parties (including external vendors), and the strengthening of recovery capabilities.

DORA and MiCAR align with the overarching framework of operational resilience and cybersecurity but are specifically tailored to the financial sector. Similar to NIS 2, these Regulations are distinguished by their in-depth focus on the management of cyber risks and operational resilience in a sector where service disruptions could have global systemic effects. The regulatory measures set forth under DORA and MiCAR encompass a wide array of obligations, including the protection of information technology infrastructures, the mitigation of risks arising from third-party service providers—such as cloud computing services—and the implementation of robust continuity and recovery plans. These requirements are designed to ensure the financial sector’s resilience in the face of critical incidents, thereby preserving market stability and public confidence.

In the contemporary digital landscape, information security represents a fundamental pillar for the protection of personal data, operational continuity, and the stability of strategic sectors. This concept, intrinsically relational, must be constantly reconsidered considering

technological advancements, the nature of data processed, and the specific processing operations carried out. At the European level, the regulatory framework underscores the necessity of adopting a proactive, resilient, and adaptive approach to information security management—one that extends beyond individual protection to encompass the broader imperative of systemic continuity and stability. This perspective fits into a broader operational resilience strategy, which considers security not only as individual protection but also as a guarantee of continuity and systemic stability. The advent of advanced technologies, particularly quantum computers, represents a crucial challenge that requires the updating of security measures, including the adoption of post-quantum cryptography algorithms.

3. Adapting the Evolving Cyber Threats: The Transition to Post-Quantum Security and Resilient Systems

The evolution of cyber threats progresses in tandem with technological advancements, necessitating the continuous enhancement of protective measures to safeguard digital infrastructures and sensitive information. Security practices that were once deemed sufficient have, over time, been rendered inadequate in the face of increasingly sophisticated attack methodologies. For instance, whereas the reliance on simple passwords may have been considered an acceptable security standard two decades ago, the proliferation of advanced cyber threats—such as phishing schemes and brute force attacks—has necessitated the widespread adoption of multi-factor authentication (MFA) as a fundamental safeguard against unauthorized access.

A particularly critical dimension of this ongoing evolution is the transition from traditional cryptographic methodologies to post-quantum cryptographic frameworks. The advent of quantum computing poses a significant challenge to the security of widely used encryption algorithms, such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), as these cryptographic mechanisms rely on mathematical problems that quantum computers could potentially solve with unprecedented efficiency. In anticipation of this paradigm shift, post-quantum cryptography seeks to establish and standardize cryptographic algorithms that are inherently resistant to quantum-enabled attacks. The objective is to ensure that the confidentiality, integrity, and authenticity of digital communications and transactions remain uncompromised in the era of quantum computing, thereby preserving an adequate and future-proof level of cybersecurity.

The protection of information must be proportional to the sensitivity of the data being processed. Personal data encompass a broad spectrum, ranging from relatively less sensitive identifiers – such as names and addresses – to highly confidential categories, including health records and financial information. European regulations, such as the Reg. (UE) 2016/679 (General Data Protection Regulation – GDPR), impose differentiated protection levels based on the nature of the data, requiring stricter measures for sensitive data. Under

the GDPR, the degree of protective measures mandated is directly proportional to the nature and potential impact of data exposure. More stringent safeguards are required for the processing of special categories of personal data, as defined under Article 9 of the Regulation, to mitigate the heightened risks associated with unauthorized access, misuse, or breaches. These obligations underscore the principle of data minimization and security by design, ensuring that entities handling sensitive information implement appropriate technical and organizational measures to uphold the confidentiality, integrity, and availability of such data in accordance with the highest legal and ethical standards

Banking transactions and communications between financial institutions, such as SWIFT transactions, are currently protected by RSA or ECC encryption. However, these encryption methods, which rely on computational problems that are intractable for classical computers, may become vulnerable to decryption by quantum computers. In the future, post-quantum cryptography techniques (among which new algorithms lattice-based, hash-based, or code-based) will be crucial for ensuring security. Financial data stored (such as information on bank accounts, contracts, and past transactions) must be protected against potential attacks in a quantum context in the coming decades. This requires the adoption of quantum-proof encryption algorithms at least at some points of the security process. Similarly, the security of blockchain networks and cryptocurrency transactions, which rely on asymmetric encryption, will be fundamentally challenged by quantum computing advancements. The adoption of post-quantum cryptographic frameworks for blockchain infrastructures is therefore crucial to preserving the integrity, authenticity, and non-repudiation of digital asset transactions in the face of emerging threats.

On the other hand, passwords are still a very common method for protecting access to computer systems, but compared to encryption, they provide lower protection, especially if not managed properly (e.g., with weak passwords or reused credentials). Many financial systems use passwords to access online portals, mobile banking apps, and trading systems. The security of these passwords can be enhanced with techniques such as two-factor authentication (2FA), which adds an additional layer of protection against unauthorized access. For access to bank accounts, it is recommended to use a complex password, combined with biometric authentication systems or OTP (One-Time Password). This is particularly useful when protecting direct access to accounts by legitimate users. It is not yet clear whether post quantum cryptography should be applied to one or more of these security measures.

Even within financial institutions, many still rely on passwords to access internal systems, such as CRMs, data management systems, or trading terminals.

The regulatory framework suggests a distinction between protection plans that can be divided into “systemic” and “individual” plans, each serving a distinct but complementary function within the broader context of cybersecurity and operational resilience.

Systemic plans are designed to ensure the resilience of the entire ecosystem, particularly in circumstances where cyberattacks involve multiple actors or extend across

interconnected supply chains. These plans are exemplified by regulations such as NIS 2 and DORA, which seek to safeguard the overall stability of critical sectors and markets. Systemic protection strategies focus on collaborative measures, including the establishment of monitoring systems, coordination mechanisms, and common response frameworks. The objective is to ensure that the broader system, encompassing various interconnected entities, remains resilient and operational even in the face of large-scale disruptions or coordinated cyber threats.

In contrast, *individual plans* are tailored to the specific needs of individual organizations, with a focus on protecting their unique infrastructures, data, and operations. These plans are developed based on a comprehensive risk assessment of each actor's vulnerabilities and the specific threats they are most likely to face. Measures such as multi-layered defense systems, the strengthening of IT infrastructure resilience, and the formulation of recovery plans are integral components of these individual protection strategies. These plans prioritize the security and continuity of each organization, ensuring that it can recover quickly from incidents and maintain the integrity of its operations.

Considering the evolving cybersecurity landscape, further analysis is necessary to determine how these distinct protection plans can or should incorporate post-quantum cryptographic solutions. As quantum computing technology advances, it is imperative to reassess existing protection strategies to include quantum-resistant measures, ensuring that both systemic and individual plans are equipped to counter emerging threats posed by quantum-enabled attacks. This evolution will require a careful examination of the potential vulnerabilities introduced by quantum computing and the implementation of cryptographic algorithms that can withstand such advanced computational capabilities.

Further analysis is needed to clarify how the different plans can or should include post quantum solutions.

4. Concluding remarks: the need of proportionality

Cybersecurity European regulation aims at preserving the integrity and the continuity of critical services and infrastructures. The perspective is broad, because it is not excluded that an attack can cause some damage or interruption. The main goal of regulation is to assure that the interruption can be followed by a new start and that damages are not disruptive. In other words, realistically it is allowed and considered acceptable even some bug, until it is detected and can be corrected. In this perspective, the systems can go on functioning as and better than before. Thus, the integrity of critical infrastructures is a means to assure the right to access services of general economic interest, such as healthcare or financial services. There are not primarily individual rights at stake. On the contrary, when regulation considers the risks and threats for digital information, as seen in the financial sector, the dimension of protection relates to the rights to liberty and to security, as well as the right to respect for private and family life. This perspective is often intertwined with the previous one also in cybersecurity acts, but it is more evident in sectorial legislation and regulation.

The major consequence of this sort of dualism in the main objectives of regulation is that it can highlight differences in the practical applications and choices, for instance in the technical and organisational measures that different actors are in charge to adopt, the technical standards and requirements to implement, and so on. In other words, sometimes it could be said that some requirements posed by legislation to assure the continuity of systems should be afforded by accountable actors even if they could appear as high level and very expensive, for instance. The same solutions can be considered useful and encouraged, but not required as compulsory, when they should serve to protect (only) individual rights.

Thus, the dualism inherent in the objectives of cybersecurity regulation highlights important distinctions in the practical application of systemic and individual protection plans. While both serve the overarching goal of ensuring resilience and security in an era of increasingly sophisticated cyber threats, their implementation can diverge significantly. These differences often arise in the technical and organizational measures required, the technical standards and requirements to be implemented, and the allocation of responsibilities among actors.

For instance, systemic plans, which focus on the continuity and stability of interconnected infrastructures, may impose high-level, standardized requirements that are both extensive and costly. These measures, such as the mandatory collaboration protocols established under the NIS 2 Directive or the stress testing obligations mandated by the DORA Regulation, are critical to ensuring the resilience of critical services and maintaining the stability of the broader ecosystem. Accountable actors, such as financial institutions or cloud service providers, are required to adopt these measures regardless of their cost or complexity, because their failure could result in cascading disruptions across multiple sectors.

In contrast, individual protection plans are more targeted, addressing the specific risks and vulnerabilities of single organizations. While systemic measures may indirectly benefit the protection of individual rights, such as privacy or data security, individual plans are specifically tailored to ensure compliance with legal requirements like the GDPR or the Payment Services Directive 2 (PSD2). These plans allow for greater flexibility in implementation, with organizations encouraged, but not always mandated, to adopt cutting-edge solutions like post-quantum encryption or multi-factor authentication.

Ultimately, systemic and individual cybersecurity protection plans serve as two interdependent pillars of the regulatory framework. While systemic plans create a resilient foundation by addressing the stability of interconnected systems, individual plans refine this approach by tailoring measures to the unique risk profiles of organizations. Both approaches must evolve in harmony to address the growing complexity of cyber threats, with legislation providing clear guidance to reconcile their objectives and ensure consistency in their implementation.

The distinction between systemic and individual protection plans is often blurred in practice, as the objectives of one frequently influence the other. For instance, systemic mandates like DORA's stress testing requirements can lead to adjustments in individual

institutions' protection plans, such as revising internal policies for third-party risk management. Similarly, innovations developed at the individual level, such as post-quantum encryption in banking applications, may later evolve into systemic standards. Despite being foundational to the regulatory framework, this distinction is challenging to maintain due to the lack of clarity and specificity in legislation regarding overarching objectives and the precise goals of individual components. Furthermore, the absence of detailed guidance or concrete examples for selecting technical solutions leaves room for interpretation, often resulting in inconsistent implementation across sectors.

However, the legal frameworks that govern these protection plans do not always provide clear, explicit definitions of their specific objectives or offer detailed technical guidance. For example, while the NIS 2 Directive establishes high-level requirements related to incident reporting and risk management, it delegates the task of implementing these measures to national authorities and individual organizations. This delegation creates challenges in aligning systemic and individual measures, particularly as emerging threats—such as the advent of quantum computing—pose new and unforeseen risks. In response to these challenges, regulatory bodies and standardization organizations, such as the National Institute of Standards and Technology (NIST) and the European Union Agency for Cybersecurity (ENISA), are working to establish more granular, technical guidelines. These bodies aim to connect specific technical solutions, such as hybrid cryptographic systems (which combine classical and quantum-resistant algorithms), to clearly defined protection objectives. By doing so, they seek to provide more concrete directions for organizations to follow, ensuring that both systemic and individual measures remain aligned and effective, even as the landscape of cyber threats continues to evolve..

This ambiguity complicates the assessment of both the level and urgency of risks across different scenarios. For example, while systemic plans focus on ensuring the resilience of interconnected infrastructures, their broad scope can make it challenging to identify which measures are most critical for specific threats, such as those posed by the advent of quantum computing. Similarly, individual plans, while tailored to the unique circumstances of specific organizations, may lack sufficient alignment with broader systemic goals. This misalignment can lead to potential gaps in the collective defense mechanism, undermining the overall security posture of the entire ecosystem. In such cases, an organization's efforts to protect its own assets may inadvertently fail to integrate with the larger network of protections, potentially leaving vulnerabilities in the collective defense against cyber threats.

The need for precision becomes even more pressing considering emerging technologies, such as quantum computing, which threaten to disrupt traditional cryptographic safeguards. The transition to post-quantum cryptography is a case in point: systemic plans, guided by institutions like NIST and the European Commission (*e.g.*, through its 2024 recommendations), emphasize the development and standardization of quantum-resistant algorithms as general tools to address quantum risks. However, the practical application of these cryptographic advancements necessitates a more granular and sector-specific analysis at the individual level. The risks posed by quantum computing vary significantly across

industries – ranging from financial services and healthcare to government and defense – each of which has distinct security requirements and operational constraints. Consequently, a one-size-fits-all approach to post-quantum security is insufficient. Instead, regulatory frameworks must balance universal standardization with context-specific implementation, ensuring that organizations adopt quantum-resistant solutions in a manner proportionate to their particular risk exposure, data sensitivity, and operational needs.

Ultimately, the effectiveness of cybersecurity regulation depends on the ability to harmonize systemic and individual responsibilities. Systemic plans provide the foundation for ecosystem-wide resilience, while individual plans address unique organizational vulnerabilities. For this delicate equilibrium to be effectively maintained, the regulatory landscape must evolve to provide greater clarity and precision in defining the scope of obligations and the methodologies for implementation. This necessitates the establishment of detailed, well-articulated criteria for the selection and deployment of technical safeguards, ensuring a proportionate and risk-based approach to cybersecurity governance. By offering comprehensive guidance on regulatory compliance, standardization of security protocols, and the integration of advanced protective mechanisms – Including post-quantum cryptographic solutions – regulatory frameworks can equip both systemic and individual actors with the requisite tools to anticipate, counteract, and withstand emerging technological threats. In doing so, they will reinforce the cohesion, adaptability, and efficacy of cybersecurity protections, fostering a legal and technical infrastructure capable of withstanding the evolving cyber threat landscape.

In conclusion, this kind of distinction is not easy to draw, because the legislations are never clear and explicit neither in defining the specific goals of legislation in se and of its parts; nor in giving indication, examples and specifications about the technical solutions to select, and about the criterions to use in the selection of any of them among a group of solutions and standards. Here lies the difficulty to correctly assess both the level of risk and of its urgency in different scenarios, in which to envisage the future use of quantum computing. The selection of post quantum cryptographic solutions is pursued by standardisation institutions (for instance NIST) looking at their efficacy, that means strength and trustworthiness of algorithms and relied upon by European institutions (see for instance the European Commission Recommendation (EU) 2024/1101 of 11 April 2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography) as general tools to face the risks created or aggravated by quantum computing capabilities. What is needed in addition is a more granular analysis of which level of protection is concretely affordable in a specific sectorial situation, considering both the risks and the rights to protect. Rather than imposing a uniform, one-size-fits-all requirement, the regulatory approach should instead develop a structured portfolio of cryptographic and cybersecurity solutions. This portfolio should encompass post-quantum cryptography, hybrid cryptographic mechanisms, and other complementary mitigation measures, allowing for a balanced integration of both systemic resilience (ensuring the continuity and security of critical infrastructures) and sector-specific or individual protections (addressing the

particular vulnerabilities of specific industries or entities). The next step is to provide useful guidelines to match technical solutions with specific protection goals in the framework of existing and forthcoming regulation.

Acknowledgements

This work was supported in part by the EU Horizon Europe Framework Program under Grant Agreement n° 101119547 (PQ-REACT).

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] N. Abriani, G. Schneider (2021), *Diritto delle imprese e intelligenza artificiale – Dalla Fintech alla Corptech*, Bologna.
- [2] J.A.R. Awad, R.M. Rojas (2024), Digital transformation influence on organisational resilience through organisational learning and innovation, *Journal of Innovation and Entrepreneurship*, 13:69
- [3] L. Bruno, I. Spano (2021), Post-Quantum Encryption And Privacy Regulation: Can The Law Keep Pace With Technology?, *SSRN Electronic Journal*, 10.2139/ssrn.3920272;
- [4] C. P. Buttigieg, B. B. Zimmermann, The digital operational resilience act: challenges and some reflections on the adequacy of Europe’s architecture for financial supervision, in *ERAForum*(2024)25:11–28
- [5] C. Calliess, A. Baumgarten (2020), Cybersecurity in the EU the Example of the Financial Sector: A Legal Perspective, 21 *German LJ* 1149.
- [6] F. Capriglione, N. Casalino (2020), Impacts, Challenges and trends of Digital Transformation in the Banking Sector, in *Law and Economics Yearly Review*, 341 ff.
- [7] F. Capriglione (2021), The Financial System Towards a Sustainable Transition, in *Law and Economics Yearly Review*, 10, 1, p. 1.
- [8] F. Casarosa, G. Comandé (2024), Aspettando la NIS2: ovvero il diritto privato della cybersicurezza, in *Il diritto dell’informazione e dell’informatica*, pp. 29-53.
- [9] D. Chawla, P.S. Mehra (2023), A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions, *Internet of Things*, <https://doi.org/10.1016/j.iot.2023>.
- [10] G. Comandé, M. Varilek (2024), The many features which make the eIDAS 2 Digital Wallet either risky or the ideal vehicle for the transition to post-quantum encryption, *Computer Law & Security Review*, Vol 54, <https://doi.org/10.1016/j.clsr.2024.106022>.
- [11] ENISA (2024), Cryptographic. Products and services market analysis, available on <https://www.enisa.europa.eu/publications/cryptographic-products-and-services-market-analysis>.

- [12] ESMA (2020), Final Report Guidelines on Outsourcing to Cloud Service Providers, available on https://www.esma.europa.eu/sites/default/files/library/esma50-157-2403_cloud_guidelines.pdf.
- [13] European Central Bank (2018), Cyber resilience oversight expectations for financial market infrastructures, available on https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.
- [14] W.G. Johnson (2019), Governance Tools for the Second Quantum Revolution, 59 *Jurimetrics*, 487-521.
- [15] E. Kosta (2023), Security of processing and data Breach Notification, available on https://www.edpb.europa.eu/system/files/2024-01/one_stop_shop_case_digest_security_data_breach_en.pdf.
- [16] S. Kourmpetis (2023), Management of ICT Third Party Risk Under the Digital Operational Resilience Act, in Böffel L. – Schürger J. (eds), *Digitalisation, Sustainability, and the Banking and Capital Markets Union: Thoughts on Current Issues of EU Financial Regulation*, Cham, 211 ff.
- [17] L. Rand, T. Rand (2022), The “Prime Factors” of Quantum Cryptography Regulation, 3 *Notre Dame Journal on Emerging Technologies*, 38 ff.
- [18] M. Leistner (2021), The Commission’s Digital Markets and Services Package – New Rules for Big Tech and Big Data, in 70 *GRUR International*, p. 515.
- [19] M. Leo (2020), Operational Resilience Disclosures by Banks: Analysis of Annual Reports, in *Risks*, 8(4), 128. 8.
- [20] C.M. Magnusson C.M., D. Blume (2022), Digitalisation and Corporate Governance, OECD Corporate Governance Working Papers n. 26, available on https://www.oecd-ilibrary.org/governance/digitalisation-and-corporate-governance_296d219f-en.
- [21] U. Malvagna (2023), Digital securities: prime note sul decreto di attuazione del DLT Pilot, in *Rivista di Diritto Bancario*.
- [22] M. Negreiro (2019), ENISA and a new cybersecurity act, European Parliamentary Research Service.
- [23] M. Negreiro (2023), The NIS2 Directive, European Parliamentary Research Service, February 2023.
- [24] S.Y. Peng (2018), Private Cybersecurity Standards: Cyberspace Governance, Multistakeholderism, and the (Ir)Relevance of the TBT Regime, 51 *Cornell Int’l LJ* 445.
- [25] M. Piani, M. Mosca (2023), Quantum Threat Timeline Report 2023, Global Risk Institute in Financial Services (GRI), <https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/>.
- [26] G. Schneider (2022), La resilienza operativa digitale come materia di corporate governance: prime riflessioni a partire dal DORA, in *Corporate Governance*, 559-563.
- [27] L.J. Trautman, K. Altenbaumer-Price (2011), The Board’s Responsibility for Information Technology Governance, in *John Marshall Journal of Computer & Information Law*, 29, 313 ff.

- [28] L.J. Trautman, P. Ormerod (2017), Corporate Directors' and Officers' Cybersecurity Standard of Care: the Yahoo Data Breach, in *American University Law Review*, 66, 1321 ff.
- [29] L.J. Trautman L.J. et al (2020), Governance of the Internet of Things (IoT), in *Jurimetrics*, 60, 315 ff.
- [30] L.J. Trautman, K.A. Price (2011), The Board's Responsibility for Information Technology Governance, in *John Marshall Journal of Computer & Information Law*, 29, 313 ff.
- [31] D.A. Zetsche, D.W. Arner D.W, R.P. Buckley (2020), Decentralized Finance (DeFi), in *Journal of Financial Regulation*, 6, pp. 172 ff.
- [32] D.A. Zetsche, R.P. Buckley, D.W. Arner, J.N. Barberis (2017), From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance, EBI Working Paper Series, 6.
- [33] A. Zygierewicz (2020), Directive on security of network and information systems (NIS Directive), European Parliamentary Research Service, EU Parliament.