Articles

Studia Iuridica Lublinensia vol. 35, 1, 2026
DOI: 10.17951/sil.2026.35.1.29-39

Dominik Bierecki
Pomeranian University in Słupsk, Poland
ORCID: 0000-0001-6993-3974
dominik.bierecki@upsl.edu.pl

The Relevance of the Proportionality Principle under DORA for the Interpretation of the Artificial Intelligence Act in the Context of AI-Based ICT Systems

Znaczenie zasady proporcjonalności wynikającej z DORA dla interpretacji aktu o sztucznej inteligencji w kontekście systemów ICT opartych na sztucznej inteligencji

ABSTRACT

This article constitutes a scientific and conceptual legal study examining the relationship between cybersecurity obligations applicable to high-risk AI systems and sector-specific ICT risk management in the financial sector under EU law. The research problem concerns the interpretation of the reference to "relevant circumstances and risks" in Article 15 (5) of the Artificial Intelligence Act (AI Act) when high-risk AI systems operate as components of ICT infrastructure within financial institutions. The article argues that these circumstances and risks should be interpreted in light of the proportionality framework laid down in Article 4 of the Digital Operational Resilience Act (DORA). The aim of the research is to determine whether the proportionality criteria established in DORA may function as an interpretative benchmark for assessing the adequacy of cybersecurity measures required under the AI Act. The main thesis advanced is that the proportionality criteria concerning the size of the entity, its risk profile, and the nature, scale and complexity of its activities provide objective parameters for identifying the "relevant circumstances and risks" referred to in Article 15 (5) of the AI Act in the financial sector. The originality of the study lies in demonstrating the systemic complementarity between horizontal AI regulation, which applies regardless of the status of the entity using the AI system, and the sector-specific ICT operational resilience rules. The research is conducted at the level

CORRESPONDENCE ADDRESS: Dominik Bierecki, PhD, Dr Habil., Associate Professor, Attorney at Law, Pomeranian University in Słupsk, Arciszewskiego 22A, 76-200 Słupsk.

of EU law and contributes to the doctrinal interpretation of emerging EU digital regulations, offering practical relevance for supervisory authorities and financial institutions implementing cybersecurity obligations for AI systems.

Keywords: Artificial Intelligence Act; Digital Operational Resilience Act; DORA; proportionality principle; cybersecurity of AI systems; ICT risk management in the financial sector

INTRODUCTION

In terms of the cybersecurity, the scopes of regulation of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)[1] and Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)[2] overlap when the financial institution deploys high--risk AI systems as part of information and communication technologies (ICT). The purpose of the study is to determine whether, in this case, the proportionality principle of Article 4 DORA can apply to the requirement of cybersecurity of the high-risk AI system. The research thesis of the article argues that, although Article 4 DORA does not provide a formal legal basis for the proportionate application of the AI Act, it nevertheless produces a functional and systemic linkage between the two regimes. In particular, the AI Act's risk classification framework becomes a relevant reference point for the proportional application of DORA to AI-based ICT systems. The article was prepared by the dogmatic-legal method.

RESEARCH AND RESULTS

The principle of proportionality constitutes a treaty-based general principle of EU law. It is expressly enshrined in Article 5 (4) of the Treaty on European Union[3] and requires that the content and form of Union action do not exceed what is necessary to achieve the objectives of the Treaties.[4] The case of proportionality

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (OJ L 333/1, 27.12.2022).

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (OJ L 2024/1689, 12.7.2024).

[3] OJ C 326, 26.10.2012.

[4] E. Herlin-Karnell, *EU Data Protection and the Principle of Proportionality*, "Nordic Journal of European Law" 2021, vol. 4(2), p. 66.

in cybersecurity exists in various EU regulations. It has a broader sense, even in the context of fundamental and human rights.[5] Rather than imposing uniform technical safeguards, the EU legislator consistently requires the adoption of appropriate and proportionate technical and organizational measures. It reflects differences in system criticality, complexity, and potential societal impact, but also in the scale and operational risks of the adopting party. In relation to cybersecurity, the principle of proportionality operates as a calibration mechanism rather than a limitation of regulatory scope. It is connected with the risk-based approach of the EU legislator to the matter of cybersecurity. By that, it allows obligations to be adjusted to the intensity and likelihood of the regulated risk. It is one of the forms of the principle of proportionality.[6]

The examples of application of the treaty-based principle of proportionality in the legal acts of the EU on cybersecurity include: Directive (EU) 2022/2555 (NIS 2 Directive),[7] Regulation (EU) 2019/881 (Cybersecurity Act),[8] Regulation (EU) 2022/2554 (DORA), and Regulation (EU) 2024/1689 (AI Act). The NIS 2 Directive gives essential and important entities a right to adopt technical, operational and organizational measures to manage cybersecurity risks in an appropriate and proportionate way (Article 21 (1) of Directive (EU) 2022/2555). The Cybersecurity Act requires proportionality through differentiated assurance levels in EU cybersecurity certification schemes, whereby the depth and stringency of security requirements increase in line with the intended use and risk profile of the ICT product, service or process (Article 46 (2) of Regulation (EU) 2019/881). DORA is the most demanding of these legal acts in the requirement of proportionality of application of its provisions.[9] Article 4 of Regulation (EU) 2022/2554 reflects a sector-specific application of proportionality in the financial sector. The provision requires that ICT risk management obligations be applied in a manner proportionate

[5] T.D. Thai Thi, P.D. Gia, *Balancing the Right to Access Information, the Right to Privacy, the Right to Personal Data Protection, and the Right to Be Forgotten in the Digital Age: The Case of Vietnam*, "Prawo i Więź" 2024, no. 6, pp. 709–730; P. De Hert, V. Papakonstantinou, *Does the Future Hold More Rights or More Proportionality? The GDPR-Message*, "European Data Protection Law Review" 2023, vol. 9(4), pp. 393–398.

[6] J. Maliszewska-Nienartowicz, *Zasada proporcjonalności jako podstawa oceny legalności ograniczeń swobód rynku wewnętrznego Unii Europejskiej*, Toruń 2020, pp. 77–84.

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333/80, 27.12.2022).

[8] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (OJ L 151/15, 7.6.2019).

[9] P. Pelc, *Zasada proporcjonalności w DORA*, "Cybersecurity and Law" 2024, no. 2, pp. 207–218.

to the size and overall risk profile of the financial entity, as well as the nature, scale and complexity of its activities and ICT systems.[10] Proportionality in DORA is not limited to the manner in which ICT risk management obligations are applied, but also manifests itself at the level of regulatory scope. This is reflected in the national options allowing Member States to exclude certain financial institutions from the application of the Regulation, thereby operationalising proportionality in light of their limited risk profile and systemic relevance (Article 2 (4) DORA). The proportionality principle in DORA also manifests itself through exclusions based on objective criteria such as capital size, assets under management, or micro-enterprise status (Article 2 (3) DORA). Exclusions based on these criteria result in application of a simplified ICT risk management framework under Article 16 DORA.[11]

The AI Act adopts a comparable logic in Article 15.[12] Under this provision, high-risk AI systems should be designed with appropriate levels of robustness, accuracy, and cybersecurity. However, Article 15 of the AI Act explicitly requires that technical solutions should be adapted to the circumstances and risks associated with the AI systems. This formulation embeds proportionality directly into the cybersecurity obligations applicable to AI systems. In this context, proportionality functions as an interpretative principle. It guides regulators and regulated entities to align cybersecurity measures with demonstrable risk, thereby avoiding both under-regulation of critical systems and over-regulation of low-risk deployments. Article 4 DORA and Article 15 of the AI Act are part of a broader EU regulatory paradigm in which cybersecurity obligations are systematically calibrated through proportionality, reflecting risk, complexity, and societal impact rather than imposing uniform technical requirements.

DISCUSSION

High-risk AI systems under the AI Act are not ICT systems by definition. According to Article 3 (1) of the AI Act, an AI system means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content,

[10] G. Tolino, G. Punia, J. Emmanuel, *Report: EU Digital Operational Resilience Regulation (DORA)*, "Global Privacy Law Review" 2025, vol. 6(1), p. 14.

[11] D. Bierecki, *Zasada proporcjonalności w stosowaniu rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience Act – DORA)*, "Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2024, no. 3, pp. 5–13.

[12] D. Bierecki, C. Gaie, M. Karpiuk, J. Langlois-Berthelot, *Creating Resilient Artificial Intelligence Systems: A Responsible Approach to Cybersecurity Risks*, "Prawo i Więź" 2025, no. 5, pp. 138–140.

recommendations, or decisions that can influence physical or virtual environments. The rules for classifying high-risk AI systems are set out in Article 6 (1) of the AI Act. According to this provision, regardless of whether an AI system is placed on the market or put into service, such a system is considered a high-risk system if two conditions are met: (1) the AI system is intended to be used as a safety-related component of a product covered by EU harmonisation legislation, or the AI system itself is such a product; (2) the product of which the AI system is a safety-related component, or the AI system itself as a product, is subject to third-party conformity assessment under Union harmonisation legislation in relation to its placing on the market or putting into service. In addition to these systems, AI systems referred to in Annex III to the AI Act (Article 6 (2) of the AI Act) are considered high-risk systems.[13] In the context of financial institutions, the relevant Annex III categories include: (1) AI systems intended to be used for assessing the creditworthiness of natural persons or determining their credit score, with the exception of AI systems used for detecting financial fraud, and (2) AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life insurance and health insurance.

By contrast, EU law does not provide a uniform definition of an ICT. Most relevant to this discussion is the definition of an ICT asset included in Article 3 (7) DORA. Under this provision, ICT asset means a software or hardware asset in the network and information systems used by the financial entity. In the literature, ICT is defined as the means that humans use for creating, disseminating, and consuming information about the world.[14]

However, when high-risk AI systems are deployed as part of an organisation's (financial institution's) information and communication technologies, they qualify as ICT and may therefore fall within sector-specific regimes such as DORA.[15] Where high-risk AI systems are deployed as part of ICT supporting the operations of financial entities, the proportionality principles under DORA and the AI Act operate in parallel. DORA and the AI Act overlap not in their material scope, but in their object of regulation, addressing different categories of risk arising from the use of AI-based ICT systems by financial institutions. While each regulation retains its autonomous scope, both rely on a shared risk-based methodology, resulting in a functional convergence of cybersecurity expectations without formal cross-application of legal norms. Consequently, applying the principle of systematic interpretation, it should be recognized that the provisions of DORA and the AI Act

[13] D. Bierecki, M. Czuryk, C. Gaie, J. Langlois-Berthelot, *Sovereignty by Design: Embedding Fiscal Risk Intelligence in Europe's Defence-Digital Strategy*, "Prawo i Więź" 2026, no. 1, pp. 151–152.

[14] C. Fuchs, *Information Technology and Sustainability in the Information Society*, "International Journal of Communication" 2017, vol. 11, p. 2433.

[15] D. Bierecki, M. Karpiuk, C. Melchior, N. Strizzolo, *Security in the Era of Threats Occurring in Cyberspace*, "Prawo i Więź" 2025, no. 4, pp. 80–82.

should be interpreted in a manner that creates a coherent and meaningful whole within the EU cybersecurity regulatory framework.[16]

Article 15 (5) of the AI Act establishes an obligation to ensure that high-risk AI systems are resilient to unauthorized interference, while providing that the scope of the cybersecurity measures applied should be adapted to the relevant circumstances and level of risk. When high-risk AI systems are deployed by financial institutions, the assessment of such circumstances and risks cannot be conducted in isolation from sector-specific regulations governing ICT risk management. In this context, Article 4 DORA, which sets out proportionality criteria relating to the size of the entity, its overall risk profile, and the nature, scale and complexity of its activities, constitutes an important point of reference for the interpretation of the requirements laid down in Article 15 (5) of the AI Act.

Consequently, the proportionality criteria deriving from Article 4 DORA should be taken into account when assessing the adequacy of cybersecurity measures applied to high-risk AI systems used by financial institutions, as in this sectoral context they constitute objective "relevant circumstances and risks" within the meaning of Article 15 (5) of the AI Act. As a result, notwithstanding the use of AI systems classified as high-risk, financial institutions operating under simplified or proportionately adjusted ICT risk management frameworks (Article 16 DORA) will not be required to implement cybersecurity measures exceeding their actual risk profile and organizational capacities.

Such an approach makes it possible to preserve coherence between the horizontal regulatory regime established by the AI Act and the sector-specific system of digital operational resilience laid down in DORA, without leading to an unjustified accumulation of regulatory obligations. At the same time, the proportionality criteria set out in Article 4 DORA cannot be interpreted as limiting the autonomous application of the AI Act or as a basis for lowering the minimum security standards required under Article 15 (5) thereof. These criteria are solely a tool for contextual and coherent interpretation in light of the sectoral framework for ICT risk management.

If the proportionality criteria laid down in Article 4 DORA were not taken into account when interpreting Article 15 (5) of the AI Act in relation to high-risk AI systems operating within the ICT frameworks of financial institutions, the assessment of the adequacy of cybersecurity measures would necessarily be conducted in isolation from sector-specific operational risk management regimes. This would result in autonomous and horizontal assessment of AI-related risk, detached from the structural differences between financial entities stemming from their size, risk profile, scale of activities, and systemic relevance.

[16] J. Helios, W. Jedlecka, *Wykładnia prawa Unii Europejskiej ze stanowiska teorii prawa*, Wrocław 2018.

In practical terms, this approach would entail the application of a uniform, high level of cybersecurity safeguards to all financial institutions deploying AI systems classified as high-risk, irrespective of whether they operate under simplified ICT risk management frameworks (Article 16 DORA). Such a regulatory outcome would decouple the requirements of Article 15 (5) of the AI Act from the actual operational risk profile and organizational capacities of the entities concerned, thereby undermining the principle of proportionality as a general principle of EU law.

Moreover, the failure to refer to the criteria set out in Article 4 DORA would give rise to an unjustified accumulation of regulatory obligations, whereby financial institutions would be required to comply with parallel and partially overlapping cybersecurity requirements stemming from both the AI Act and DORA, without any mechanism for their mutual coordination. This would increase the risk of inconsistent supervisory assessments, divergent regulatory expectations, and the fragmentation of supervisory practices at the national level.

Finally, the refusal to apply sector-specific proportionality would paradoxically weaken the regulatory objectives of both instruments. The excessive burden imposed on smaller or locally operating financial institutions could incentivize a formalistic, checklist-driven approach to AI cybersecurity, rather than a targeted allocation of resources to areas generating the highest risk. As a result, instead of strengthening the operational resilience of AI systems, such an approach could lead to its normative dilution.

Therefore, the relation between Article 4 DORA and Article 15 of the AI Act complies with the concept of security at large and cybersecurity, which measures risk and security according to objective criteria.[17] In contemporary risk-based regulatory frameworks, security cannot be understood as a fixed or absolute standard but rather as a context-dependent normative benchmark calibrated to the likelihood and potential impact of harm. Accordingly, the reference in Article 15 (5) of the AI Act to "relevant circumstances and risks" should be interpreted, in the context of financial-sector AI deployments, in light of the proportionality criteria articulated in Article 4 DORA. As explained, the latter provision translates the general principle of proportionality in EU law into operational parameters such as the size of the entity, its overall risk profile, and the nature, scale and complexity of its activities. Properly understood, the proportionality framework established in Article 4 DORA provides the sector-specific analytical lens through which the reference to "relevant circumstances and risks" in Article 15 (5) of the AI Act should be interpreted in the financial sector. Thereby ensuring that cybersecurity obligations applicable to

[17] M. Karpiuk, *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, "Studia Iuridica Lublinensia" 2019, vol. 28(1), pp. 185–194; K. Kaczmarek, M. Karpiuk, C. Melchior, *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź" 2024, no. 3, pp. 105–106.

high-risk AI systems remain both effective and context-sensitive while preserving coherence between horizontal AI regulation and the operational resilience framework governing ICT risk in financial services.

CONCLUSIONS

This article set out to examine whether the proportionality framework established in Article 4 DORA should inform the interpretation of cybersecurity obligations applicable to high-risk AI systems under Article 15 (5) of the AI Act when such systems operate within the ICT infrastructures of financial institutions. The central research question concerned the normative relationship between the horizontal regulatory regime governing artificial intelligence and the sector-specific framework of ICT risk management applicable to financial entities. The analysis conducted in this article supports the thesis that the reference to "relevant circumstances and risks" in Article 15 (5) of the AI Act should be interpreted, in the financial sector, through the proportionality criteria articulated in Article 4 DORA. Consequently, the adequacy of cybersecurity measures applied to high-risk AI systems deployed by financial institutions should be assessed in light of objective factors such as the size of the entity, its overall risk profile, and the nature, scale and complexity of its activities.

The study contributes new knowledge by clarifying the systemic relationship between two recently adopted EU regulatory instruments that operate at different levels of the legal framework for digital technologies. While the AI Act establishes horizontal obligations concerning the design, deployment and operation of high-risk AI systems, DORA provides a sector-specific architecture for managing ICT-related risks in the financial sector. The article demonstrates that the proportionality criteria set out in Article 4 of DORA can function as an interpretative benchmark for identifying the "relevant circumstances and risks" referred to in Article 15 (5) of the AI Act in situations where AI systems operate as components of ICT systems within financial institutions. This interpretative linkage allows the two regulatory regimes to operate coherently, ensuring that cybersecurity obligations applicable to AI systems remain both effective and appropriately calibrated to the operational risk environment in which they function.

The legal significance of this study lies in its contribution to the systematic interpretation of EU digital regulation. By demonstrating that the proportionality framework of DORA provides an appropriate analytical context for assessing cybersecurity obligations under Article 15 (5) of the AI Act in the financial sector, the article proposes a method for avoiding both regulatory duplication and the miscalibration of compliance requirements. Such an approach supports regulatory coherence between horizontal and sector-specific instruments while preserving

the autonomous application of the AI Act and maintaining the minimum security standards it establishes.

More broadly, the findings of this study illustrate how proportionality-based risk assessment can function as a key mechanism for integrating emerging regulatory regimes governing artificial intelligence, cybersecurity, and digital operational resilience. As the EU legal framework for digital technologies continues to expand, interpretative approaches that emphasize coherence between horizontal and sectoral instruments will become increasingly important for ensuring the effectiveness, consistency, and practical enforceability of EU law. In this sense, the analysis presented in this article contributes to the broader doctrinal discussion on the systemic architecture of EU digital regulation and the role of proportionality in managing the interaction between overlapping technological governance regimes.

REFERENCES

Literature

Bierecki D., *Zasada proporcjonalności w stosowaniu rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience Act – DORA)*, "Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2024, no. 3. **DOI: https://doi.org/10.52097/eppism.9272**

Bierecki D., Czuryk M., Gaie C., Langlois-Berthelot J., *Sovereignty by Design: Embedding Fiscal Risk Intelligence in Europe's Defence-Digital Strategy*, "Prawo i Więź" 2026, no. 1. **DOI: https://doi.org/10.36128/2z2k7566**

Bierecki D., Gaie C., Karpiuk M., Langlois-Berthelot J., *Creating Resilient Artificial Intelligence Systems: A Responsible Approach to Cybersecurity Risks*, "Prawo i Więź" 2025, no. 5. **DOI: https://doi.org/10.36128/0akf8v90**

Bierecki D., Karpiuk M., Melchior C., Strizzolo N., *Security in the Era of Threats Occurring in Cyberspace*, "Prawo i Więź" 2025, no. 4. **DOI: https://doi.org/10.36128/PRIW.VI57.1476**

De Hert P., Papakonstantinou V., *Does the Future Hold More Rights or More Proportionality? The GDPR-Message*, "European Data Protection Law Review" 2023, vol. 9(4). **DOI: https://doi.org/10.21552/edpl/2023/4/5**

Fuchs C., *Information Technology and Sustainability in the Information Society*, "International Journal of Communication" 2017, vol. 11.

Helios J., Jedlecka W., *Wykładnia prawa Unii Europejskiej ze stanowiska teorii prawa*, Wrocław 2018.

Herlin-Karnell E., *EU Data Protection and the Principle of Proportionality*, "Nordic Journal of European Law" 2021, vol. 4(2). **DOI: https://doi.org/10.36969/njel.v4i2.23782**

Kaczmarek K., Karpiuk M., Melchior C., *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź" 2024, no. 3. **DOI: https://doi.org/10.36128/PRIW.VI50.907**

Karpiuk M., *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, "Studia Iuridica Lublinensia" 2019, vol. 28(1). **DOI: https://doi.org/10.17951/sil.2019.28.1.185-194**

Maliszewska-Nienartowicz J., *Zasada proporcjonalności jako podstawa oceny legalności ograniczeń swobód rynku wewnętrznego Unii Europejskiej*, Toruń 2020.
Pelc P., *Zasada proporcjonalności w DORA*, "Cybersecurity and Law" 2024, no. 2.
Thai Thi T.D., Gia P.D., *Balancing the Right to Access Information, the Right to Privacy, the Right to Personal Data Protection, and the Right to Be Forgotten in the Digital Age: The Case of Vietnam*, "Prawo i Więź" 2024, no. 6. **DOI: https://doi.org/10.36128/PRIW.VI53.1221**
Tolino G., Punia G., Emmanuel J., *Report: EU Digital Operational Resilience Regulation (DORA)*, "Global Privacy Law Review" 2025, vol. 6(1). **DOI: https://doi.org/10.54648/gplr2025010**

Legal acts

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333/80, 27.12.2022).
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (OJ L 151/15, 7.6.2019).
Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (OJ L 333/1, 27.12.2022).
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L 2024/1689, 12.7.2024).
Treaty on European Union (OJ C 326, 26.10.2012).

ABSTRAKT

Artykuł ma charakter naukowo-badawczy i koncepcyjny. Dotyczy relacji pomiędzy obowiązkami cyberbezpieczeństwa dotyczącymi systemów sztucznej inteligencji wysokiego ryzyka a regulacjami zarządzania ryzykiem ICT w sektorze finansowym w prawie Unii Europejskiej. Problem badawczy dotyczy interpretacji pojęcia „odpowiednich okoliczności i ryzyka" zawartego w art. 15 ust. 5 aktu o sztucznej inteligencji w sytuacji, gdy systemy AI wysokiego ryzyka funkcjonują jako elementy infrastruktury ICT instytucji finansowych. W artykule przyjęto tezę, że okoliczności te powinny być interpretowane z uwzględnieniem kryteriów proporcjonalności określonych w art. 4 aktu w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA – Digital Operational Resilience Act). Celem jest wykazanie, że kryteria proporcjonalności ustanowione w DORA mogą stanowić punkt odniesienia przy ocenie adekwatności środków cyberbezpieczeństwa wymaganych na podstawie aktu o sztucznej inteligencji. Teza badawcza stanowi, że w sektorze finansowym kryteria dotyczące wielkości podmiotu, jego ogólnego profilu ryzyka oraz charakteru, skali i złożoności działalności stanowią „odpowiednie okoliczności i ryzyka" w rozumieniu art. 15 ust. 5 aktu o sztucznej inteligencji. Oryginalność pracy polega na wykazaniu systemowej komplementarności pomiędzy regulacją AI, która znajduje zastosowanie bez względu na status podmiotu korzystającego z systemu AI, a sektoro-

wymi ramami odporności operacyjnej ICT. Badanie ma zakres unijny i wnosi wkład do doktrynalnej interpretacji rozwijających się regulacji cyfrowych Unii Europejskiej, a jednocześnie ma znaczenie praktyczne dla organów nadzorczych i instytucji finansowych wdrażających obowiązki w zakresie cyberbezpieczeństwa dla systemów AI.

Słowa kluczowe: akt o sztucznej inteligencji; rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego; DORA; zasada proporcjonalności; cyberbezpieczeństwo systemów AI; zarządzanie ryzykiem ICT w sektorze finansowym