The International Journal of Engineering and Science (IJES)
|| Volume || 14 || Issue 6 || June || Pages || PP 161-167 || 2025 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Legalbasis of the EuropeanUnion'sdigitisation policy - analysis of selecteddevelopments

Izabela Oleksiewicz

---------- ***Summary***----------
The ever-increasing impact of ICT on the socio-economic development of the European Union Member States and the growth in their use mean that the products and services offered are now increasingly dependent on ensuring cybersecurity. The extensive architecture of ICT systems, including operations on large data resources, serve the development of communication, trade, transport and constitute the basis for the functioning of key, digital services and services provided by public administration. Unfortunately, the possibilities offered by modern digital technologies are also used to apply unfair competition practices, interrupt the continuity of selected services, commit crimes using the Internet, or conduct cyberterrorist activities. Based on the analysis of the issue, the following research theses will be verified. Firstly, the evolution of policy is a reaction to the increase in instability and threats in this area and the lack of appropriate mechanisms and regulations in this area. Determining the definitional discrepancies of the concept of "incident" will allow us to determine how it affects the digitalization policy. It will also show that the reason for the creation of this policy was the lack of regulations in this area and the existence of appropriate mechanisms in this area. Therefore, we are dealing with both the process of institutionalization and transformation. However, the NIS 2 Directive constitutes lex generaliin relation to other legal acts, because each legal act adopted subsequently is a particularisation of it, i.e. it constitutes lex speclis.
Keywords: *digitalization policy, European Union, cybersecurity,*

Date of Submission: 15-06-2025 Date of acceptance: 30-06-2025

I. Introduction to research

The aim of this study will be to analyse legal changes in the European Union, with particular emphasis on such legal acts as NIS 2, CRA, AI Act or the Cyber Solidarity Act. The main research problem is to demonstrate how important an element of current legal regulations is a skillfully conducted digitalisation policy at the EU level. This is of great importance for the internal security of the Member States themselves and the entire EU.

The impetus for taking such actions turned out to be the deep processes related to the integration changes in the European Union that we have been dealing with on a daily basis, especially in the last five years. Rapid civilizational, political and economic changes are a test for individual societies of their ability to find their way in a new reality and live in a virtual world. The future order and balance of power in the world will depend on how societies recognize and use emerging opportunities and how they cope with threats.

Thus, the analysis of legal changes from the systemic perspective that take place in the EU digitalization policy, especially in recent years, is the main objective of this article. The subject of the research analysis is the European Union, and its digitalization policy and legal changes that are taking place. At the outset, it should be assumed that legal changes in cyberspace at the EU level will evolve depending on the speed of progress and changes in the EU digitalization policy. It is therefore important to create coherent and transparent mechanisms of digitalization policy that define the determinants of mutual assistance in in the event of the occurrence of so-called incidents and the introduction of a European legal framework in this area.

It will be necessary to conduct a preliminary study consisting in defining the essence and scope of the concept of what an incident is in individual EU legal acts and whether its scope of meaning is coherent. An institutional and legal analysis of protection will show how differently and with what varying effectiveness and detail the same issue can be regulated at the EU level in various legal acts that are currently in force in individual countries, but the countries have until 2028 (in most cases) to fully implement them. An analysis of the essence of the content of individual EU legal acts will show that there is a digitalization policy that is based on the social and internal security of the state and is subject to constant evolution. Thus, we are dealing with a process that has not been completed and is still ongoing.

In order to analyze the research subject, i.e. actions related to the implementation of individual legal acts into the law of the Member States, it will be shown that the reason for the interest in digitalization policy is, firstly, the lack of appropriate mechanisms and regulations in this area, which is why we are dealing with both

the process of institutionalization and transformation. Secondly, it should be assumed that the existing digitalization policy is evolving and aims to eliminate legal loopholes and harmonize legal norms adopted in EU law, although this process progresses at different speeds in each Member State and should not be considered complete.

The source basis for the conducted analysis are legal documents of the European Union regulating the issues of cybersecurity policy and digitization. The conducted analyses used legal acts (primarily NIS2, CRA, AI Act) and materials found on the websites of: the Parliament, the Commission of the European Union and the Council of the EU (draft regulations and their justifications), ECJ rulings. Reports of institutions such as ENISA were also created on this subject. Access to source materials was possible thanks to the unlimited possibilities of the Internet, mainly thanks to access to the service database. Numerous statistical, post-conference, press and scientific articles related to this issue published on the Internet were very important. Obtaining so many materials was possible thanks to the many years of collecting literature, numerous scientific items, primarily foreign literature.

The publication is interdisciplinary in nature, covering issues from the field of law, security sciences, and political science, which became the basis for a broad and thorough analysis of source materials and texts. The starting point for the research were source queries and literature studies aimed at jointly defining competence profiles that are key from the point of view of cybersecurity challenges. Then, the most important legal and political-strategic program documents were analyzed and assessed in terms of the vision of digitalization protection contained therein. The dogmatic and heuristic methods were also used to thoroughly analyze the applicable EU legal regulations in the field of EU cyberspace protection policy and digitalization. Then, the decision-making method was used to see what impact individual legal instruments adopted by the EU and currently being implemented could have. In turn, the document analysis technique allowed for examining the content of legal acts regulating the issue of digitalization in the Union. The case law analysis method allowed for a comparison and determination of the shape of court practice. A prognostic technique was also used to present a vision of the development of the EU's digitalization policy and the protection of cyberspace. The final method chosen was the synthesis of the entire phenomenon based on the observations conducted so far.

NIS2 and CRA

The next Directive of the European Parliament and of the Council (EU) 2022/2555NIS 2 (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022) was adopted in response to the identified deficiencies in the NIS I Directive. The NIS 2 Directive introduces a division into key entities and important entities of a larger number of entities, and also introduces *ex ante and ex post supervision regarding new supervision mechanisms,* including regular security audits, on-site inspections and security scans. NIS2 promotes cooperation and exchange of information at national and EU level through the Cooperation Group, the CSIRT Network, CYCLONe and the European Database (Chałubińska-Jentkiewicz, Nowikowska, 2024). In addition, based on the decision of the Member State, other entities from these sectors or entities that have been recognized as key entities based on the NIS Directive may be included in the key entities. However, it should be noted that Article Article 4 of the NIS 2 Directive states that where there are sectoral provisions which impose requirements that are at least equivalent to the obligations laid down therein, the sectoral provisions shall prevail and the NIS 2 Directive shall not apply.

The CRA Regulation (Kolupaieva, Sheiko, Polozova, 2024, p. 89) is to be *a lex specialis*to NIS 2, and its scope of entities includes a wide catalog of entities with digital elements that will be introduced to the internal market. Its systemic goal is to lead to the increase and Strengthening the level of resilience (cybersecurity) of the European Union to cyber threats by imposing regulatory obligations on manufacturers, distributors and importers of products with digital elements placed on the internal market to eliminate the vulnerability of such products. Article 1(1) of the CRA Act sets out measures to increase the EU's capabilities in the area of detecting cybersecurity threats and incidents in cybersecurity and preparing for and responding to such threats and incidents. According to Article 3, point 1 of the CRAa product with digital elements should be considered to be a software or hardware product and the related remote data processing solutions, including separately placed on the market software or hardware components. The definition of a product with digital elements will generally not cover cloud services, such as those provided on a software as a service (*SaaS*) model, unless the provision of that service takes place in connection with the use of the product with digital elements for which such software was designed and developed, the absence of which would result in the digital product not being able to perform one of its functions (Recital 12 of the CRA Preamble).The CRA provides for certain exclusions from the provisions of the Regulation, which will apply to specific categories of products, including medical devices (pursuant to Article 2 paragraph 2 point a of the CRA, the Regulation shall not apply to products with digital elements to which Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 applies). On medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ

L 117, 5.5.2017, p. 1, as amended), including *in vitro diagnostics* (in accordance with Article 2 paragraph 2 point b of the CRA, the Regulation shall not apply to products with digital elements to which Regulation (EU) 2017/746 of the European Parliament and of the Council of 5.4.2017 applies), motor vehicles (in accordance with Article 2 paragraph 2 point c of the CRA, the Regulation shall not apply to products with digital elements to which Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27.11.2019 applies). On type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1, as amended), certified aeronautical products (in accordance with Article 2(3) of the CRA, the provisions of the Regulation shall not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4.7.2018). On common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency and amending Regulation (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 of the European Parliament and of the Council and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1, as amended) and marine equipment (in accordance with Article 2 paragraph 4 of the CRA, the Regulation does not apply to equipment covered by Directive 2014/68/EC of the European Parliament and of the Council 2014/90/EU of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146, as amended), for which the European Union has established separate cybersecurity requirements in the relevant sectoral legislation. The CRA provisions will also not apply to products with digital elements developed exclusively for national security or defence purposes or to products specifically designed to handle classified information (Article 2, paragraph 7 of the CRA). The CRA will also not apply to spare parts if they are identical to the components of the original product with digital elements and manufactured in accordance with the specifications of those components they are intended to replace (Article 2, paragraph 6 of the CRA).

It is worth noting that CRA is the next stage of harmonization of EU law after NIS 2, where it is manufacturers who are obliged to ensure compliance of products with EU cybersecurity standards at every stage of the product life cycle, which means that new procedures and standards will have to be implemented. There will be a need for long-term support and updates for at least 5 years after the product is introduced to the market.

At present, the adopted secondary legal acts have an identical understanding of the two concepts of "incident" and "large-scale cybersecurity incident". In addition, the existing legal acts use the term "serious incident", which is defined in two different ways depending on the legislative scope and regulatory subject. What is common to these definitions is the way they are presented (cause-and-effect) and the emphasis that the essence is the malfunction of the system. The evolution of the concept of "incident" in selected EU acts is presented in Table 2.

Table 1. Evolution of the concept of "incident" in selected EU acts

NIS2	CRA	Cyber Solidarity Act	AI
Incident means an event that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services offered by or accessible via networks and information systems;	**an incident** as defined in NIS II;	incident as defined in NIS II	
	"A digital product security incident" means an incident that negatively affects or may negatively affect the ability of a digital product to protect the availability, authenticity, integrity or confidentiality of data or functions.	**A serious incident** means an incident that causes a disruption that exceeds the response capacity of the Union entity and CERT-EU or that has a significant impact on at least two Union entities;	**A serious incident** means a malfunction of the AI system that leads directly or indirectly to any of the following events, e.g.: a) death of a person or serious damage to health, b) serious and irreversible disruptions in the management of critical infrastructure
" large-scale cybersecurity incident " means an incident that causes a level of disruption that exceeds the		**"large-scale cybersecurity incident" means a large-scale cybersecurity incident** as	

capacity of a Member State to respond to the incident or that has a significant impact in at least two Member States;		defined in the NIS II;	
		"serious cybersecurity incident" and) has caused or may cause significant operational disruptions to services or financial losses to the entity; b) has influenced or is capable of influencing other natural or legal persons, causing significant property or non-property damage.	

Source: own study

A completely separate matter is the creation of a definition of a serious cybersecurity incident by the Cyber Solidarity Act, as well asan incident affecting the security of a product with digital elements. These are two different definitions, although they are related due to the very root, which is the word "incident". The first one concerns virtual space and the possibility of incurring damage and losses as a result of the actions of another entity or natural person. The second one concerns a situation when the credibility of a product with digital elements decreases as a result of an incident. Technological development generates a need in the EU and the Member States to adapt the definitions and legal terms corresponding to various cyber threats, which are consistent with the concept of "incident" with the terminology adopted by NIS. However, if we look at it in more detail, each legal act creates, in accordance with the principle of *lex specialis,* detailed legal norms in relation to NIS 2, and thus constructs its own definitional solutions.

CRA and the AI ACT Regulation

Machine learning can help detect and identify threats in IT networks, but its use in the field of cybersecurity carries certain risks, as there is a risk of an attack on the system from using knowledge about the operation of a trained algorithm (Bar, 2021, 10-13). This is another example of a systemic solution in the EU that establishes harmonized rules on artificial intelligence, and at the same time constitutes the world's first comprehensive legal system on this issue. The aim of this legal act is to support innovation, improve the functioning of the internal market (similarly to the CRA) while ensuring a high level of protection of health, safety and fundamental rights. As you can see, the provisions of the AI Act concern safety and establish rules to ensure the safety of products and mitigating the risks associated with the use of AI. The AI Regulation therefore defines a framework for understanding the risks associated with AI. It classifies AI systems based on their potential risks and divides them into different categories depending on the data they collect and the decisions or actions taken based on that data. The EU obligations will vary depending on depending on the category of AI used. The creators of the act aim to understand what factors influence the AI system's decision-making, which will allow for a more effective response to potential threats.

Article 2 of Regulation (EU) 2024/1689 of the European Parliament and of the Council (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024) defines artificial intelligence as a machine system that, in order to achieve explicit or implicit goals, infers from the input data received how to generate results, such as predictions, content, recommendations or decisions that may affect the physical or virtual environment. It is worth emphasizing here that, in the legislator's assumption, different artificial intelligence systems differ in their level of autonomy and adaptability after implementation. In accordance with Art. 2 sec. 3 CRA, the provisions of the Regulation shall not apply to products with digital elements certified in accordance with Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency and amending Regulation (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 11.12.2018, p. 22.8.2018, p. 1, as amended)

As is clear from the CRA and the AI Act, products with digital elements classified as high-risk AI systems that meet the essential requirements imposed by the CRA will be deemed to meet the cybersecurity requirements set out in Article 15 of the AI Act, without prejudice to the other requirements set out in that Article and to the extent that the achievement of the level of protection set out in those requirements is demonstrated in the EU declaration of conformity issued under the CRA (Article 12(1) of the CRA). The relevant conformity assessment procedure provided for in Article 43 of the AI Act shall apply to those products. By way of derogation, important products with digital elements that are subject to conformity assessment

procedures and critical products with digital elements that are required to obtain a European cybersecurity certificate or that, in the absence thereof, are subject to conformity assessment procedures and that are also classified as high-risk AI systems pursuant to Article 6 of the AI Act shall be subject to the conformity assessment procedures provided for in the CRA (Article 12(3) of the CRA). The market surveillance authorities within the meaning of the CRA for products with digital elements also classified as high-risk AI systems will be the authorities designated for the purposes of the AI Act (Article 52(14) of the CRA).

According to the CRA,Each Member State will have to designate at least one market surveillance authority to ensure the effective implementation of the Regulation (Article 52(2) of the CRA). These authorities will be responsible for verifying whether products with digital elements meet the requirements specified in the regulation. They will also have the right to order corrective actions or to withdraw products from the market, depending on the level of risk (Wysokińska, 2021, p. 81). Additionally, the supervisory authority may require manufacturers to eliminate non-compliance related to affixing the CE marking, drawing up or not an EU declaration of conformity, completeness and availability of technical documentation and affixing the identification number of the notified body involved in the conformity procedure, if required (Banasiński, Rojszczak, 2020, pp. 323-325; Nowak , 2020, pp. 103-113).

Cyber Solidarity Act

The EU Cyber Solidarity Act (Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024), which entered into force on 4 February 2025, is gaining importance in in the context of deepening cyber conflicts, taking the form of digital warfare, the so-called cyberwar. The aim of this regulation is to increase the EU's capacity to detect cyber threats and incidents and to prepare and respond to such threats, including the European Cyber Warning System. At the same time, cybersolidarity (Radzińska,2014, pp. 58-68) is intended to mitigate the effects of other cyber threats resulting from geopolitical tensions (Article 3 of Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021). However, two fundamental issues play a key role, i.e. the creation of a European Cybersecurity Shield and a Cyber Crisis Mechanism. The European Cybersecurity Shield is an interconnected pan-European infrastructure of security monitoring centres, which includes national security monitoring centres and cross-border security monitoring centres. The main objective of implementing the European Cybersecurity Shield is to process data on cyber threats and cyber incidents. The Cyber Solidarity Act establishes a system for assessing and reviewing cyber incidents, which is procedurally similar to NIS 2. It can be seen that the creators intended to achieve the next level of cybersecurity of products (this time with digital elements). The idea is to facilitate the functioning and consistency with the NIS 2 Directive and strengthen the security of the entire supply chain.

It is worth paying attention to the systemic solution itself, which is to strengthen the EU's resilience to serious cybersecurity threats and to prepare for the short-term effects of serious and large-scale cybersecurity incidents in order to mitigate them in accordance with Article 222 of the TL (Oleksiewicz, 2021, p. 173). In addition, the mechanism is a cross-border protection of management against cyber threats and is to constitute "increasing common cybersecurity and cyberdefense against malicious checkmate and acts of aggression in cyberspace" (Miszczak, 2024, pp. 152-153). Article 13 of the Cyber Solidarity Act introduces the conditions for applying for support in responding to incidents and in immediately removing the effects of incidents. It was determined that the application procedure would be appropriate in this respect, and In In the event of multiple requests at the same time, the hierarchy of requests will be taken into account, in accordance with the criteria set out in Article 14(2) of the Cyber Solidarity Act. With this in mind, it should be acknowledged that cyber solidarity is the cornerstone of the common EU cybersecurity framework and incident response services are to be provided by trusted providers participating in the EU Cybersecurity Reserve (private sector providers).

II.Conclusions

Cyber incidents are difficult to predict because they are cross-border and fluctuating, Therefore, close cooperation between the public and private sectors is necessary. Such incidents can also negatively impact business activities, leading to significant financial losses, undermining user confidence or causing serious damage to the economy.

The CRA Regulation aims to make it easier for digital infrastructure providers to meet the supply chain requirements of NIS2 by ensuring that products with digital elements used by these providers to provide services are developed in a secure manner and that providers receive timely security updates for these products. The Cybersecurity Act aims to increase the security of ICT products, services and processes by introducing a voluntary European cybersecurity certification framework. Its impact on industry entities will be indirect, when a framework is issued relating to the subject matter of the company's activities (Dygnatowski, 2020, pp. 309-320). However, this act does not contain provisions directly imposing obligations on private entities.

Currently, cyber solidarity is considered to be a key determinant of cybersecurity, which is to become an effective cyberdefense tool and strengthen common EU capabilities in the field of cybersecurity. Cyber

solidarity should be considered through the prism of actual actions, such as cooperation in the matter of detecting and monitoring cybersecurity threats, developing common mechanisms for responding to cyber threats or providing mutual financial assistance. Within cyber solidarity, new changes cover both the normative level, resulting from applicable legal regulations, and the actual level – materializing in the event of an actual threat. Member States will therefore be obliged not only to declared solidarity, but above all to practical solidarity (Radzińska, 2014, pp. 63-64). It is impossible not to agree with B. Krzan, who indicates that solidarity can be a clear signal emphasizing a common, coherent approach within the European Union (Krzan, 2022, p. 645). Considering the current cyber threats, such as, among others , disinformation or cyberwar, "global cyberspace may become fragmented", and this may have negative consequences for European security in the form of limiting the intelligence capabilities of EU Member States. Cybersolidarity is therefore a *sine qua non condition* for the security of the entire European Union.

Bibliography

[1]. Andersson, J. et al. (2017). *Envisioning European Defense: Five Futures* , No. 137. Chaillot Paper.
[2]. Banasiński, C., Rojszczak, M. (eds.), (2020). *Cybersecurity* , 323-325. Wolters Kluwer Polska Publishing House .
[3]. Bar, G. (2021). *Prohibited Use of Artificial Intelligence* , 10-13, ABI Expert.
[4]. Brzostek, A. (2023). *Cybersecurity in public administration – legal aspects* , 23, 98-100, ZeszytyPrawnicze.
[5]. Chałubińska-Jentkiewicz, K., Nowikowska, M. (2024). *Entities involved in the policy of ensuring the security of networks and information systems in the light of the NIS 2 directive (part 2)* , 5-24, Cybersecurity and Law.
[6]. Dygnatowski, S. (2020). *Cybersecurity as the foundation of critical infrastructure security in the context of contemporary threats* , 50(4), 309-320, Journal of KONBiN.
[7]. Kolupaieva, I., Sheiko, I., Polozova, T. (2024). *Digital Transformation in the Context of Sustainable Development of European Countries* , 19(1), 89–102, Problems of Sustainable Development.
[8]. Krzan, B. (2022). The principle of solidarity in European Union law. In: A. Kozłowski (ed.), *The rule of law as a universal value. The jubilee book of Professor Krzysztof Wójtowicz*, 633-645, E-Publishing House. Legal and Economic Digital Library. Faculty of Law, Administration and Economics of the University of Wrocław.
[9]. Janowski, J. (2012). Cybernetization of law. In: E. Galewska, S. Kotecka (eds.), *X-rocznia CBKE. Commemorative book on the occasion of the 10th anniversary of the Center for Research on Legal and Economic Problems of Electronic Communication and the Student Scientific Club* , 143-156,Publisher: LAW OFFICE .
[10]. Małecka, A. (2021). *European Union cybersecurity policy at the beginning of the third decade of the 21st century* , 73-89, International Security Yearbook.
[11]. Malešević, S. (2017). *Terrorism. In The Rise of Organized Brutality: A Historical Sociology of Violence* , Cambridge.
[12]. Miszczak, K., (2024). *Strategic Compass of the European Union. Greater security and more effective defence of the EU - a roadmap to 2030* , 1 (88/1), 152-153, Politeja.
[13]. Nowak , W. (2020). Specificity of threats in cyberspace. In:C. Banasiński, M. Rojszczak(eds.), *Cybersecurity* , 103 -113, Publisher: Wolters Kluwer Polska .
[14]. Oleksiewicz I., Pomykała M. (2024). Cybersecurity as a new dimension of contemporary state security.In: Oleksiewicz I., Pomykała M. (eds .), *Threats and challenges of security in cyberspace* , Publishing House of the Rzeszów University of Technology .
[15]. Oleksiewicz, I. (2021). *Cyberspace Protection. Policy-Strategy-Law* . PWN Scientific Publishing House .
[16]. Radzińska, J. (2014). *Solidarity: definition and contexts* , 48, 58-68, Etyka.
[17]. Skoczylas, D. (2023). *Cyber threats in cyberspace. Cybercrime, cyberterrorism and network incidents,* 53, 97-113, Law in Action. Criminal Cases.
[18]. Skoczylas, D. (2023). *National Cybersecurity System* , CHBeck Publishing House Sp. z o. o .
[19]. Skoczylas, D. (2024). *Strengthening the European Union's cybersecurity capabilities – cybersolidarity in the context of cyber threats,* 12, 39-44, European Judicial Review.
[20]. Szpor, G. (2021). *The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland* , 46 (3), 219-235, Review of European and Comparative Law.
[21]. Woszek, S. (2022). *Cybersecurity of states in the 21st century on the example of the Republic of Poland* , 14 (27), 198-217, Internal Security Review.
[22]. Wysokińska, Z. (2021). *A Review of the Impact of the Digital Transformation on the Global and European Economy* , 24(3), 75-91, Comparative Economic Research. Central and Eastern Europe.
[23]. Żywucka-Kozłowska, E., Dziembowski, R. (2023). *Around the definition of cybersecurity* , 2 (10), 123-132, Cybersecurity and Law.

Legal acts

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 2016, p. 1).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning 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 EU L 333, p. 80) – hereinafter referred to as the NIS 2 Directive.

Judgment of the District Court of Paris of 20 October 2000 in the case Anit-Semitism LICRA v. Yahoo Inc., file reference RG 00/05308.

European Parliament resolution of 10 June 2021 on the EU cybersecurity strategy for the Digital Decade (2021/2568(RSP)) [OJ EU C 67. 81, 8.02.2022].

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1, as amended).
Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe programme and repealing Decision (EU) 2015/2240 (OJ EU L 166, p. 1).
European Parliament resolution of 10 June 2021 on the EU cybersecurity strategy for the Digital Decade (2021/2568(RSP)) [OJ EU C 67. 81, 8.02.2022].
Regulation 2019/881 on "cyber threat" means any potential circumstance, event or action that may cause damage, disrupt or otherwise adversely affect networks and information systems, users of such systems or other persons.
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 communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ EU L 151, p. 15) – hereinafter referred to as the Cybersecurity Act.
The Regulation does not apply to equipment covered by Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146, as amended).
Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 establishing measures to strengthen solidarity and the Union's capacity to detect, prepare for and respond to cybersecurity threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) [OJ L 2025.38, 15.01.2025].
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 12, 12.7.2024, p. 1689; hereinafter referred to as AI Act.
Judgment of the ECJ in case C-176/03 Commission v Council.
Act of 5 July 2018 on the national cybersecurity system (Journal of Laws of 2023, item 913, as amended).