Marek Porzeżyński*
Łukasz Kulicki**

Changes Introduced by the NIS Directive 2.0 and their Potential Effect on Shaping the Cybersecurity Labour Market[1]

Abstract

Ensuring cybersecurity is – next to AI development – one of humanity's greatest challenges nowadays. This is not a hyperbole – cybersecurity threats are real for public and private sectors, as well as individuals. With the rapid technological advancements and galloping digitisation, malicious entities and individuals are looking to take advantage of the online security gaps created by lack of caution. The European Union tried to counteract this by extensively discussing the issue, giving rise to the NIS directive. After a few years in force, its effects were assessed, and several changes were prepared to improve overall cybersecurity. However, these solutions will not work unless it becomes standard practice to employ cybersecurity specialists in a wide range of environments, extending far beyond those of the biggest organisations. This is what happened in the case of the General Data Protection Regulation (GDPR). The original provisions had been expanded to such an extent that they led to the emergence (separation) of an independent consultancy market in the field of information protection, with particular emphasis on personal data from the

* Assoc. Prof. Marek Porzeżyński, PhD, Warsaw University of Technology, expert in the field of new technology law with a special focus on intellectual property, privacy and cybersecurity, e-mail: marek.porzezynski@pw.edu.pl, ORCID: 0000-0002-4709-2788.
** Łukasz Kulicki, Analyst at Center for Security Studies, War Studies University in Warsaw, attorney-at-law, expert in the field of new technology law and legal aspects of digital transformation, e-mail: l.kulicki@pracownik.akademia.mil.pl, ORCID: 0009-0006-1940-5392.
1 This article in part prepared by Marek Porzeżyński was funded from a grant for the research visit at the European University Institute (Florance, Italy).

technical and legal consultancy markets. Hence, comparisons to the GDPR are valid. In this article, the authors review and assess the changes in cybersecurity legislation. This includes the NIS 2.0 directive category of digital service providers and their expected effects on the labour market.

Key words: cybersecurity, NIS 2, labour market

Introduction

Ensuring the cybersecurity of trading entities is an increasingly pressing issue. Despite its recognition years ago and attempts to address it through the introduction of dedicated regulations, in particular the NIS Directive[2], the dynamic growth of cyberthreats does not seem to have slowed down. At the same time, there is a steadily growing demand for cybersecurity specialists. As a result, it is possible that the cybersecurity sphere will split from the broader IT labour market. However, a mature labour market is yet to emerge. For the time being, most experts are employed at a small number of organisations, including specialist cybersecurity service providers, large corporations and dedicated state agencies. Every day seems to provide evidence of the growing role of cybersecurity. Its simportance became even more obvious during the COVID-19 pandemic, which further accelerated the digitalisation, and in the early stages of the war in Ukraine when the number of attacks targeting various sectors of the economy far exceeded previously observable levels and, their management left much to be desired. Admittedly, although being a step in the right direction, the aforementioned regulation alone did not provide sufficient impetus for the development of the cybersecurity labour market.

One study found that during the COVID-19 pandemic, almost two-thirds of the surveyed organisations recorded at least one cyberincident[3]. At the same time, the number of cyberincidents began to grow at a high rate at medium-sized entities, whereas previously, cyberattacks mainly targeted large organisations. In the case of the initial period of the war in Ukraine, increased hostile online activity was recorded both for entities from within

2 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 (Official Journal of the European Union 2016, L 194/1).

3 *Report: Barometr cyberbezpieczeństwa. COVID-19 przyspiesza cyfryzację firm – marzec 2021*, https://kpmg.com/pl/pl/home/insights/2021/04/raport-barometr-cyberbezpieczenstwa-2020-covid-19-przyspiesza-cyfryzacje-firm.html [access: 15.06.2023].

Ukraine, where cyberattacks on the government and military sectors almost tripled, as well as for entities on Polish territory, where more malicious traffic was shown, predominantly originating from Russian territory[4]. Taken together, the two crises have significantly increased cyberthreats, while also drawing broader public attention to the fact that cybersecurity is a growing and increasingly real problem. Another study highlighted that the proportion of Polish businesses targeted by a cyberattack[5] increased from 13% in 2020 to 77% in 2021[6]. However, to gain a full picture, these statistics should be additionally „filtered", since they reflect only the detected and reported cyberattacks. Potentially unidentified cyberthreat activities, including those recognised but not reported based on a business decision, were hence left out of the figures[7].

These trends have clearly driven the emergence of a self-contained cybersecurity market. A report prepared in cooperation with the Polish Agency for Enterprise Development indicated that some of the most desirable competencies sought after on the market[8] are those in the field of cybersecurity (55% of respondents). This specialisation came second after software development, which has topped the lists of sought-after specialists for years. Interestingly, it is also the only sector that does not appear under „factors influencing company growth" in the same survey[9]. It should be noted that this is not the only situation in which new technologies foster the socio-economic sphere[10].

It is worth noting in this context that, in addition to the pandemic situation, there have been important legislative developments for the sector in the

4 K. Pasławski, *Cyberwojna wokół Ukrainy. Nowe dane*, 2022, https://crn.pl/aktualnosci/wojna-na-ukrainie-cyberwojna-wokol-ukrainy-nowe-dane/ [access: 15.12.2023].

5 More specifically, a ransomware attack.

6 P. Mahendru, *The State of Ransomware in Retail 2022*, https://news.sophos.com/en-us/2022/09/07/the-state-of-ransomware-in-retail-2022/ [access: 15.12.2023].

7 The problem of ransomware attacks, in which a ransom is paid in order for the breaching party not to inform the public of the incident, is often highlighted.

8 *Wpływ skutków pandemii koronawirusa na potrzeby kompetencyjne sektorów informatyki oraz telekomunikacji i cyberbezpieczeństwa w konsekwencji rozwoju zastosowań technologii cyfrowych oraz kształtowania się nowego modelu pracy – kwiecień 2023*, p. 20 etff., https://antal.pl/wiedza/raport/wplyw-skutkow-pandemii-koronawirusa-na-potrzeby-kompetencyjne-sektorow-informatyki-oraz-telekomunikacji-i-cyberbezpieczenstwa [access: 15.06.2023].

9 Ibidem.

10 A. Zalcewicz, *New Technologies in the Control of Public Finances and Building Public Confidence in the State*, „Bialystok Legal Studies" 2023, vol. 28, no. 2, p. 25.

meantime. The NIS Directive was one of the first formalised[11] responses by public authorities to provide adequate protection to ensure the security of networks and information systems. While proposal[12] for the so-called NIS Directive 2.0 enumerates several positive aspects of the NIS Directive, it concludes by stating that several shortcomings that „prevented the NIS Directive from reaching its full potential" have also been addressed. In the authors' opinion, one of the elements that failed to achieve its objectives is the failure to create a labour market for cybersecurity professionals in a mature form. Indeed, services of this kind are still reserved for a narrow group of specialised entities.

One of the most important changes proposed in the drafts and introduced in the enacted version of the NIS Directive 2.0[13] is the catalogue of entities to which the obligations apply. At the same time, by obliging a wider range of entities to achieve an adequate level of cybersecurity, this amendment will further accelerate the emergence of the cybersecurity market and intensify the need for cybersecurity professionals in a larger number of entities from different sectors. While other changes are not as profound, in this case, the NIS Directive's distinction between operators of essential services and digital service providers has been completely abandoned[14]. This is meant to increase the level of security by sealing the entire system, which was one of the reasons why the NIS Directive did not fully meet the hopes placed in it[15].

In this article, the authors present and analyse the subjective scopes of both pieces of legislation and identify their possible impact on creating a mature and self-contained cybersecurity market by analogy to the data protection situation, which appears to be comparable. This analysis and comparison allow a preliminary assessment of the effects of the introduced changes. These, in

11 In the sense of being structured and enshrined in the form of a legal act.

12 Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, Brussels, 16 December 2020, COM (2020) 823 final.

13 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) (Official Journal of the European Union 2022, L 333/80).

14 In addition to the other categories for which specific obligations were also addressed under the NIS Directive.

15 M. Porzeżyński, *Cyberbezpieczeństwo dostawców usług cyfrowych*, Warszawa 2021.

turn, provide a basis for preliminary conclusions and suggested solutions for more effective or more complete achievement of the intended impacts of the NIS 2 Directive.

Subjective scope of the NIS Directive

The NIS Directive provided an implicit framework[16] for Member States to designate the entities responsible for meeting the obligations imposed by the Directive. In principle, however, it was envisaged that security requirements should be established for operators of essential services and digital service providers, as well as for entities that can be broadly described as public[17]. The establishment of computer security incident response teams (CSIRTs) was also envisaged. This has also been taken into account in the Act on the National Cybersecurity System (ANCS 2022), which constitutes a comprehensive implementation of the NIS Directive into Poland's internal legal system, taking into account the need to clarify specific provisions and specify the entities on which obligations are to be imposed. To this end, Article 4 of the ANCS provides a complete list of entities falling within the scope of the national cybersecurity system.

The basic distinction of market entities was drawn between operators of essential services and digital service providers. Pursuant to Art. 5 of the ANCS, an operator of essential services was an entity indicated in the relevant annex to the Act which relied on information systems to provide an essential service and which could be significantly disrupted in providing this service by a possible incident. The indicated criteria, the assessment of which is necessary for qualification to the category of operators of essential services, are vague. As it seems, the procedure for making such an assessment had many shortcomings, and identifying the entities responsible for meeting the obligations set out in the NIS Directive (and the ANCS) already proved problematic.

The second of the categories identified in the NIS Directive, as well as in the ANCS, were digital service providers. This group was singled out because of its decidedly more private nature (in principle, in contrast to the other obligation

16 In accordance with the principle of minimum harmonisation as indicated in Art. 3 of the NIS Directive.

17 It should be noted that this is a generalisation used by the author in order not to list in detail and discuss the nature of categories that are not the purpose of the analysis.

groups). In addition, as per the explanatory memorandum of the draft Act, they were digital infrastructure providers, qualifying them as services essential to the maintenance of critical socio-economic operations (explanatory memorandum of the draft ANCS 2022, 2). Provisions for this group of entities, therefore, seemed justified as a means of achieving the overarching objective of the NIS Directive – that is, attaining the minimum level of cybersecurity.

At first sight, the briefly described subjective scope of the NIS Directive did not seem to create a broader space[18] for the use of specialised cybersecurity services. This is because except for the last of the indicated categories, which is discussed in the next chapter, the other subjective groups were already subject to specific regulations obliging them to ensure an adequate level of cybersecurity[19].

Status of digital service providers in the NIS Directive

It was digital service providers, therefore, who could count themselves among the entities that, before the NIS Directive, were not subject to the specific cybersecurity requirements they had to meet. However, these entities first had to deal with the problem of assessing their eligibility, which was not helped by a rather complicated definition. Indeed, the act implementing the NIS Directive referred to a definition from another piece of legislation[20]. The definition of a digital service provider thus consists of two elements which have to occur together, i.e. provision of services by electronic means and provision of a specific service within the appropriate annex to the ANCS. It should be noted that the assessment was left to the digital service providers, in contrast to the operators of essential services, for whom appropriate assessment procedures were foreseen. This was because of a lighter approach[21] to this entity category manifested in the absence of a principled top-down imposition of eligibility for this category in favour of an obligation for entities with full knowledge of their activities to make their assessment.

18 Or, more precisely, a need.
19 Or information security.
20 Act of 18 July 2002 on the Provision of Services by Electronic Means (Journal of Laws 2020, item 344).
21 Such arguments were given by ENISA at the Workshop on Network and Information Security, Bratislava, 17–18 October 2016.

According to the subjective scope, the NIS Directive (and, with it, the ANCS) imposes obligations on legal persons or entities providing digital services that fall under the heading of online trading platform services, cloud computing or search engine services. The Directive leaves these entity categories without further clarification. However, the legislator implementing the requirements of this piece of legislation into the internal legal system decided on the need for guidelines to fully recognise the scope of the various categories.

The indicated annex defines an online trading platform as a service that enables consumers or traders to contract with traders electronically. This is either on the website of the trading platform or on the website of the trader using the services provided by the online trading platform. In addition to this definition, it should be emphasised that, according to the preamble of the NIS Directive, an online trading platform should not be limited to intermediary services to third parties. This means that the category includes entities offering only their services and goods, as well as those offering services and goods of other entities as well[22]. A cloud computing service, on the other hand, is defined as „enabling access to a scalable and elastic pool of shareable computing resources for shared use by multiple users"[23]. However, not much additional guidance was provided on these elements, excluding the basis for understanding the scope of scalability[24], which the legislator addressed. Thus, a broad evaluation possibility is left for cloud computing services, which can also be considered a future-proof approach. A search engine, in turn, is a service that allows users to search for all websites or webpages in a given language through a query by entering a keyword, phrase or other element, presenting links referring to information related to the query as a result. For the search purpose, providers of so-called „price comparison services" were excluded from the scope[25]. To further reduce the risk, Recital 16 stipulates that the definition in question „should not include search functions that are

22 Recital 15 of the NIS Directive.

23 In particular, access to these resources can be provided in models: SaaS (Software as a Service – provision of specific resources in the form of a service provided remotely), IaaS (Infrastructure as a Service – provision of resources such as e.g. computing power in the form of a service provided remotely), PaaS (Platform as a service – services characterised by the provision of an environment (platform) in which one can create one's own work).

24 Recitals 16 and 17 of the preamble to the NIS Directive.

25 Entities that „compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product".

limited to the contents of a specific website, irrespective of whether the search function is provided by an external search engine"[26].

For the sake of argument, it should be noted that according to legal commentators, by contrast, other types of services not listed in the aforementioned annex cannot be considered digital services within the meaning of the Act[27]. This caused a fundamental problem in recognising whether a given entity is a digital service provider within the meaning of the ANCS and, at the same time, does not fall under the exemption indicated in this Act. The lack of a clear qualification or the possibility to verify an independent qualification has caused many entities to prefer not to resolve this issue in order not to commit themselves to meet the requirements, which entailed additional costs, e.g. related to the need to use cybersecurity services or employ a suitably qualified specialist. At the same time, it should be noted that a similar situation may have been observed within the area of personal data protection in the years 1997–2018 when the APPD[28] was in force, plus its regulation did not result in a broader knowledge of this area of law and mostly did not evoke a sense of obligation to adequately manage personal data.

Changes to the scope of the NIS 2 Directive

The monitoring of the NIS Directive's functioning[29] led to the decision to make several changes to improve its effectiveness. One of them involved a complete overhaul of the entity categories provided for in this legal instrument. This is reflected, e.g., in the change of nomenclature, which directly translates into the composition of each category and manifests itself in their characteristics. The previously adopted nomenclature, i.e. operators of essential services and digital service providers, has been abandoned. In their place, essential entities[30] have appeared, listed in an annex[31] dedicated to each of these categories, including the nature of the sector, subsector and description of the

26 Recital 16 of the NIS Directive.
27 *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 153.
28 Act of 29 August 1997 on the Protection of Personal Data (Journal of Laws 1997, no. 133, item 883).
29 As well as the acts implementing the NIS Directive.
30 The draft NIS Directive 2.0 uses the terms essential and important entities.
31 Appendix I and Appendix II to the draft, respectively.

entity. Changes to the nomenclature are irrelevant to achieving the objectives of the legislation, although they do affect its usefulness. From this point of view, the proposed category names appear to better reflect their meaning.

As part of Recital 6 of the legislation in question, the changes are indicated, in particular, to broaden the scope of sectors – and, by extension, of those subject to the obligations – in order to ensure comprehensive coverage of those likely to be of key importance. At the same time, the previous distinction was indicated to have become obsolete in light of developments in the internal market, which does not seem to reveal the real reason for the change. It appears that not enough time has passed (given the pace of technological change) to justify such a far-reaching modification. However, Recital 15 of this legislation indicates the need to distinguish between the importance of an entity for its sector and the sensitivity of the services it provides, thus departing from the basis of categorisation from the NIS Directive it replaces.

It should, therefore, be noted that the blanket exclusion of micro and small entrepreneurs from the framework of the Directive has been abandoned. This is because it was considered that size measurable through employment or earnings is not relevant in certain cases, which should be verified as meeting certain requirements. These requirements may include, in particular, relevance to the supply of other services that may be considered essential for the country concerned.

Thus, the designed changes are generally perceived as common sense and seem to result from a real and thorough analysis of the problems encountered in the implementation of the NIS Directive regulations. However, it is necessary to delve into the adopted solutions in more detail and compare them with the existing regulations to be able to answer the question of whether the modifications will contribute to the achievement of the intended objectives and, in particular, whether they will allow for the development of the cybersecurity labour market by increasing the demand for cybersecurity professionals on a wider scale.

Introducing a distinction between essential and important entities

In order to ensure that a wider range of entities are covered by the NIS Directive 2.0, an entirely new subdivision of entities included was proposed. This was also intended to avoid unnecessary definitional difficulties arising from using the same terminology for different cases. It should be noted, however, that the newly designed categories reveal a significant convergence with the

existing regulation and the entities that are included within them. This only confirms the claim that they have been modified rather than completely transformed. However, it is observed at the very outset that „the level of criticality of a sector or type of service, as well as the level of dependence of other sectors or types of services, should be taken into account in this division. Both essential and important entities should be subject to the same risk management requirements and incident reporting obligations"[32]. At the same time, an explanation is given as to why such a division is made if both entity groups are to be subject to the same requirements. This is is dictated by the differentiation of „the supervisory and enforcement regimes for those two categories of entities to ensure a fair balance between risk-based requirements and obligations on the one hand, and the administrative burden stemming from the supervision of compliance on the other"[33]. This is, therefore, a very different approach to the differentiation between the introduced categories compared to the NIS Directive, where the obligations imposed already diverged significantly from each other.

The essential entities identified in the NIS 2 Directive are, according to Appendix I and Table 1 above, those belonging to the energy, transport, banking and financial markets infrastructure, healthcare, drinking water and wastewater, digital infrastructure and business-to-business ICT service management[34], public administration and space sectors. This list is, therefore, considerably broader than that provided for under Appendix II of the NIS Directive, with which it can be compared. It additionally includes, e.g., public administration and entities in the space sector, which have not been directly identified to date.

The second of the newly introduced groups is the category of important entities detailed in Appendix II, which includes the following sectors: 1) postal and courier services, 2) waste management, 3) production, manufacture and distribution of chemicals, 4) production, processing and distribution of food, 5) manufacturing in its broadest sense, within which several sub-categories are provided for, as well as 6) digital service providers, which includes the familiar NIS Directive providers of online trading platforms and search engines and a new category – providers of social networking service

32 Recital 11 of the NIS Directive 2.0.
33 Ibidem.
34 This category was not present in the draft legislation in question and was added at the last legislative stage.

platforms, and 7) the research sector[35]. Interestingly, the English version of the NIS 2 Directive does not include the term „digital service providers", which would correspond to the category of the same name found in the NIS Directive, but „digital providers", although the reason for this change and its purpose is not indicated[36].

It would, therefore, appear that it is the category of important entities that are responsible for the fundamental extension of the scope of the regulation in question concerning the repealed act[37]. This also coincides with the demands expressed by the authors in view of their research on the cybersecurity of digital service providers. Indeed, the expansion of the entity categories is essential for the sealing of the entire system, which is only as resilient as its weakest element[38]. A similar qualitative change was the introduction under the GDPR[39] of a wide range of obliged entities compared to Directive 95/46/EC[40], which it repealed, although, in this case, the decision has been made to further consolidate the provisions by changing the legal form from a directive to a regulation. This also seems inevitable for the cybersecurity sphere in the coming years and most likely as part of the next revision of cybersecurity rules at EU level[41].

Relationship between the nis 2 directive entity categories and those in the nis directive

The relationship between the „newly designed" entity categories and those found in the predecessor of the legislation under discussion is discernible at first glance and manifests itself, for example, in the convergence between the

35 This category was also added at the last legislative stage.

36 The rule of rationality of the legislator leads to the assumption that the marked change may have a substantive basis.

37 Highlighting the relevance of including the public administration sector in the group of essential entities.

38 Although this may be a truism, it is a fact that the potentially weakest elements are also those that are mostly targeted by violators.

39 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the European Union 2016, L 119/1).

40 Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal of the European Communities 1995, L 281/31).

41 Which is already advocated by the authors as a necessary next step.

components of these categories. At the same time, they are key changes for increasing the demand for cybersecurity professionals for a wide range of entities, and not only within cybersecurity service providers or entities obliged to ensure its adequate level under other acts. This is even clearer given that the NIS 2 Directive provides for a correlation table[42] between this legislation and the NIS Directive it repeals. This can only confirm that this scope is not wholly separate from the categories provided for under the repealed act but rather constitutes a modification of it and should be seen as such. Simultaneously, this is consistent with the arguments set out in the explanatory memorandum of the legislation and its recitals, as referred to above.

It should be clear from the table provided in the annex to the legislation in question that the operators of essential services are designated as essential entities in the NIS Directive 2.0, where the very name makes clear the link between them. However, this should not come as any surprise. These entities were already treated in a considerably more restrictive manner under the existing act, which justifies their joint treatment also in the revised cybersecurity regime. These are, therefore, entities that must be considered indispensable for the organisation of this system of each state and, consequently, entities to which a number of cybersecurity obligations are dedicated. It is worth noting the inclusion of public administration entities in this category. This may have a significant impact on the formation of the cybersecurity labour market. Indeed, public administration is a significant employer on a national scale.

Interestingly, cloud computing providers have also been included in this category[43], whereas in the repealed act, they were included in the category of digital service providers. However, the other two types of digital services, i.e., online trading platforms and search engines, have been provided for under Annex II, i.e. under the category of valid entities. The existing category of digital service providers has, therefore, been split. Only cloud computing service providers have been recognised as entities that should meet higher standards regarding the organisation of a cybersecurity system.

It should be noted that the changes introduced in this area under the NIS 2 Directive result in a dramatic increase in the number of entities obliged under this act, from almost 15,500 to 110,000 entities in the European Union,

42 As part of Appendix III.
43 Appendix II (8).

according to estimates[44]. This estimated scale alone could, therefore, result in a huge increase in demand for cybersecurity professionals, creating a labour market.

Additional scope of obligated entities in nis 2.0 and impact on the labour market

Although the approach regarding the size of the entity in question for qualification under the NIS 2 Directive has been applied as described earlier, Art. 2(2) indicates which entities, regardless of their size[45], will always be treated as falling within the scope of the act. This, therefore, indicates that although the size criterion is indicated, it will not apply in „sensitive" cases, yet it is in many cases that these entities will demonstrate a need for specialised services to meet the requirements of this legislation.

This provision should be divided into two main parts. The first indicates which entities will always be subject to the requirements of the Directive and its implementing acts by virtue of the type of services provided. According to the element indicated, undertakings providing public electronic communications networks or publicly available electronic communications services, trust service providers, top-level domain name registries and domain name system (DNS) service providers will be subject to certain requirements regardless of status. Furthermore, five additional indications are provided for entities that are not covered by the previous requirements. The first indication, in contrast to the first draft of this legislation, is for entities that are the sole provider of services critical to maintaining critical social or economic activity. The content of this category itself – and therefore also its scope – has changed from the draft. The quantifying element of the service has been added. It is now insufficient that the service is provided by a sole provider, plus it must be critical for maintaining essential social or economic operations in the state. The range of entities potentially covered by this category has, therefore, been narrowed considerably. This seems strongly warranted. Two categories were subsequently identified, emphasising the possible impact of the disruption of

44 European Commission. Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 2020, p. 20, SWD (2020) 345 final.

45 That is, including micro and small entrepreneurs.

their services on the wider public. The first includes service providers whose disruption could significantly impact public order, public safety or public health. The second includes service providers whose disruption could lead to serious systemic risks, particularly in sectors where such disruption could have a cross-border impact[46]. A separate category also exists for those which are critical because of their particular importance at a national or regional level for a specific sector or type of service or other interdependent sectors in a Member State[47].

The last category of the list is dedicated to public administration entities, where the scope has also been significantly modified for the draft legislation. The draft legislation identifies them only by reference to a definition, emphasising that they are entities which, in the Member State concerned, are established for meeting needs in the general interest and not having an industrial or commercial character, have legal personality and are financed, for the most part, by the state, regional authorities or other bodies governed by public law[48], and are empowered to take administrative or regulatory decisions affecting their rights in relation to the cross-border movement of persons, goods, services or capital. As adopted, Art. 2(2)(f) of the NIS 2 Directive provides for two constituent categories of public administration of a mandatory nature, i.e. central and regional administrations and local administrative entities to which the NIS 2 Directive may apply based on a decision by a state authority[49]. This gives the impression of a cascade arrangement of entities belonging to the public administration group due to the scope and extent of their competencies. This is warranted because of the possible impact on the broader national interest, which, in the case of local entities, is far more geared towards serving individuals. Invariably, administrative bodies that „carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal

46 Relative to the draft, the scope of these two categories has only changed by removing the „contingency" of disruption to a particular service, which was not indicated in the adopted version of the act.

47 Irrespective of the entities identified as critical, which in the project were also included in a separate letter of this list.

48 Or its management is subject to supervision by those authorities or bodies; or more than half of the members of its administrative, management or supervisory body have been appointed by the State, regional authorities or other bodies governed by public law.

49 In accordance with Art. 2(5)(a).

offences" are excluded[50]. This exclusion is justified on the grounds that individual states should be able to take the necessary measures to protect the interest indicated in the wording of the cited exclusion[51].

It should also be noted that another change concerning the draft, which appears to be purely technical, is the exclusion from the above list – to a separate paragraph – of entities identified as critical under Directive (EU) 2022/2557. This, however, is not essential from this study's point of view, as these entities were already among those employing or using the services of cybersecurity specialists in connection with separate regulations.

These developments, together with the geopolitical situation and other factors mentioned at the beginning of this text, are of fundamental importance to the wider labour market. In particular, they are affecting all aspects of work as digitalisation and remote working arrangements become more common[52]. This also further increases the need for specialists dealing with business security issues and a wide range of employees working remotely – a previously uncommon situation. The combination of all the factors identified results in one of the broadest surveys on IT trends, showing cybersecurity (78% of respondents) as the top trend with the broadest relevance to the labour market. More importantly, however, cybersecurity was considered more significant than the trend related to artificial intelligence and machine learning technology, which came second in this survey (62%), with cybersecurity at a clear advantage. This shows that there is already a high awareness of the growing staffing needs within this specialisation in the IT industry. This, combined with the creation of market needs under the new regulations, will inevitably lead to the overall separation of the cybersecurity labour market from the broader IT labour market, along the lines of the information security area[53] or the video game development industry.

Conclusions

The NIS Directive has clearly initiated a holistic approach to cybersecurity. Additionally, the NIS 2 Directive discussed in this text is a leap forward towards

50 Art. 2(7) of the NIS 2 Directive.
51 According to Recital 9 of the NIS 2 Directive.
52 And in a hybrid form, which is increasingly becoming the standard.
53 Which may now fall into the area of cybersecurity.

the goals set by these lawss. This effect seems achievable only through the sealing of obligations for a broader category of entities. This, in turn, is linked to an increased demand for cybersecurity professionals and the creation of a self-contained labour market. A similar situation occurred, albeit seemingly on a smaller scale, in 2018 when the GDPR came into force and the market for data protection consultants and, in particular, the services of Data Protection Officers emerged from the broader legal market. Notwithstanding the above, it should be noted that the act also provides for a number of other elements that are significantly similar, warranting a comparison between the possible effects of the changes and those associated with the entry into force of the GDPR. For instance, the territorial scope of the act is consistent with that established in the GDPR[54]. Moreover, it has a similar penalty regime[55] to „incentivise" obliged entities to comply with the requirements of the NIS 2 Directive.

The mere extension of the scope of entities obliged under the NIS Directive is intended as a remedy to, or has the potential to help combat, the cybersecurity threat identified in the first place by ENISA for the coming decade – supply chain attacks[56]. This is because broadening the scope of obliged entities will undoubtedly allow supply chain participants, who until now have often not used cybersecurity services, to be largely covered. This in itself will have a positive impact on the knowledge of cyber risks and, in combination with the other factors identified, should allow for a faster and wider emergence of a labour market related to, for example, securing against these risks or fulfilling formal requirements, as was the case with the protection of personal data.

In many cases, the solutions coincide with the propositions put forward by the authors within the framework of the monograph presenting the results of the research on the requirements for digital service providers under the NIS Directive. However, these propositions still hold valid. Indeed, it is necessary to further expand the scope of obliged entities to tightly cover the supply chains in the first place and then eliminate any cases in which a given entity[57] is not subject to any „digital hygiene" obligations, i.e. basic rules of functioning in the virtual space, which may include the installation of basic cybersecurity

54 V. Lucini, *The ever-increasing cybersecurity compliance in Europe: The NIS 2 and what all businesses in the EU should be aware of*, „Russian Law Journal" 2023, vol. 11, no. 6, p. 150.

55 And thus tested in the market.

56 *Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!*, https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030 [access: 2.05.2023].

57 Regardless of the industry in which it operates or its size.

software, prompt software updates, obligations to report cyber-attacks and password strength requirements. Of course, these should be supported by awareness-raising and digital competence campaigns conducted by dedicated public administration bodies, as was the case with the data protection system and the labour market for data/information protection specialists created within it. The research results seem to be confirmed by analyses according to which the number of vacancies in this sector is expected to reach 3.5 million positions by 2025[58]. It seems that this could already represent a considerable segment of the labour market.

Bibliography

Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!, https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030 [access: 2.05.2023].

Lucini V., *The ever-increasing cybersecurity compliance in Europe: The NIS 2 and what all businesses in the EU should be aware of*, „Russian Law Journal" 2023, vol. 11, no. 6.

Mahendru P., *The State of Ransomware in Retail 2022*, https://news.sophos.com/en-us/2022/09/07/the-state-of-ransomware-in-retail-2022/ [access: 15.12.2023].

Official Cybersecurity Jobs Report, 2022, https://www.esentire.com/resources/library/2023-official-cybersecurity-jobs-report [access: 15.06.2023].

Pasławski K., *Cyberwojna wokół Ukrainy. Nowe dane*, 2022, https://crn.pl/aktualnosci/wojna-na-ukrainie-cyberwojna-wokol-ukrainy-nowe-dane/ [access: 15.12.2023].

Porzeżyński M., *Cyberbezpieczeństwo dostawców usług cyfrowych*, Warszawa 2021.

Report: Barometr cyberbezpieczeństwa. COVID-19 przyspiesza cyfryzację firm – marzec 2021, https://kpmg.com/pl/pl/home/insights/2021/04/raport-barometr-cyberbezpieczenstwa-2020-covid-19-przyspiesza-cyfryzacje-firm.html [access: 15.06.2023].

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

Wpływ skutków pandemii koronawirusa na potrzeby kompetencyjne sektorów informatyki oraz telekomunikacji i cyberbezpieczeństwa w konsekwencji rozwoju zastosowań technologii cyfrowych oraz kształtowania się nowego modelu pracy – kwiecień 2023, https://antal.pl/wiedza/raport/wplyw-skutkow-pandemii-koronawirusa-na-potrzeby-kompetencyjne-sektorow-informatyki-oraz-telekomunikacji-i-cyberbezpieczenstwa [access: 15.06.2023].

Zalcewicz A. *New Technologies in the Control of Public Finances and Building Public Confidence in the State*, „Bialystok Legal Studies" 2023, vol. 28, no. 2.

58 *Official Cybersecurity Jobs Report*, 2022, https://www.esentire.com/resources/library/2023-official-cybersecurity-jobs-report [access: 15.06.2023].

Zmiany wprowadzone dyrektywą NIS 2.0 i ich potencjalny wpływ na kształtowanie rynku pracy w obszarze cyberbezpieczeństwa

Streszczenie

Zapewnienie cyberbezpieczeństwa jest obecnie jednym z największych wyzwań ludzkości, oprócz rozwoju sztucznej inteligencji. Sformułowanie to nie jest hiperbolą, gdyż zagrożenia te dotyczą zarówno władz publicznych, jak i przedstawicieli podmiotów prywatnych oraz osób fizycznych. Wraz z dynamicznym rozwojem technologii i galopującą cyfryzacją nie ustają działania podmiotów, które chcą wykorzystać to, że nie przykładają one wystarczającej wagi do zabezpieczenia sfery obecności w sieci. Unia Europejska próbowała temu przeciwdziałać licznymi wystąpieniami, a w efekcie także przyjęciem dyrektywy NIS. Po kilku latach funkcjonowania tego aktu prawnego dokonano oceny jego skutków i przygotowano wiele zmian mających na celu podniesienie ogólnego poziomu cyberbezpieczeństwa. Nie przyniesie to żadnego efektu bez specjalistów z dziedziny cyberbezpieczeństwa i wprowadzenia ich do różnorodnych środowisk, nie tylko największych podmiotów. Analogiczna sytuacja miała miejsce w przypadku wprowadzenia ogólnego rozporządzenia o ochronie danych osobowych (RODO), kiedy to istniejące wcześniej przepisy w tym zakresie zostały rozwinięte do tego stopnia, że doprowadziły do powstania (wyodrębnienia się) niezależnego rynku doradztwa w zakresie ochrony informacji, ze szczególnym uwzględnieniem danych osobowych dotyczących doradztwa technicznego i prawnego. Stąd porównania do RODO są uzasadnione. W niniejszym artykule autorzy dokonali przeglądu i oceny zmian przepisów dotyczących cyberbezpieczeństwa, w tym kategorii dostawców usług cyfrowych, dyrektywy NIS 2.0 oraz ich przewidywanego wpływu na rynek pracy.

Słowa kluczowe: cyberbezpieczeństwo, NIS 2, rynek pracy