Legal Assessment of the National Cybersecurity System in Poland in the Light of the New Developments in the NIS2 Directive

A. Besiekierska
Cardinal Stefan Wyszynski University, Department for Informatics Law, Warsaw, Poland
agnieszka.besiekierska@uksw.edu.pl

***Abstract* – The Polish Act on the National Cybersecurity System was adopted on 5 July 2018. Unlike with the NIS Directive, which it implemented, the scope of its regulation covered public administration. It turned out in the course of its application that the introduced regulations were rather ineffective. It was particularly visible in the case of local governments, which, as indicated by the reports of the Supreme Audit Office, showed numerous shortcomings in the implementation of relevant cybersecurity policies. For more than two years, work has been underway on a draft amendment to the Act on the National Cybersecurity System, which has aroused great controversy, and the ninth draft has now been published. Discussions are taking place primarily in the area of the supply chain cybersecurity and include its geopolitical aspects, which will undoubtedly be of great importance for the further development of the cybersecurity system in Poland and Europe.**

Keywords – cybersecurity; national cybersecurity system; NIS2 Directive

I. INTRODUCTION

In recent years, the number of ICT legislation has increased significantly in the EU, especially in the area of cybersecurity. It includes the NIS Directive, its successor – the NIS2 Directive, the Cybersecurity Act, sectoral acts, such as the DORA, as well as the proposed EU Cyber Resilience Act. A large number of legal acts cause problems with the absorption of the EU legislation at the national level. A negative example could be the protracted works in Poland on the implementation of the European Electronic Communications Code which had been planned to be completed in 2021 and are still pending (as of 19 March 2023). This intense legislator's activity is often referred to as the legislative tsunami [1].

In the maze of the existing and planned legal acts, the NIS Directive, and its successor, i.e. the NIS2 Directive, are the first cross-sectoral legal acts in the area of cybersecurity, as well as a starting point for establishing the National Cybersecurity System in Poland. The paper outlines the main principles of the NIS and NIS2 Directives and points out some pros and cons for the existing legal provisions in the context of the planned amendment of the Polish National Cybersecurity System. The research was based on the analysis of legal acts and literature, including reports on the implementation of obligations in the field of cyber security issued by the Supreme Audit Office, as well as the analysis of the position papers raised in the pre-legislative process for the draft amendment of the Act on the National Cybersecurity System.

II. NIS DIRECTIVE

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 (NIS Directive), adopted on 6 July 2016, imposed a number of obligations on the Member States concerning the establishment of specific institutions and cooperation mechanisms. Each Member State was obliged to set up the National Competent Authorities for network and information security, whereas the function could be performed by the already existing institution or institutions. The task of the National Competent Authority was to monitor the implementation of the provisions of the Directive at the national level throughout all sectors addressed by the regulation. Those Competent Authorities had the power to investigate cases of non-compliance in the field of network and information security, issue IT security guidelines as well as impose sanctions for non-compliance [2].

In order to strengthen the Member States' cooperation, each Member State had to establish a Single Point of Contact. Its task was to collect information on incidents on a national scale, and exchange information on significant international incidents with its foreign counterparts. The NIS Directive also provided for the creation of CSIRTs, i.e. a Computer Security Incident Response Teams. Member States could designate one country-wide CSIRT or build a network of sectoral CSIRTs covering market sectors [3].

The NIS Directive provided for two types of entities, their role being to fulfil cybersecurity obligations: operators of essential services from among those listed in Annex II to the Directive (energy, transport, banking, financial markets, health sector, drinking water supply and distribution, digital infrastructure) and digital service providers (online marketplace, online search engine, cloud computing service, as indicated in Annex III). The operators of essential services were required to assess the risk of cyber threats and to adopt appropriate measures to

ensure network and information security. They also had to report any incidents seriously threatening their networks and IT systems to the competent authorities. Incidents bearing a significant impact on the continuity of operations of operators were subject to mandatory reporting, which meant that the reporting thresholds were to be determined by the Member States in the process of implementing the provisions of the Directive. Digital service providers were subject to the so called "light touch" approach. It consisted in *ex post* supervisory activities, i.e. following an incident and only by the country where the service provider was based [4]. It is worth noting that the communications undertakings had not been included within the scope of the NIS Directive and remained subject to sector specific regulation, i.e. Directive 2002/21/EC (Framework Directive) [5]. The NIS Directive was to be transposed into the Member States' national laws by 9 May 2018.

III. NATIONAL CYBERSECURITY SYSTEM

In Poland, the NIS Directive was implemented by the Act of 5 July 2018 on the National Cybersecurity System, which created the National Cybersecurity System, and which is still the most important Polish legal act in the field of cybersecurity. The National Cybersecurity System provides for the competent authorities for network and information security, three CSIRTs, essential services operators, digital service providers and public administration entities [6]. Unlike the NIS Directive, which did not apply to public administration services, the Polish legislator decided to include the public sector. That was possible due to the fact that the NIS Directive served as a minimum harmonization framework which meant that it only set out certain minimum conditions that had to be met [7]. With their number amounting to approximately 3,000, public entities are currently the largest group within the National Cybersecurity System [8].

A significantly less numerous group are the essential services operators and digital service providers, with probably nearly 400 operators of essential services and about 50 providers of digital services [9]. The numbers are not exact, as the operators are designated and placed on the list of operators of essential services by the competent minister, and both the decision and the list of operators of essential services are confidential.

In practice, it turned out that the entities covered by the National Cybersecurity System do not fully fulfil the obligations arising from the Act. To a large extent this applies to public entities, which, despite the binding legal obligations to ensure the data security and integrity, often fail to comply with basic security principles and are exposed to cyberattacks. In its audit reports, the Polish Supreme Audit Office (NIK) negatively assessed the performance of tasks related to ensuring the security of the processed information, indicating that the public entities, especially local governments, lacked a systemic approach to ensuring information security. The public entities did not have information about their IT resources, did not perform risk assessments, as well as did not carry out an annual audit. 48% of them failed to make backups, improperly stored the backups or did not check the correctness of the copies made [10]. Failure to comply with basic security principles makes the public entities highly vulnerable to cyberattacks. As bad as it is, the situation may to a large extent result from the technical and organizational problems related to the high costs of professional IT support. Neither do the low financial fines which may be imposed for infringements on the basis of the Act support law enforcement.

IV. NIS2 DIRECTIVE

The Commission was obliged to periodically review the functioning of the NIS Directive and to report to the European Parliament (Article 23(2) of the NIS Directive), whereas the report on the results of the first review was to be presented by 9 May 2021. As part of the review activities, the Commission identified numerous issues relating to the implementation of the NIS Directive. First of all, it identified significant differences in the implementation and identification of essential services operators in the Member States. Since the Directive established a minimal legal framework for harmonization, each Member State could enjoy considerable freedom in implementing its provisions. As a result, there were different thresholds for identifying operators of essential services as well as different thresholds for reporting ICT incidents. That resulted in a highly fragmented market, with operators providing services in several Member States having to comply with different legal regimes. Further, the scope of the NIS Directive was found to be insufficient as it did not address certain sectors and operators, despite their key importance from the point of view of cybersecurity [11]

As a result of the review and the discussions which followed, the European legislator decided to adopt a new Directive, 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 (NIS2 Directive), which replaced the NIS Directive. The NIS2 Directive extends the subjective scope of its predecessor to cover new sectors and include, among others, public administration, food, chemical, sewage, industry (production of medical devices and medical devices for *in vitro* diagnostics, computer, electronic and optical products, electrical equipment, machinery and equipment, motor vehicles, trailers and semi-trailers, other transport equipment), waste management and space, and treats some sectors more broadly (e.g. expanding the scope of digital infrastructure). Unlike the NIS Directive, which distinguished between essential services operators and digital service providers, NIS2 divides entities from the above mentioned sectors into two categories: essential entities and important entities. Communications undertakings, i.e. providers of public electronic communications networks and/or providers of publicly available electronic communications service, fall within the scope of the NIS Directive as essential entities [12]. Such approach may potentially result in losing the experience with legal, technical and economic aspects of security which had been built in the telecommunications sector framework for over 10 years.

As regards the terms of management, operation and disclosure of security vulnerabilities, testing cybersecurity

levels and effective use of encryption, entities covered by the NIS2 Directive are subject to much stricter requirements than before [13]. The new Directive also includes more precise provisions in the field of incident reporting. In addition, Member States may require essential and important entities to obligatorily certify products, services and processes in accordance with the European certification schemes provided for under the Cybersecurity Act. Undoubtedly, mandatory certification would contribute to increasing cybersecurity. However, taking into account the long lasting works on European cybersecurity certification schemes and the controversies that those works raise, in particular in relation to cloud computing services, one may be concerned that such mandatory cybersecurity certification will not be introduced soon. Also the fact that the NIS2 Directive, similarly to the Cybersecurity Act, does not deal with the issue of cybersecurity certification in relation to digital resources can be considered a drawback [14].

Another new element is the introduction of a coordinated risk assessment of critical supply chains at the EU level. Following consultations with the Cooperation Group and ENISA, the European Commission may identify critical ICT services, systems or products that may be subject to a coordinated risk assessment which will correspond to the one that was carried out for the 5G network [15].

To ensure better law enforcement, the NIS2 Directive provides for high financial penalties for entities which fail to implement its provisions in a proper manner. Those penalties amount to a maximum of at least EUR 10.000.000 or up to 2% of a company's total annual worldwide turnover, whichever is higher. A novelty is the introduction of the company management's responsibility for compliance with cybersecurity risk management measures. Further, the NIS2 Directive also introduced provisions increasing the role of the European Commission, which will assess the implementation of the Directive in the Member States every 18 months, whereas the review should also address such issues as funds allocated to cybersecurity, resources and development of cybersecurity capabilities. Thus, unlike in the case of the NIS Directive, it will not only serve as an assessment of the transposition of the provisions of the Directive itself.

The NIS2 Directive has to be transposed into national laws by 17 October 2024.

V. PLANNED AMENDMENT TO THE NATIONAL SECURITY SYSTEM

The work on the amendment of the Polish Act on the National Cybersecurity System has been underway since 2020, with the first draft act published in September 2020 and the most recent, the ninth one, in January 2023. The amendment process has been carried out independently of the adoption of the NIS2 Directive and the planned provisions do not implement it. The release of the drafts was often preceded by public consultations, including hundreds of position papers, which makes the amendment process incomparably more intense than any other before. The non-completion of this long-lasting process hinders the announcement of the auction for 5G frequencies, as the planned amendment should introduce the security measures referred to in the EU 5G Toolbox. Due to the delayed assignment of the 5G frequencies, Poland is at the very end in Europe when it comes to the use of the 5G technology [16].

The most significant and, at the same time, the most controversial change introduced by the draft act amending the Act on the National Cybersecurity System relates to the development of the 5G network in Poland. It provides for a new status of communications undertakings, i.e. providers of communications services and networks, which are to be included in the National Cybersecurity System. The inclusion of communications undertakings has been combined with the planned provisions on the control of the supply chain. As part of the supply chain control, a procedure is to be introduced to identify a supplier as a high-risk one. The procedure would be initiated by the minister competent for computerization and might apply to a software or equipment supplier. When issuing a decision, the minister would take into account an analysis, prepared by a special collegial body, which would cover both technical as well as non-technical and political aspects, such as economic, intelligence and terrorist threats to national security or threats to the implementation of allied and European commitments, or the likelihood that the hardware or software supplier remains under the control of a country outside the EU or NATO territory. Should a decision to identify a supplier as a high-risk one be issued, the entities being part of the National Cybersecurity System would not be allowed to use ICT products and software within the scope covered by the decision and provided by the high-risk supplier, and would have to withdraw those used within a certain time limit (5 or 7 years). The decision would be immediately enforceable and courts would not have the capacity to stop its execution. In the intense public debates, which may be fuelled by different interest groups, strong opinions have been voiced that the planned changes raise controversies concerning their constitutionality, in particular regarding the freedom of economic activity or openness of proceedings, as well as those indicating the geopolitical situation in which the World is getting polarized along the West – Far East axis [17].

For the first time, the draft amendment creates a national cybersecurity certification system and defines rules and a procedure for cybersecurity certification of ICT products, ICT services or ICT processes, and thus implements the provisions of the EU Regulation Cybersecurity Act. By way of a regulation, the Council of Ministers may determine a national cybersecurity certification program for a given product, service or process, taking into account the need to develop requirements in accordance with current scientific and technical knowledge and with the aim of increasing cybersecurity in Poland. certification system corresponds with the provisions the Cybersecurity Act.

VI. CONCLUSION

The Polish legislator was ahead of the European one by including public entities within the national cybersecurity system. However, the Polish Supreme Audit Office (NIK) audits indicate a low level of cybersecurity

compliance by those entities. Currently, trying to control the maze of cybersecurity regulations, the Polish legislator has chosen a strategy that has not been successful so far. It is still dealing with 5G security requirements, creating a legal framework allowing the exclusion of hardware and software from high-risk vendors, while it is already time to start implementing the NS2 Directive. Taking into account the problems with the amendment of the Act on the National Cybersecurity System, the question arises how long it will take to implement the NIS Directive. Any delay in the transposition of the NIS2 Directive is harmful, as the Directive contains numerous legal solutions conducive to better law enforcement.

At the same time, the example of the works relating to the amendment shows how closely today's cybersecurity issues are related to global politics and how the political aspects may be even more important than the technical ones. This will probably result in works on any subsequent legal acts addressing cybersecurity issues, such as the aforementioned EU level coordinated risk assessment of critical supply chains even more complex and time-consuming.

REFERENCES

[1] A. Besiekierska, J. Mazur, A. Mednis, J. Mojsiejuk, W. Paluszyński et al., "The law is no substitute for common sense", Prawo nie zastąpi zdrowego rozsądku, Domena , 2022, vol. 2, pp. 4-9.

[2] S.Schmitz-Berndt, P. G. Chiara, "One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive", Int. Cybersecur. Law Rev., 2022, no. 3, pp.294-295.

[3] G. Szpor, "European regulation of network and information systems security and state sovereignty", Europejska regulacja bezpieczeństwa sieci i systemów informacyjnych a suwerenność państwa, in G. Szpor, A. Gryszczynska, Internet. Strategie Bezpieczeństwa, Warsaw, C.H. Beck, 2017, pp. 13-15.

[4] D. K. Kipker, "The EU NIS Directive compared to the IT Security Act- Germany is well position for the new European Cybersecurity Space, ZD-Aktuell 2016, 05363.

[5] S. Piątek, "Obligations of telecommunications undertakings related to cybersecurity", Obowiązki przedsiębiorców telekomunikacyjnych w zakresie cyberbezpieczeństwa, internetowy Kwartalnik Antymonopolowy i Regulacyjny, 2020, vol. 9 , no 2, pp. 28-41.

[6] P. Wajda, "Cybersecurity – sectoral aspects of the regulation", Cyberbezpieczeństwo – sektorowe aspekty regulacyjne, internetowy Kwartalnik Antymonopolowy i Regulacyjny, 2020, vol. 9 , no 2, pp. 14-26.

[7] A.Besiekierska, "Commentary to the Act on National Cybersecurity System", Ustawa o krajowym systemie cyberbezpieczństwa, C.H. Beck, Warsaw, 2019, p.103.

[8] Regulatory impact assessment (OSR) of 17 January 2023, https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/630873_projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html., pp. 8-13, [access: 19.03.2023].

[9] Regulatory impact assessment (OSR) of 17 January 2023, pp.-8-13.

[10] Information on the results of the NIK au-dit, Implementation of public services for citizens using the ePUAP platform, Informacja o wynikach kontroli NIK, Realizacja usług publicznych dla obywateli zwykorzystaniem platformy ePUAP , 2021, https://www.nik.gov.pl/kontrole/P/20/004/ [access: 19.03.2023], Information on the results of the NIK audit, Information security management in local government units, Informacja o wynikach kontroli NIK, Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego, 2019 https://www.nik.gov.pl/kontrole/P/18/006/[[access: 19.03.2023], Information on the results of the NIK au-dit, Information security at remote work and mobile data processing (Informacja o wynikach kontroli NIK, Bezpieczeństwo informacji w pracy na odległość imobilnym przetwarzaniu danych, 2022, https://www.nik.gov.pl/kontrole/P/21/081/LOL/ [access: 19.03.2023].

[11] Z. Bederna, Z. Rajna, "Analysis of the cybersecurity ecosystem in the European Union," Int. Cybersecur. Law Rev., no. 3, 2022, pp. 45–46,

[12] A. Piechocki, K. Gorzkowska, "Planned changes in cybersecurity", Planowane zmiany w cyberbezpieczeństwie, PNT 2021, no 1,

[13] T. Sievers, "Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations", Int. Cybersecur. Law Rev., 2021, vol. 2, pp. 225–227.

[14] S.A. Salvaggio, S.A., N. González, "The European framework for cybersecurity: strong assets, intricate history". Int. Cybersecur. Law Rev., 2023, vol. 4, pp. 140–142; D. D. Stewart Ferguson, "European Cybersecurity Certification Schemes and cybersecurity in the EU internal market", Int. Cybersecur. Law Rev., vol. 3, 2022, pp. 54-55.

[15] EU Coordinated Risk Assessment published October 9, 2019 https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-as-sessment-5g-networks-security, acces: 19.03.2023.

[16] Kearney 5G Readiness Index 2022: https://www.kearney.com/telecommunications/article/-/insights/time-is-tight-for-telcos-on-5g-strategies-even-as-the-european-rollout-lags , [access: 19.03.2023].

[17] A. Besiekierska, "Legal Aspects of the Supply Chain Cybersecurity in the Context of 5G Technology", Review of European and Comparative Law, 2022, vol. 51, no. 4, 129–147; R. Siudak, "Cybersecurity in Poland. From discourses to public policies", Cyberbezpieczeństwo w Polsce, Od dyskursów do polityk publicznych, Księgarnia akademicka, Cracow, 2022, pp. 165–170.