Supervision and Inspection in the Field of Cybersecurity

MAŁGORZATA CZURYK

Abstract The national cybersecurity system consists of a number of entities that play important roles in protecting cyberspace from threats, including those compromising the normal functioning of the state. The national cybersecurity system aims to ensure national cybersecurity, including the uninterrupted provision of critical and digital services, by achieving an adequate level of security within the information systems used to provide these services and ensuring incident handling. Supervision and inspection in terms of compliance with security requirements covers providers of cybersecurity services, operators of essential services, as well as digital service providers.

Keywords: • supervision • inspection • cybersecurity • essential service • digital service

CORRESPONDENCE ADDRESS: Małgorzata Czuryk, Ph.D., Dr. Habil., University Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, ul. Obitza 1, 10-725 Olsztyn, Poland, e-mail: malgorzata.czuryk@uwm.edu.pl, ORCID: 0000-0003-0362-3791.

https://doi.org/10.4335/2022.1.11 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Cybersecurity can be seen in both public and private aspects. The development of information technologies has, on the one hand, resulted in much greater opportunities for the rapid acquisition, transmission, or collection of information, while on the other hand, new threats have arisen that occur in cyberspace. In view of the great importance of ICT systems and networks, both for the economic and public sphere, the state must have appropriate tools to combat cyberattacks, especially those that are relevant to its functioning. It is the purpose of supervision and inspection to prevent unwanted incidents in cyberspace, thus ensuring cybersecurity at an appropriate level and allowing the uninterrupted performance of public tasks. The ideal state of being free of all disruptions is not achievable, so the realistic objective is to ensure a level of cybersecurity that allows public needs to be met uninterruptedly, while maintaining appropriate quality standards and adequate availability of services at optimal cost of service provision.

Cybersecurity involves the prevention of threats, their anticipation, as well as the removal of consequences arising from their occurrence. The sphere in which such threats and threat outcomes occur is cyberspace (Karpiuk, 2021a: 612). According to Article 2(4) of the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Polish Journal of Laws of 2020, item 1369, as amended) – the Act is hereinafter referred to as the 'NCSA', cybersecurity is the resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems. As information systems develop, an adequate protective infrastructure must also be created to ensure security in cyberspace.

Nowadays, cybersecurity is very important, and the consequences of actions that undermine this type of security are experienced not only in the public sphere, but also in the economic and social spheres. Therefore, the state must react quickly and decisively to cyberattacks by looking for ever more modern protection mechanisms (among other actions). Responding to the increasingly frequent threats to cyberspace, the legislators have decided that an appropriate legal regulation is necessary, allowing for both a proper diagnosis and an adequate response in the event of cyberattacks (Karpiuk, 2021b: 234). In today's highly computerised world, in addition to the activities of public entities in ensuring the security of various resources, technical protection is increasingly needed (Chałubińska-Jentkiewicz, Karpiuk, Kostrubiec, 2021: 52).

Under the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Polish Journal of Laws of 2020, item 1369, as amended), supervision and inspection applies to operators of essential services, digital service providers and providers of cybersecurity services, and it is these aspects that the analysis will focus on. An essential service, according to Article 2(16) of the NCSA, is a service that is deemed essential in maintaining critical social or economic activity and which is included on the list of essential services. A digital service, according to Article 2(15) of the NCSA, is an

electronically supplied service. Provision of an electronically supplied service is, according to Article 2(4) of the Act of 18 July 2002 on Providing Services by Electronic Means (consolidated text, Polish Journal of Laws of 2020, item 344, as amended), the performance of a service rendered without the simultaneous presence of the parties (at a distance), through the transmission of data at the individual request of the customer, sent and received by means of electronic processing devices, including digital compression and data storage, which is entirely broadcast, received or transmitted via a telecommunications network. At the same time, telecommunications networks, pursuant to Article 2(35) of the Act of 16 July 2004 – Telecommunications Law (consolidated text, Polish Journal of Laws of 2021, item 576, as amended), should be understood as transmission systems and switching or routing equipment, as well as other resources, including inactive network elements, that enable the broadcasting, reception or transmission of signals by wire, radio, optical or other electromagnetic means, regardless of their type.

2 The concept of supervision and inspection

The concept of supervision should be understood as such shaping of mutual relations between public administration entities, in which the supervisory entity has the power to directly interfere with the activities of the supervised entity (Polinceusz, 2013: 312). Supervision is an institution that enables authoritative interference in the sphere of activity of the supervised entity when irregularities are detected. The criteria, as well as the supervisory authorities, and the scope of supervision must be clearly specified by the legislators. It cannot be presumed that there is any authoritative interference with the sphere of independence of supervised entities; such interference must be clearly provided for in statutory-grade generally applicable laws. If there is no clear legal basis for initiating the supervisory procedure, it is not permissible.

The concept of inspection is a multidimensional term that applies to all forms of organisation of social life, therefore it can be used in various semantic contexts (Kostrubiec, 2013: 329). The purpose of inspection – as provided for in Article 3 of the Act of 15 July 2011 on Inspection in State Administration (consolidated text, Polish Journal of Laws of 2020, item 224, as amended) – the Act is hereinafter referred to as the 'ACSA' – is to assess the activity of the inspected entity on the basis of established facts, subject to the adopted inspection criteria. Where irregularities are found, the purpose of inspection is also to determine their extent, causes and effects, as well as those responsible, and to formulate recommendations aimed at correcting the irregularities. Inspection can be conducted under an ordinary and simplified procedure. It should be emphasised, however, as provided for in Article 51(1) of the ACSA, that inspection can be ordered in a simplified procedure in cases justified by the nature of the case or urgency of inspection activities.

3 Supervision in the field of cybersecurity

The issues of supervision in the application of the provisions of the NCSA, therefore, in the field of cybersecurity, are set out in Article 53 of the NCSA. This supervision, according to Article 53(1) of the NCSA, is exercised by: 1) the minister competent for computerisation in respect of the fulfilment by the providers of cybersecurity services of the requirements concerning: a) the fulfilment of organisational and technical conditions making it possible to ensure cybersecurity to the served operator of an essential service; b) the possession of premises for the provision of incident response services, protected from physical and environmental threats; c) the application of a safeguard to ensure confidentiality, integrity, availability and authenticity of the processed information, taking into account personal security, operation and architecture of the systems; 2) the competent authorities for cybersecurity with regard to: a) fulfilment by operators of essential services of their obligations under the Act with respect to countering cybersecurity threats and reporting serious incidents; b) compliance by providers of cybersecurity services with the security requirements of their services and performance of their obligations with respect to reporting major incidents; this concerns both the application of appropriate technical and organisational measures, acting on the basis of risk analysis, identifying threats, or proper management of ICT networks and systems.

Pursuant to Article 41 of the NCSA, the competent authorities for cybersecurity, who also exercise supervision, include: 1) for the energy sector – the minister competent for energy; 2) for the transport sector, excluding the water transport sub-sector – the minister competent for transport; 3) for the water transport sub-sector – the minister competent for the maritime economy and the minister competent for inland navigation; 4) for the banking sector and financial markets infrastructure – the Polish Financial Supervision Authority; 5) for the healthcare sector – the minister competent for health; 6) for the healthcare sector and the digital infrastructure sector covering entities subordinated to the Minister of National Defence or supervised by him and enterprises of special economic and defence importance in respect of which the Ministry of National Defence is the authority organising and supervising the performance of tasks for state defence – the Minister of National Defence; 7) for the drinking water supply and distribution sector – the minister competent for water management; 8) for the digital infrastructure sector and digital service providers – the minister competent for computerisation. As a rule, therefore, the supervisory authorities are ministers in charge of a specific department of government administration, only in the case of the banking sector and financial market infrastructure is it the Polish Financial Supervision Authority.

As part of the supervision of operators of essential services, digital service providers and providers of cybersecurity services, pursuant to Article 53(2) of the NCSA: 1) the competent authority for cybersecurity or the minister competent for computerisation exercises inspection on compliance with security requirements and obligations in this respect; 2) the competent authority for cybersecurity imposes fines on operators of essential services and digital service providers. Supervision in the field of cybersecurity

is carried out in two stages: first, inspection is conducted, covering the performance of obligations on countering cybersecurity threats and reporting incidents, as well as meeting requirements to ensure cybersecurity, including the security of digital services provided. Where irregularities are found, the competent authority for cybersecurity may impose a fine on the supervised entity. In the case of a digital service provider, a fine is imposed upon evidence that it fails to comply with the security requirements of the digital services provided or the statutory obligations regarding the reporting of material incidents.

4 Cybersecurity-related inspection

If the inspection concerns an entity that is an entrepreneur, pursuant to Article 48 of 6 March 2018 – the Entrepreneurs Law (consolidated text, Polish Journal of Laws of 2021, item 162, as amended) – the Act is hereinafter referred to as the "EL" – the inspection authority notifies the entrepreneur of its intention to initiate an inspection. The inspection is initiated no sooner than after 7 days and no later than after 30 days from the date of delivery of the notice on the intention to initiate inspection. At the request of the entrepreneur, inspection may be initiated within 7 days from the date of delivery of the notice. If inspection is not initiated within 30 days from the delivery of the notice, the initiation of the inspection requires a new notice. The lack of a notice of inspection undoubtedly has a significant impact on the inspection's outcome. It prevents the entrepreneur from proper preparation for the inspection activities. Nevertheless, since the law stipulates that an effective notice is a necessary condition for conducting inspection, prior to its initiation, the inspecting entity is obliged to have evidence of delivery of a relevant notice to the entrepreneur (judgement of the Voivodeship Administrative Court in Warsaw of 25 October 2017, VI SA/Wa 1122/17, LEX No. 2425534). A notice of the intention to initiate inspection is not issued, among others, in the event when: 1) inspection is to be conducted in accordance with the ratified international agreement or directly applicable provisions of the European Union law; 2) the inspection must be conducted to prevent an crime or petty offence, a fiscal crime or a fiscal petty offence, or to secure the evidence that such offence or crime has been committed; 3) the inspection is justified when there is a direct threat to life, health or the environment; 4) the entrepreneur does not have the address of residence or the registered address, or the delivery of letters to the given addresses was ineffective or difficult.

It does not follow from the regulations that the inspection authority, in explaining the reasons for an inspection without prior notice, is required, at the moment of its initiation, to provide the justification for accepting such a basis for inspection, indicating why such inspection is, for example, essential to prevent the commission of an crime or a petty offence, a fiscal crime or a fiscal petty offence, or to secure the evidence of its commission. In view of these considerations, it seems hardly justified to warn the inspected entity about the evidence that the authority will look for as part of the initiated proceedings. Therefore, the citation of the relevant legal basis should be treated as sufficient (judgement of the Supreme Administrative Court of 28 September 2017, I FSK 1125/17, LEX No. 2404466). The list of exemptions from the obligation to notify about

the inspection indicates that the legislators included it in special cases, related to the protection of particularly socially sensitive goods, where the balance of the entrepreneur's interest related to the possession of information about the planned inspection and the protection of these goods by the inspection authorities speaks in favour of the primacy for the protection and possibly rapid response to threats or pathologies. And it is indisputable here that the inspection authority, within the scope of its competence, may act ex officio and the source from which the authority obtained information about the threat is of no significance (judgement of the Supreme Administrative Court of 29 December 2015, II OSK 1001/14, LEX No. 1999995).

A person conducting inspection related to entities that operate as businesses – as provided for in Article 55 of the NCSA – has the right to: 1) freely enter and move around the premises of the inspected entity without the obligation to obtain a pass; 2) access documents related to the activity of the inspected entity, collect against a receipt and secure documents related to the scope of inspection, while observing the provisions on legally protected secrets; 3) prepare, and if necessary request the preparation of, copies, excerpts or extracts of documents, as well as statements or calculations indispensable for the inspection; 4) process personal data as needed for the achievement of the inspection objective; 5) request to provide oral or written explanations in matters related to the scope of inspection; 6) perform the visual inspection of devices, carriers and information systems. These are the standard inspection powers that make it possible to verify the facts and identify possible irregularities.

Article 56 of the NCSA imposes obligations on inspected entrepreneurs that make it possible to conduct inspections efficiently. Inspected entities that are entrepreneurs provide the inspecting person with the conditions necessary to efficiently conduct the inspection – in particular, by ensuring the immediate presentation of requested documents, providing oral and written explanations in a timely manner in matters covered by the inspection, providing access to the necessary technical equipment, as well as making copies or printouts of documents and information collected on carriers, in devices or in information systems on their own. The inspected entity certifies copies or printouts as true copies of the originals. In the event of refusal to certify consistency with the originals, they are confirmed by the inspecting person, who makes a note about this fact in the inspection report. Without access to documentation or explanations from the entrepreneur, it may prove impossible to conduct the inspection. Therefore, the legislators have imposed an obligation on the inspected entity to immediately present the requested documents, provide oral and written explanations in a timely manner, as well as to make the necessary technical equipment available, or to make copies or printouts of documents. It should be emphasised, however, that all these obligations may not go beyond the scope of the inspection, i.e. the inspection authority may not demand more information than required by the scope of the inspection.

The details of the inspection are documented in a report. Pursuant to Article 58 of the NCSA, the person inspecting entities that are entrepreneurs shall present the details of the

inspection in a inspection report. An inspection report provides: 1) the name or first name and surname and address of the inspected entity; 2) the first name and surname of the person representing the inspected entity and the name of the body representing this entity; 3) the first name and surname, position and authorisation number of the inspecting person; 4) the start and end dates of inspection activities; 5) the subject and scope of the inspection; 6) the facts established in the course of the inspection and other information essential for the conducted inspection, including the scope, reasons and effects of the irregularities found; 7) attachments, if any. This is the basic information that makes it possible to take relevant decisions at a later stage, particularly to identify irregularities and persons responsible for them, especially if it proves necessary to take appropriate punitive measures against the inspected entity.

A inspection report is signed by the inspecting person and the person representing the inspected entity. Prior to signing the report, the inspected entity may, within 7 days from the date of its presentation for signing, make written reservations to the report. If reservations are made, the inspecting person analyses them and, if necessary, takes additional inspection steps. In the event that the reservations are justified, the inspecting person changes or supplements the relevant part of the report in the form of an annex to the report. In the event that the reservations are not accepted in whole or in part, the inspecting person informs the inspected entity in writing. A reservation may not be made after the inspection report has been signed. The inspecting person makes a note on the refusal to sign the report, including the date of such refusal. The report in paper form is drawn up in two copies, one of which is left for the inspected entity, and if the report is drawn up in electronic form, it is delivered to the inspected entity.

Pursuant to Article 51 of the EL, the inspection is conducted in the entrepreneur's registered office or place of business, and during working hours or at the time of the actual performance of business activity by the entrepreneur. Upon the entrepreneur's consent or request, the inspection is conducted in the place where documentation, including tax books, is stored other than the registered office or place of business to facilitate the inspection. With the consent of the entrepreneur, the inspection, or individual inspection activities, may also be conducted in the registered office of the inspection authority to facilitate the inspection. Subject to the entrepreneur's consent, the inspection, or individual inspection activities, may be conducted remotely via a postal operator or by electronic means of communication, if this serves to facilitate the inspection or is justified by the nature of the business activity conducted by the entrepreneur. If, in cases requiring the consent or request of the entrepreneur, the inspection authority undertook inspection activities without such consent or request, the documents and information collected in the course of such activities do not constitute evidence in the inspection proceedings.

Inspection activities should be performed in an efficient manner and in such a way as not to disturb the functioning of the entrepreneur's business. In the event that the entrepreneur indicates in writing that the performed activities significantly interfere with the entrepreneur's business activity, the necessity to undertake such activities shall be

justified in the inspection report. This rule is introduced by Article 54 of the EL. The purpose of the entrepreneur's activity is to conduct business, and the inspection may not lead to the suspension of the business activity – it may limit it, but only to the extent necessary to achieve the objective of the inspection. The inspection may not be excessive, and it should create as little burden for the entrepreneur as possible.

If deficiencies are identified, the inspection authority may issue follow-up recommendations to the inspected entity. Pursuant to Article 50 of the NCSA, if, on the basis of the information contained in the inspection report, the competent authority for cybersecurity or the minister competent for computerisation recognises that there may have been a breach of the provisions of the NCSA by the inspected entity, it will issue follow-up recommendations concerning the removal of irregularities. The follow-up recommendations may not be appealed against. The inspected entity is required, within the prescribed time limit, to inform the competent authority for cybersecurity or the minister competent for computerisation on the manner in which the recommendations have been implemented.

5 Conclusion

Supervision and inspection related to cybersecurtiy (and other areas) is exercised and conducted by the authorities expressly mentioned by the legislators, including in the NCSA. Supervisory and inspection powers may not be presumed due to the onerousness of these measures for the the entities that are supervised and inspected. Specific solutions in this regard are provided in Article 60 of the EL, on the basis of which the executive body of a municipality may take actions aimed at suspending the entrepreneur's business activity, including if it does not meet the conditions provided for ensuring cybersecurity, and, at the same time, leads to qualified threats. Pursuant to this provision, in the event that a threat to life or health, danger of substantial damage to property or a direct threat to the environment is identified as a result of the performance of this activity, the commune head or the mayor of the city must immediately notify the competent authorities – in this case, the competent authorities competent cybersecurity, as set out in the NCSA. The notified authorities shall immediately apprise the commune head or the mayor of the city of the actions taken. Should it be impossible to inform the competent authorities, the commune head or the mayor of the city may order the entrepreneur, by way of a decision, to suspend business activity for a necessary period of time, not longer than three days. The decision ordering the suspension of business activity in the event of a threat to life or health, danger of substantial damage to property or a direct threat to the environment as a result of the performance of such activity is immediately enforceable. The entrepreneur's business activity may be suspended where the entrepreneur fails to comply with their obligations with respect to countering cybersecurity threats and incident reporting and where, at the same time, this has led to a threat to life or health, danger of substantial damage to property or a direct threat to the environment.

The tasks to be completed by the inspection should be specified in terms of the functioning of the entire cybersecurity system. An effective inspection system should contribute to ensuring that the implementation processes run properly and that the best possible results are achieved in each activity. Several elements contribute to the effectiveness of inspection activities. One is the proper selection of the subject matter of the inspection. Professionalism of the inspection is also important. This term should be understood as the due preparation of the inspectors, both substantive and ethical (Nowikowska, 2021: 100). Professionalism is the element of the inspection that is manifested in the substantive and organisational preparation of the inspecting entity, whose employees have sufficient knowledge and experience (Kostrubiec, 2013: 331).

References:

Chałubińska-Jentkiewicz, K., Karpiuk, M. & Kostrubiec, J. (2021) *The Legal Status of Public Entities in the Field of Cybersecurity in Poland* (Maribor: Lex Localis), https://doi.org/10.4335/2021.5.

Karpiuk, M. (2021a) The Local Government's Position in the Polish Cybersecurity System, *Lex Localis – Journal of Local Self-Government*, 3, pp. 609-620, https://doi.org/10.4335/19.3.609-620(2021).

Karpiuk, M. (2021b) The Organisation of the National System of Cybersecurity: Selected Issues, *Studia Iuridica Lublinensia*, 2, pp. 233-244, http://dx.doi.org/10.17951/sil.2021.30.2.233-244.

Kostrubiec, J. (2013) Kontrola administracji publicznej, In: Karpiuk, M. & Kowalski, J. (eds.) *Administracja publiczna i prawo administracyjne w zarysie* (Iuris: Warszawa-Poznań), pp. 329-364.

Nowikowska, M. (2021) Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa, *Cybersecurity and Law*, 1, pp. 77-103.

Polinceusz, M. (2013) Nadzór nad administracją publiczną, In: Karpiuk, M. & Kowalski, J. (eds.) *Administracja publiczna i prawo administracyjne w zarysie* (Iuris: Warszawa-Poznań), pp. 311-327.