Paweł Romaniuk*

The Functional Model of Local Government Units Based on Ensuring the Appropriate Level of Cybersecurity

Abstract

The article characterises the elements of a model for shaping the conditions for the proper functioning of local government units, which is based on ensuring an acceptable level of cybersecurity. In the practice space, there is a correlation between local government units and cyberspace, thus also cybersecurity. The functioning of local government in different environmental conditions involves visible benefits for its actors as well as many potential threats – all the more so, as even larger self-governments, equipped with greater financial and human resources, cannot avoid them. The dangers involved, which are increasing every year, result in a growing number of various incidents, which is a test for local governments in building appropriate security platforms and models.

Key words: local government unit, cyberspace, cybersecurity, public administration, technology, information

* Assoc. Prof. Paweł Romaniuk, PhD, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail pawel.romaniuk@uwm.edu.pl, ORCID: 0000-0002-7217-956X.

Introduction

In recent years, it has become undisputedly evident that the use of information and communication technologies in the day-to-day functioning of local government units is becoming increasingly widespread, which is completely understandable. It is also noticeable that the entities administering public tasks are shifting to the 4.0 economy standards. The observed phenomenon of assimilation of local governments to digitally changing economies is also so widespread that we can already speak openly about local government units' progressive and inevitable digital transformation.

However, this phenomenon entails the need for ICT security, known as cybersecurity. In doing so, it is observed that the number of reported digital incidents and hacking attacks on all public administration offices, including local government units, increases every year. The latter carry an incredibly heavy burden of responsibility and face the need to ensure the security of ICT networks and systems. This is especially important as local governments, performing tasks on behalf of and for their residents, and having access to many electronic databases, must take special care to protect these resources. Therefore, it becomes important to build universal standards for protecting the resources held by them against unauthorised and unlawful use. According to the adopted assumption, verifying the article's objectives justifies stating the need to define a model of functioning of local government units based on planning and ensuring an appropriate level of cybersecurity. At the same time, the indicated proposals are only selected elements shaping the principles of safe functioning of local government units in the area of building cybersecurity.

Legal status of local government units

Local government units are defined from the level of various planes of evaluation, many theories or a variety of existing models, and the local government in Poland has a long tradition. Due to the specificity of the topic of this paper, the public structure in question will be characterised in a very general way. The beginning of local government was observed as early as the period of the first Piasts, where there were rallies whose main role was to perform advisory and judicial tasks. The dynamisation of local government was particularly evident during the development of the estate monarchy. Also, the Constitution of 3 May 1791 spoke of the right of cities, where desiderata were

indicated, giving the residents of cities the right to elect municipal officials. An essential push in shaping the role of local government was Poland's regaining of independence. In the March Constitution of 17 March 1921, local government was regarded as the main form of organisation and state functioning. Along with the development of self-government, there was also a period of decline. This occurred after the Second World War[1]. The re-establishment of the nature and role of local government took place during the Round Table talks, which resulted in the legal formation and definition of the role and place of local government in the Constitution of the Republic of Poland of 2 April 1997[2]. In addition, the organisational structure of public administration, including local government units, the rules it uses, and the procedures it adopts based on the law, make it a primary objective to guarantee the efficiency and effectiveness of the public services it provides[3]. Therefore, local governments must have both the capacity to perform public tasks and the conditions to ensure an acceptable level of security.

The functioning of local government at its three levels is characterised by its common features, which include self-governance, subsidiarity and the scale of the tasks they carry out. The duties of local government units as regards the performance of their tasks are set out by the legislator in three acts on the system of local government units. The first legal act, which defines the municipality as the basic local government unit, is the Act of 8 March 1990 on Municipal Self-Government[4]. The second act, which determines the competencies of the second local government level, is the Act of 5 June 1998 on District Self-Government[5]. The third legal construction, which determines the position of provincial self-government in the system, is the Act of 5 June

1 A. Gołębiowska, P.B. Zientarski, E. Stępień, *Konstytucja Rzeczypospolitej Polskiej a samorząd terytorialny* [in:] *Funkcjonowanie samorządu terytorialnego – uwarunkowanie prawne i społeczne*, eds. A. Gołębiowska, P. B. Zientarski, Warszawa 2016, p. 13–14.

2 See Art. 15, 16 and Chapter VII entitled „Local government" of the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws 1997, no. 78, item 483, as amended), hereinafter referred to as the Polish Constitution.

3 For more information see: A. Gołębiowska, *Geneza oraz konstytucyjno-prawne aspekty samorządu powiatowego i jego koncepcje prawno-organizacyjne* [in:] *Rzeczpospolita w koncepcjach transformacji ustrojowej 1989 r*., ed. eadem, Warszawa 2015, p. 60–74.

4 Art. 7(1) of the Act of 8 March 1990 on Municipal self-government (consolidated text, Journal of Laws 2023, item 40, as amended).

5 Art. 4(1) of the Act of 5 June 1998 on District self-government (consolidated text, Journal of Laws 2022, item 1526, as amended).

1998 on Provincial Self-Government[6]. The principal law, in the provisions of Art. 166(1), explicitly characterises public tasks that serve to satisfy the needs of the local government community. Here, they are performed by the local government unit as its own tasks[7]. Obviously, if the legitimate needs of the state arise in the form of primary acts, the legislator may entrust local government units with other public tasks. Thus, local government units established as a result of the territorial reform of the state, being the effect of decentralisation of public administration, perform the tasks indicated above.

As an effect of the decentralisation of public administration and because of the three-level division of local government, local government units perform the above tasks independently or indirectly. It should be noted here that the designated legal order, which is the foundation of security, built from a complex public system, is regarded universally. Security is therefore identified as the state's ability to ensure full preparedness to respond to and cope with potential dangers. If such dangers materialise, the state must endeavour to eliminate or mitigate the costs and consequences of their emergence in an appropriate manner and using appropriate methods[8]. Under such conditions, economic and legal trends also translate very directly into the functioning of local government administration. The changing contribution of new information technologies to the everyday lives of citizens is also recognised. In addition, the expectations of citizens as to the way local government services are provided are also changing. Consequently, in the standard course of events, local governments tend to increasingly use modern information and communication technologies[9]. It is therefore a fundamental task for local government units to protect the resources they have and, in the event of an „attack" on these resources, to respond appropriately. By way of example, in 2021 alone, CERT Polska recorded as many as 525 incidents in local government units[10].

6 Art. 14(1) of the Act of 5 June 1998 on Provincial self-government (consolidated text, Journal of Laws of 2022, item 2094, as amended).

7 See Art. 166(1) of the Polish Constitution.

8 Cf. R. Gwardyński, *Racjonalizacja działań Policji na poziomie lokalnym* [in:] *Racjonalizacja zarządzania jednolitymi formacjami umundurowanymi odpowiedzialnymi za bezpieczeństwo wewnętrzne*, eds. B. Wiśniewski, P. Lubiewski, T. Zwęgliński, Warszawa 2020, p. 119–121.

9 E.M. Włodyka, *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, „Cybersecurity and Law" 2022, no. 1, p. 205–208.

10 The CERT Polska team operates within the structures of NASK, which is a state-owned research institute that conducts scientific activities, a national register of domains and also provides advanced ICT services.

Local government units in the sphere of security

Within the scope of their statutory competencies, local government units carry out tasks in the field of information security management. An important area assigned to local government administration is meeting collective social needs. These take the form of telecommunications activities. From this point of view, local government units are entitled to perform the following tasks, which are part of the segment of telecommunication competencies. These include in particular:

– construction or operation of a public telecommunications network or telecommunications infrastructure, and the acquisition of rights of access to telecommunications infrastructure and telecommunications networks;

– delivery of telecommunications networks and the ability to provide access to telecommunications infrastructure;

– services, which consist of the use of the owned telecommunications infrastructure and telecommunications networks, as well as offering services in favour of telecommunications undertakings, state organisational units and certain state legal entities and end-users, which may include entities using a publicly available telecommunications service or requesting the provision of such a service to satisfy their own needs[11].

At the same time, it should be borne in mind that, pursuant to Art. 3(6) of the Act on supporting the development of telecommunications services and networks, information on the commencement of the aforementioned activity by a given local government unit shall be announced, both on the website of the Public Information Bulletin and in the registered office of the specific unit. Such information shall be forwarded in electronic form to the President of the Office of Electronic Communications, who in turn shall promptly announce such information in the Public Information Bulletin on the website of the Office of Electronic Communications.

The duty of each public administration body is, in particular, to provide public services, ensuring their high level. Many public services provided by local government units are carried out using new IT technologies via the Internet. This type of activity is also connected with the necessity to

11 See Art. 3(1) of the Act of 7 May 2010 on support for the development of telecommunications services and networks (consolidated text, Journal of Laws 2023, item 733, as amended).

guarantee the security of the data contained in IT systems[12]. Therefore, the public tasks performed by local government units, both their own tasks and those entrusted to them, are often related to the obligation to process the personal data of their residents. The local government is legally and formally obliged to take special care of the data in its possession. A major role is attributed to employees working in local government units. Such employees, with appropriate professional qualifications adequate to various threats, must constantly improve their expertise, particularly in the area of cybersecurity, strengthening their awareness of potential threats that may arise at any time[13].

The administration of personal data shall entail any activity that involves the collection, organisation, recording, monitoring, transfer or deletion of such data[14]. Such responsible data processing is carried out according to several key principles. These include, in particular:

– the principle of integrity and confidentiality, where personal data should be processed in such a way as to guarantee their security, including protection against unauthorised or unlawful processing and accidental loss, destruction or mechanical damage;

– the principle of applying appropriate technical means that use modern IT tools together with their software[15].

The security controller or the entity that manages such data is obliged to mitigate the possible risk of a data breach. An extremely important action is to take immediate follow-up measures when an incident involving a data breach occurs. However, after a personal data breach has already materialised, the GDPR determines, in Art. 24, the obligations for the controller, namely:

– putting in place procedures to ensure that the risk of a breach of individuals' rights and freedoms is identified;

12 A. Chodakowska, S. Kańduła, J. Przybylska, *Jak polskie gminy radzą sobie z cyberbezpieczeństwem – wyniki badań własnych*, „Kontrola Państwowa" 2022, no. 1, p 131.

13 M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1, p. 48.

14 Cf. M. Magdziarczyk, *Wdrożenie i realizacja przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE przez jednostki samorządu terytorialnego – na przykładzie gminy*, „Samorząd Terytorialny 2021, no. 4, p. 72–74.

15 For more information see: 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), hereinafter referred to as the GDPR.

– reporting the incident to the supervisory authority and notifying data subjects of the breach;
– keeping records of incidents;
– taking measures to mitigate the effects of the breach[16].

Universal conditions for shaping and developing cybersecurity in local government units

In trying to define a model of functioning of local government units, based on ensuring the appropriate level of cybersecurity, it is essential to point to the role of the Act of 5 July 2018 on the National Cybersecurity System (ANCS) in terms of building a cybersecurity platform[17]. Pursuant to Art. 2(4) of the ANCS, cybersecurity means the protection of information systems against action that compromises the confidentiality, integrity, availability and authenticity of the data processed or of the related services offered by those systems[18]. The above-mentioned obligations, imposed on the operator of an essential service in each local government unit, compel the implementation of a security management system to assist in providing the essential service. These measures focus in particular on:
– conducting successive risk management in the area of incidents;
– implementing adequate technical measures in risk management;
– collecting, managing and analysing information on cybersecurity risks and potential vulnerabilities of information systems;
– implementing procedures to prevent the possibility of incidents affecting the security level of information and information systems;
– using communication means to ensure secure and authorised communication within the national cybersecurity system[19].

Local government units, as an important part of public administration, have become a subject of the national cybersecurity system. The legislator has delegated many of the responsibilities in this area to units of the public finance sector, including local government administration, where local government units become, next to central authorities, co-creators of the

16 Cf. ibidem, Art. 24.
17 See the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Journal of Laws 2023, item 913, as amended), hereinafter referred to as the ANCS.
18 Ibidem, Art. 2(4).
19 For more information see: ibidem, Art. 8.

state's cybersecurity policy, which is extremely important for the state's security[20]. The responsibilities of public entities and local administration related to cybersecurity are indicated in Chapter 5 of the above-mentioned Act. Therefore, it becomes an extremely important task to designate a person responsible for maintaining permanent contact with the entities of the national cybersecurity system[21]. A local government unit may appoint one person responsible for maintaining contact with the entities of the national cybersecurity system concerning the public tasks dependent on information systems carried out by its organisational units[22]. Given the need for the correct response, the local government unit that carries out a public task dependent on the information system must, inter alia:

– ensure incident management in the public entity;

– report the incident in the public entity immediately, no later than within 24 hours from detection, to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV;

– ensure the handling of the incident in the public entity and the critical incident in cooperation with the relevant CSIRT MON, CSIRT NASK or CSIRT GOV, providing the necessary data, including personal data;

– ensure that the persons for whom the public task is carried out have access to knowledge, allowing them to understand the essence of cybersecurity and to apply effective protection mechanisms[23].

It must be noted that local government units need to have appropriate personnel structures and procedures in place to ensure adequate response to the emergence of incidents (events) that may adversely affect cybersecurity. Within the framework of the adopted solutions, the local government must therefore guarantee the skilful management of incidents regarding information security. This is the ability to ensure the handling of incidents, seeking integration between them, removing the causes of such threats, and developing conclusions and recommendations to eliminate the appearance of such threats in the future. It is important that, as soon as an incident occurs and is identified, the situation is reported to the relevant body in order to implement countermeasures, and also that the responsibilities of the key

20 M. Karpiuk, *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, vol. 19, no. 3, p. 613.

21 Cf. idem, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2, p. 59.

22 Art. 21(1) and (3) of the ANCS.

23 For more information see: ibidem, Art. 22(1) (1–5).

service operators adopted in a given unit are deployed[24]. It should also be ensured that the incident is handled in cooperation with the Data Protection Officer, whose task is to inform the controller and its employees of the obligations arising from the GDPR and other legal regulations, as well as to monitor compliance with personal data protection regulations on an ongoing basis and to raise awareness of the related potential threats.

Ensuring the appropriate and acceptable state of security in local government units also correlates with the obligation to guarantee the often changing and supervised essence of its obvious conversion. This modification consists of an action where the adequate level of security in local government administration is related to natural changes occurring due to various factors. A specific transfiguration can be a situation where social attitudes towards security are changing, where there are legal changes directly affecting all actors involved in building cybersecurity[25]. Also, various social interactions contribute to ensuring an acceptable level of security. Security culture, which forms the organisational culture of local government units, sets out the attitude of a given organisation towards potential risks, threats and concerns, and indicates the formal way in which the unit is secured against threats in the sphere of computer and information resources. Each municipality, district or province, taking into account the area of cyberspace which develops every year, must put effort into building an appropriate platform for securing its resources and data. This approach is particularly indicative of the responsibility of the managers for the data administration process. This is all the more important as operations in virtual space, characterised by the peculiar cultural behaviour of its participants, require constant concentration and awareness of the efforts made in this regard in the area of building safeguards for resources. Therefore, it is worth pointing out that the phenomenon of ensuring the appropriate level of security in local government units in terms of the operation of ICT networks creates conditions that do not necessarily have to be present in the world outside cyberspace[26].

24 K. Świtała, *Obowiązki operatorów usług kluczowych* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019, p. 117–123.

25 J. Szmyd, *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna* [in:] *Zarządzanie bezpieczeństwem*, ed. P. Tyrała, Kraków 2000, p. 165–168.

26 For more information see K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, no. 2, p. 13–14.

Conclusions

As Poland enters the era of the information society, local government units must also adapt the scope of their public services to the requirements of the 21st century and to the assumptions that are based on electronic communication. This also entails the necessity for such entities to ensure the protection of the resources and diverse data they possess and administer, which are aggregated in a digital version. There are growing expectations of citizens towards local governments, not only in terms of improvements in the functioning of e-administration. Public expectations encompass a guarantee that all widely collected and aggregated information and data will also be appropriately secured against cyberattacks and unauthorised access.

It therefore becomes essential to formulate a model for the functioning of local government units, the role of which will be to guarantee the appropriate level of cybersecurity. In this respect, each local government unit becomes responsible for taking all measures in terms of actions to prevent the occurrence of critical incidents in the area of cybersecurity. However, in this segment, it also becomes important to provide adequate infrastructural and educational support at the level of central authorities, the private sector or the non-governmental sector for the secure functioning and development of local government units in cyberspace.

Bibliography

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, no. 2.

Chodakowska A., Kańduła S., Przybylska J., *Jak polskie gminy radzą sobie z cyberbezpieczeństwem – wyniki badań własnych*, „Kontrola Państwowa" 2022, no. 1.

Gołębiowska A., *Geneza oraz konstytucyjno-prawne aspekty samorządu powiatowego i jego koncepcje prawno-organizacyjne* [in:] *Rzeczpospolita w koncepcjach transformacji ustrojowej 1989 r.*, ed. A. Gołębiowska, Warszawa 2015.

Gołębiowska A., Zientarski P.B., Stępień E., *Konstytucja Rzeczypospolitej Polskiej a samorząd terytorialny* [in:] *Funkcjonowanie samorządu terytorialnego – uwarunkowanie prawne i społeczne*, eds. A. Gołębiowska, P. B. Zientarski, Warszawa 2016.

Gwardyński R., *Racjonalizacja działań Policji na poziomie lokalnym* [in:] *Racjonalizacja zarządzania jednolitymi formacjami umundurowanymi odpowiedzialnymi za bezpieczeństwo wewnętrzne*, eds. B. Wiśniewski, P. Lubiewski, T. Zwęgliński, Warszawa 2020.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.

Karpiuk M., *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, vol. 19, no. 3.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.

Magdziarczyk M., *Wdrożenie i realizacja przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE przez jednostki samorządu terytorialnego – na przykładzie gminy*, „Samorząd Terytorialny" 2021, no. 4.

Szmyd J., *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna* [in:] *Zarządzanie bezpieczeństwem*, ed. P. Tyrała, Kraków 2000.

Świtała K., *Obowiązki operatorów usług kluczowych* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019.

Włodyka M., *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, „Cybersecurity and Law" 2022, nr 1.

Model funkcjonowania jednostek samorządu terytorialnego oparty na zapewnieniu właściwego poziomu cyberbezpieczeństwa

Streszczenie

Autor artykułu charakteryzuje elementy modelu kształtowania warunków do prawidłowego funkcjonowania jednostek samorządu terytorialnego opartego na zagwarantowaniu akceptowalnego poziomu cyberbezpieczeństwa. W przestrzeni praktycznej istnieje korelacja między jednostkami samorządu terytorialnego a cyberprzestrzenią i tym samym cyberbezpieczeństwem. Funkcjonowanie samorządu terytorialnego w różnych warunkach środowiskowych wiąże się nie tylko z widocznymi korzyściami dla jej podmiotów, lecz także z wieloma potencjalnymi zagrożeniami, tym bardziej że nie udaje się ich uniknąć nawet większym samorządom, mającym większe zasoby finansowe i kadrowe. Rosnące z każdym rokiem niebezpieczeństwa z tym związane skutkują pojawieniem się większej liczby różnorodnych incydentów, co stanowi sprawdzian dla samorządów terytorialnych w budowaniu odpowiednich platform i modeli zabezpieczeń.

Słowa kluczowe: jednostka samorządu terytorialnego, cyberprzestrzeń, cyberbezpieczeństwo, administracja publiczna, technologia, informacja