Małgorzata Czuryk*

# Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity

**Abstract**

Local and regional governments play a special role in public life. They perform, on their own behalf and responsibility, certain tasks commissioned by the State by way of legal Acts. The objective of the local and regional governments' existence is to meet the collective requirements of their respective communities. Meeting the needs of residents also requires activities in the field of telecommunications, including support for the development of telecommunications services and networks. However, such development must be monitored. The role of local and regional governments, on the one hand, is to support this development, and, on the other, to protect the users of telecommunications services and networks from threats. Cybersecurity must therefore occupy the right place in the catalogue of local and regional governments' tasks; it cannot be marginalised, as cyberthreats are real, and can result in substantial damage that is not only virtual.

Key words: telecommunications services, telecommunications networks, cybersecurity, local and regional government, telecommunications infrastructure, the Internet

* Dr hab. Małgorzata Czuryk, Professor of the University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: malgorzata.czuryk@uwm.edu.pl, ORCID: 0000-0003-0362-3791.

## Introduction

Local and regional governments are established in order to carry out public tasks at the local and regional levels. Depending on the type of public activities carried out by a body, they are referred to as local or regional governments. Despite the fact that all local and regional government bodies are entrusted with powers to perform tasks related to telecommunications, their impact on the development of telecommunications services and networks varies. This does not result solely from the authority vested in communes, districts, and provinces, but also from the financial resources of the respective entities and their policies, including the priorities and objectives of local and regional government bodies.

Local and regional governments, as separate legal entities, are forms of decentralisation[1]; when performing activities in the field of telecommunications, they must recognise the potential threats, and they are obligated to ensure security in cyberspace. Cybersecurity is particularly important in the context of supporting the development of telecommunications services and networks. Local and regional government bodies must remember that the dynamism of this development must not result in relaxing the protection of cyberspace against threats. Both these elements must evolve simultaneously - i.e. the development of telecommunications services and networks should enforce the application of new, more effective mechanisms of protection against cyberthreats, and improvements to the existing measures.

Local and regional governments participate in exercising public authority, and perform an essential part of the public tasks assigned to them on their own behalf and responsibility[2], i.e., they have been granted the authority to perform the entrusted tasks[3]. Supporting the development of telecommunications services and networks also belongs to the tasks of local and regional government; however, it should be remembered that this development must be monitored and protected from threats.

**1** M. Karpiuk, *Samorząd terytorialny a państwo. Prawne instrumenty nadzoru nad samorządem gminnym*, Lublin 2008, s. 58.
**2** M. Karpiuk, J. Kostrubiec, *Rechtsstatus der territorialenSelbstverwaltung in Polen*, Olsztyn 2017, s. 191.
**3** M. Karpiuk, *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014, s. 15.

## Local and regional government activities in the fields of telecommunications and cybersecurity

The legislators have authorised the respective local and regional government bodies to carry out activities in the field of telecommunications, provided that their goal is to meet the collective needs of the local or regional governments' communities, depending on the level of the local or regional government. The telecommunications activities of local and regional governments cannot be carried out without regard for the necessity to simultaneously care for network security. Cybersecurity must be taken into consideration by local and regional government bodies when performing activities related to telecommunications, and must form part of the policy of supporting the development of telecommunications services and networks.

Cybersecurity is a notion relating to the provision of security and counteracting threats referring to cyberspace, as well as to functioning in cyberspace, which concerns both the public and private sectors, and their mutual relationships[4]. Cyberspace is becoming not only the space where people work, learn, communicate with each other, and seek entertainment, but also has become a space where people are exposed to various threats[5]. Cybersecurity is not limited to information security, as the latter is only one of the elements of cybersecurity[6].

**4** K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019, s. 21.

**5** A. Pieczywok, *Cyber threats and challenges targeting man versus his education*, „Cybersecurity and Law" 2019, nr 1, s. 227.

**6** K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność…*, s. 20. More on information security and information protection: P. Zając, *Classified Information and its Protection in Polish Armed Forces. General Assumptions*, „Teka Komisji Prawniczej. Oddział PAN w Lublinie" 2017, t. X; M. Karpiuk, *Odmowa wydania poświadczenia bezpieczeństwa przez polskie służby ochrony państwa*, „Secretum" 2015, nr 2; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015; M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014; M. Karpiuk, *Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2018, nr 1; M. Czuryk, *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017; M. Karpiuk, *Cyfrowe transmisje radiofoniczne i telewizyjne i ich wpływ na bezpieczeństwo informacyjne* [w:] I. Oleksiewicz, M. Polinceusz, M. Pomykała (red.), *Nowoczesne technologie – źródło zagrożeń i narzędzie ochrony bezpieczeństwa*, Rzeszów 2014; M. Karpiuk, K. Chałubińska-Jentkiewicz, *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015; M. Czuryk, *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.

The legislators define cybersecurity as the immunity of information systems to violations of the integrity, availability, and authenticity of the processed data or related services afforded by these systems[7]. Cybersecurity is a specialised aspect of security[8] which includes the protection of information systems against threats.

Local and regional governments are part of the national cybersecurity system, whose objective, according to Article 3 of the Act on the national cybersecurity system (u.k.s.c.), is to ensure cybersecurity at the national level, including undisturbed provision of key services and digital services through

**7** rt. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 ze zm.), hereinafter u.k.s.c.

**8** More on security: M. Karpiuk, *Safety as a legally protected value*, „Zeszyty Naukowe KUL" 2019, nr 3; M. Czuryk, J. Kostrubiec, *The legal status of local self-government in the field of public security*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2019, nr 1; M. Karpiuk, *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, nr 2; M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016; M. Karpiuk, K. Prokop, P. Sobczyk, *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017; M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3; M. Karpiuk, *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013; W. Kitler, M. Czuryk, M. Karpiuk (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013; M. Karpiuk, *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia IuridicaLublinensia" 2017, nr 4; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9; M. Karpiuk, N. Szczęch, *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017; M. Bożek, M. Karpiuk, J. Kostrubiec, K. Walczuk, *Zasady ustroju politycznego państwa*, Poznań 2012; M. Karpiuk, *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, nr 3; M. Karpiuk, *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2, M. Karpiuk, *Tereny zamknięte ze względu na obronność i bezpieczeństwo państwa ustanawiane przez organy administracji rządowej*, „Ius Novum" 2016, nr 4; M. Karpiuk, J. Kostrubiec, *The VoivodeshipGovernor's Role in HealthSafety*, „Studia IuridicaLublinensia" 2018, nr 2; M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Prawo zarządzania kryzysowego. Zarys systemu*, Olsztyn 2016; M. Karpiuk, *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019; J. Kostrubiec, *Status of a VoivodshipGovernor as an Authority Responsible for the Matters of Security and Public Order*, „Barometr Regionalny" 2018, nr 5; M. Karpiuk, *Służba funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego oraz żołnierzy zawodowych wyznaczonych na stanowiska służbowe w tych formacjach*, Olsztyn 2017; K. Chałubińska-Jentkiewicz, M. Karpiuk, K. Zalasińska, *Prawo bezpieczeństwa kulturowego*, Siedlce 2016; M. Karpiuk, *Pomoc Sił Zbrojnych Rzeczypospolitej Polskiej udzielana Policji*, „Wojskowy Przegląd Prawniczy" 2018, nr 1; M. Karpiuk, *Position of the LocalGovernment of Commune Level in the Space of Security and Public Order*, „Studia IuridicaLublinensia" 2019, nr 2; M. Karpiuk, *Position of County Government in the Security Space*, „Internal Security" 2019, nr 1.

achieving the appropriate security level of information systems intended for the provision of these services and managing incidents. The objective of the national cybersecurity system, including the bodies creating the system, will thus be to protect the provision of key services and digital services so that they can be delivered without disruptions.

## The range and rules of operation of local and regional government bodies in the field of telecommunications

The legislators clearly state that a local or regional government body may perform the following activities in order to meet the collective needs of local or regional government communities: 1) build or use telecommunications infrastructure and networks and acquire the rights to telecommunications infrastructure and networks; 2) provide telecommunications networks or access to telecommunications infrastructure; 3) provide, with the use of the available telecommunications infrastructure and networks, services to: a) telecommunications companies, b) authorised entities, c) end users[9]. Article 3 section 1 of the Act on supporting the development of telecommunications services and networks (u.w.r.) specifies the major types of local and regional government tasks in the telecommunications sector, which can be carried out directly by the given local or regional government body. Thus, it can build telecommunications infrastructure and networks, provide them to businesses and other administrators, i.e. supply wholesale telecommunications services. The provision also facilitates direct activities in the field of telecommunication services provision for end users[10]. A local or regional government unit may not only build or operate telecommunications infrastructure and networks, but also acquire rights to telecommunications infrastructure and networks, and it may also provide services to external entities, deliver telecommunications networks, or provide access to telecommunications infrastructure. The competences of local and regional government in the field of telecommunications are therefore quite broad, which creates extensive possibilities for supporting the development of telecommunications services and networks, taking into consideration the provision of security in cyberspace.

**9** Art. 3 ust. 1 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (t.j. Dz.U. z 2019 r., poz. 2410 ze zm.), hereinafter u.w.r.
**10** Wyrok NSA z dnia 18 września 2018 r., II FSK 2423, LEX nr 2601705.

Despite the fact that the legislators allow local and regional government bodies to construct telecommunications infrastructure and networks, such activities cannot be performed if in a given area: 1) telecommunications infrastructure and networks do not exist; 2) existing telecommunications infrastructure and networks are not available or do not meet the needs of the local or regional government body. These conditions are introduced by Article 3 section 1a of u.w.r. A local or regional government body may perform such public utility tasks only if in the area of a given commune, district, or province (depending on where the local or regional government body intends to perform activities related to the construction of telecommunications infrastructure and networks) there are no telecommunications infrastructure or networks, and, if they exist, they are inaccessible or do not meet the needs of the local or regional government body. The prerequisite according to which the construction of the telecommunications infrastructure and networks exist but do not meet the needs of the local or regional government body is not a clear-cut one. It is associated with the objectives of local and regional government related to the computerisation of a given area. However, computerisation must take into consideration threats present in cyberspace, so it must simultaneously adopt protective solutions.

Activities in the field of construction, or the operation of or acquiring rights to, telecommunications infrastructure and networks, and delivering telecommunications networks or providing access to telecommunications infrastructure, as well as the provision of services to other entities with the use of the available telecommunications infrastructure and networks according to Article 3 section 2 of u.w.r., should be performed in a way ensuring compatibility and connectivity with other telecommunications networks created by public bodies, or financed from public funds and guaranteeing telecommunications companies, on an equal treatment basis, the possibility of the joint use of telecommunications infrastructure and networks and access to them, in a transparent manner, not interfering with the development of equal and effective competition on telecommunications markets. Such public utility activities must not interfere with the competitiveness framework, i.e. must not lead to violations of market principles, violations in which local

and regional government would be in a privileged position in relation to telecommunications companies[11].

Local and regional governments' undertaking activities in the field of telecommunications must not violate regulations involving State aid. Any aid provided by an EU Member State, or with the use of national resources in any form, which disrupts or threatens to disrupt competition by favouring certain companies or the production of certain goods, is non-compliant with the EU internal market to an extent to which it impacts on trade between EU Member States. The following types of aid are considered compliant with the internal market: 1) aid designed to support the economic development of regions in which living standards are abnormally low or regions with a substantial level of underemployment, taking into consideration their structural, economic, and social situations; 2) aid intended for supporting the implementation of crucial projects of common interest in the EU or aimed at remedying major disturbances in an EU Member State's economy; 3) aid designed to facilitate the development of certain economic activities, or certain economic regions, as long as it does not precipitate a change in trade conditions contrary to the common interest; 4) aid intended for supporting culture and preserving cultural heritage, as long as it does not result in a change to trade conditions and competition in the EU contrary to the common interest[12]. The definition of State aid is broad, and includes an unlimited number of State support measures for enterprises. The definition of aid does not cover general funds which do not favour specific companies or entire sectors of the economy. Such funds can impact on trade between Member States; however, they do not constitute State aid[13].

The activities of local and regional governments may consist of the provision of Internet access services through publicly available Internet access points free of charge, or for a fee lower than the market price. In such cases, as stipulated in Article 3 section 7a of u.w.r., information on commencing such activities published in the Public Information Bulletin should include, i.a., the

**11** M. Karpiuk, *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, nr 1, s. 40.

**12** Art. 107 Traktatu o funkcjonowaniu Unii Europejskiej (Dz.U. z 2004 r. nr 90, poz. 864/2 ze zm.).

**13** B. Kurcz, *Komentarz do art. 107* [w:] K. Kowalik-Bańczyk, M. Szwarc-Kuczer, A. Wróbel (red.), *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, t. II, LEX 2012.

location of publicly available Internet access points and the identification of the area where the service is provided through these points.

A local or regional government may provide Internet access services through publicly available Internet access points without collecting any charges, or for a fee lower than the market price, which stems directly from Article 7 section 1a of u.w.r. The minimum bandwidth for Internet access services provided by local and regional governments through publicly available Internet access points free of charge, or for a fee lower than the market price, is 30 Mb/s[14].

The executive body of a local or regional government, pursuant to Article 3a of u.w.r., may provide entities not included in the public finance sector and not conducting business activities with a designated subsidy from the local or regional government's budget for financing or co-financing the costs of projects associated with meeting the needs of these entities related to access to a fast telecommunications network at the end user's location. The rules for the provision of such a designated subsidy, in particular the selection criteria for a project for financing or co-financing, and the procedure for granting such a subsidy and the manner of settling it, are specified by the governing body of the local or regional government entity by way of a resolution. The subsidy is provided on the basis of an agreement concluded by a local or regional government entity. The agreement should contain: 1) a detailed description of the task, including the purpose for which the subsidy was granted, and the date of its completion; 2) the amount of subsidy provided to the entity performing the task, and the payment method; 3) the time limit for using the subsidy, up to 31 December of a given budget year; 4) the procedure for controlling the performance of the task; 5) the date and settlement method of the subsidy; 6) the date for returning the unused part of the subsidy[15].

A local or regional government entity, pursuant to Article 4 of u.w.r., before commencing activities in the field of the construction or operation of, or acquiring rights to, telecommunications infrastructure and networks, or delivering telecommunications networks or providing access to telecommunications infrastructure, as well as the provision of services to other entities with the

**14** § 1 rozporządzenia Ministra Cyfryzacji z dnia 18 października 2018 r. w sprawie minimalnej przepływności łącza dla świadczonej przez jednostki samorządu terytorialnego usługi dostępu do Internetu (Dz.U. z 2018 r., poz. 2087).

**15** Art. 221 ust. 3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2019 r., poz. 869 ze zm.).

available telecommunications infrastructure and networks, may apply to the President of the Office of Electronic Communications with a request for an assessment of the performance of these activities. The initiative of the local and regional governments in this respect is of a preventive nature, and makes it possible to avoid certain future problems as to the planned activities.

Pursuant to Article 8 of u.w.r., a local or regional government entity entrusting a telecommunications company with the performance of activities resulting from Article 3 section 1of u.w.r., in the event of the economic conditions' not enabling the company to perform financially profitable telecommunications activities in a given area, may: 1) provide a telecommunications company with telecommunications infrastructure or networks in return for charges lower than production cost; 2) co-finance the costs related to the provision telecommunications services to end users or telecommunications companies for the purpose of the provision of such services. A local or regional government entity entrusting a telecommunications company with the constructed telecommunications infrastructure or networks does not constitute a business activity[16]. The preferences arising from Article 8 of u.w.r. may apply only when conducting financially profitable business activity is not possible, as otherwise the competitiveness on the telecommunications market could be disrupted[17].

Article 8 of u.w.r. contains the rule that local and regional government entities shall not provide telecommunications infrastructure or network in return for charges below production cost, and shall not finance activities consisting of the provision of services to end users, except for situations in which, due to economic conditions, it is impossible to conduct financially profitable activities in a given field, and, with regard to financing, this must only entail the provision of telecommunications services to end users or the provision of services to telecommunications companies for the purposes of providing these services to end users[18].

Pursuant to Article 15 of u.w.r. local and regional government entities may carry out activities aimed at stimulating or aggregating users' demand for services associated with broadband Internet access[19], especially

**16** Wyrok NSA z dnia 13 stycznia 2017 r., II FSK 2818/16, LEX nr 2227004.
**17** M. Karpiuk, *Activities…*, s. 43.
**18** Wyrok NSA z dnia 18 września 2018 r., II FSK 2423/16, LEX nr 2601705.
**19** Internet access is considered broadband if the efficiency of the connection is not a factor limiting the possibility of launching applications available online, as per Art. 2 ust. 1 pkt 1 u.w.r.

educational and training services, consisting of providing consumers with telecommunications end devices or computer equipment, or funding telecommunications services for consumers. The governing body of a local or regional government entity specifies by way of a resolution the conditions and funding methods of such activities, in particular the conditions for qualifying the beneficiaries of the aid granted. The above-mentioned activities should be carried out in a non-discriminatory manner, in accordance with transparency and proportionality principles, and aim at maintaining technological neutrality. Each undertaking of a local or regional government entity carried out within the aforementioned activities requires a prior announcement, with a description, in a Public Information Bulletin on the website of the given local or regional government entity, and in its registered office. Local and regional government's efforts to increase residents' interest in broad access to the Internet, and ensuring such access, stimulates the activity of the community and contributes to the development of a given area.

Activities aimed at stimulating or aggregating user demand for services related to broadband Internet access cannot marginalise threats existing in cyberspace. A major role here is played by educational and training initiatives. The users of services associated with broadband Internet access must be aware of the mechanisms conducive to ensuring cybersecurity, i.e. protection from online threats. Local and regional governments have important tasks to perform in this regard as entities supporting the development of telecommunications services and networks.

## Bibliography

### Literature

Bożek M., Czuryk M., Karpiuk M., Kostrubiec J., *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014.

Bożek M., Karpiuk M., Kostrubiec J., Walczuk K., *Zasady ustroju politycznego państwa*, Poznań 2012.

Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2019.

Chałubińska-Jentkiewicz K., Karpiuk M., *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.

Chałubińska-Jentkiewicz K., Karpiuk M., Zalasińska K., *Prawo bezpieczeństwa kulturowego*, Siedlce 2016.

Czuryk M., *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, nr 3.

Czuryk M., *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015.

Czuryk M., *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017.

Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016.
Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Prawo zarządzania kryzysowego. Zarys systemu*, Olsztyn 2016.
Czuryk M., Kostrubiec J., *The legal status of local self-government in the field of public security*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2019, nr 1.
Karpiuk M., *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, nr 1.
Karpiuk M., *Cyfrowe transmisje radiofoniczne i telewizyjne i ich wpływ na bezpieczeństwo informacyjne* [w:] I. Oleksiewicz, M. Polinceusz, M. Pomykała (red.), *Nowoczesne technologie – źródło zagrożeń i narzędzie ochrony bezpieczeństwa*, Rzeszów 2014.
Karpiuk M., *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, nr 4.
Karpiuk M., *Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2018, nr 1.
Karpiuk M., *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014.
Karpiuk M., *Odmowa wydania poświadczenia bezpieczeństwa przez polskie służby ochrony państwa*, „Secretum" 2015, nr 2.
Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, t. 9.
Karpiuk M., *Pomoc Sił Zbrojnych Rzeczypospolitej Polskiej udzielana Policji*, „Wojskowy Przegląd Prawniczy" 2018, nr 1.
Karpiuk M., *Position of County Government in the Security Space*, „Internal Security" 2019, nr 1.
Karpiuk M., *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, nr 2.
Karpiuk M., *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, nr 3.
Karpiuk M., *Safety as a legally protected value*, „Zeszyty Naukowe KUL" 2019, nr 3.
Karpiuk M., *Samorząd terytorialny a państwo. Prawne instrumenty nadzoru nad samorządem gminnym*, Lublin 2008.
Karpiuk M., *Służba funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego oraz żołnierzy zawodowych wyznaczonych na stanowiska służbowe w tych formacjach*, Olsztyn 2017.
Karpiuk M., *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019.
Karpiuk M., *Tereny zamknięte ze względu na obronność i bezpieczeństwo państwa ustanawiane przez organy administracji rządowej*, „Ius Novum" 2016, nr 4.
Karpiuk M., *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, nr 2.
Karpiuk M., *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, nr 2.
Karpiuk M., *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013.
Karpiuk M., Chałubińska-Jentkiewicz K., *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015.
Karpiuk M., Kostrubiec J., *Rechtsstatus der territorialen Selbstverwaltung in Polen*, Olsztyn 2017.
Karpiuk M., Kostrubiec J., *The Voivodeship Governor's Role in Health Safety*, „Studia Iuridica Lublinensia" 2018, nr 2.
Karpiuk M., Prokop K., Sobczyk P., *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017.
Karpiuk M., Szczęch N., *Bezpieczeństwo narodowe i międzynarodowe*, Olsztyn 2017.

Kitler W., Czuryk M., Karpiuk M. (red.), *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, Warszawa 2013.
Kostrubiec J., *Status of a Voivodship Governor as an Authority Responsible for the Matters of Security and Public Order*, „Barometr Regionalny" 2018, nr 5.
Pieczywok A., *Cyber threats and challenges targeting man versus his education*, „Cybersecurity and Law" 2019, nr 1.
Zając P., *Classified Information and its Protection in Polish Armed Forces. General Assumptions*, „Teka Komisji Prawniczej. Oddział PAN w Lublinie" 2017, t. X.

**Legal Acts**

Traktat o funkcjonowaniu Unii Europejskiej (Dz.U. z 2004 r. nr 90, poz. 864/2 ze zm.)
Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2019 r., poz. 869 ze zm.).
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 ze zm.).
Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (t.j. Dz.U. z 2019 r., poz. 2410 ze zm.).
Rozporządzenie Ministra Cyfryzacji z dnia 18 października 2018 r. w sprawie minimalnej przepływności łącza dla świadczonej przez jednostki samorządu terytorialnego usługi dostępu do internetu (Dz.U. z 2018 r., poz. 2087).

**Rulings**

Wyrok NSA z dnia 13 stycznia 2017 r., II FSK 2818/16, LEX nr 2227004.
Wyrok NSA z dnia 18 września 2018 r., II FSK 2423, LEX nr 2601705.
Wyrok NSA z dnia 18 września 2018 r., II FSK 2423/16, LEX nr 2601705.

## Wspieranie rozwoju usług i sieci telekomunikacyjnych przez samorząd terytorialny a cyberbezpieczeństwo

**Streszczenie**

Szczególne miejsce w życiu publicznym zajmuje samorząd terytorialny. Wykonuje on we własnym imieniu i na swoją odpowiedzialność część zadań powierzonych przez państwo w drodze ustawy. Zaspokajanie zbiorowych potrzeb lokalnej lub regionalnej wspólnoty jest celem istnienia samorządu terytorialnego. Zaspokajanie potrzeb mieszkańców wymaga również działań w dziedzinie telekomunikacji, w tym wspierania rozwoju usług i sieci telekomunikacyjnych. Rozwój ten nie może być jednak pozostawiony sam sobie. Samorząd terytorialny z jednej strony ma go wspierać, z drugiej jednak ma chronić użytkowników usług i sieci telekomunikacyjnych przed cyberzagrożeniami. Cyberbezpieczeństwo musi zatem znaleźć odpowiednie miejsce w katalogu zadań samorządu terytorialnego, który nie może go marginalizować, ponieważ zagrożenia w sieci są rzeczywiste i mogące wyrządzić znaczne szkody, a nie wirtualne.

Słowa kluczowe: usługi telekomunikacyjne, sieci telekomunikacyjne, cyberbezpieczeństwo, samorząd terytorialny, infrastruktura telekomunikacyjna, internet