ROCZNIKI NAUK PRAWNYCH
Tom XXX, numer 2 – 2020
DOI: https://doi.org/10.18290/rnp20302-7

DOMINIKA SKOCZYLAS

THE ACT ON THE NATIONAL CYBERSECURITY SYSTEM AND OTHER LEGAL REGULATIONS IN THE CONTEXT OF ENSURING STATE CYBERSECURITY
SELECTED ISSUES

INTRODUCTION

The increasing use of electronic means of communication has forced a number of legal and organizational changes. These changes result from the need for proper flow of information between the message sender and recipient, improving the provision of e-services and ensuring adequate protection of personal data, and the operation of technical infrastructure. It should be noted that the speed and efficiency of distance communication is undoubtedly a positive aspect while maintaining a good quality e-service. Globalization and free movement of goods and services have transformed the way of thinking about society and public administration bodies regarding the traditional management model. Globalization itself is a multi-faceted concept. Given its many meanings, it should be highlighted that:

– it includes supranational integration processes,

– decisions taken in a specific part of the world affect the functioning of the international community,

– integration takes place on an economic, social and political level,

– it determines mechanisms of international cooperation and interdependence of parties to a given relationship,

DOMINIKA SKOCZYLAS—Faculty of Law and Administration University of Szczecin, e-mail: dominika.skoczylas@usz.edu.pl; ORCID: https://orcid.org/0000-0003-1231-8078

– it intensifies and develops international relations in trade, transactions, social communication,

– information and communication technologies are a necessary condition for the internationalization of contacts [MIR, HASSAN and QADRI 2014, 611-612].

It follows that system tools in the 21st century are not only used for intersocial communication, but also fulfill a socio-economic function. What is more, they improve the ability to do things over the internet. Unfortunately, the amount of information in the system is very often used by unauthorized persons in an illegal manner, thereby causing damage in an individual (stealing personal data) or nationwide dimension (hacking government websites). Each country is obliged to secure IT systems against cybercriminals.

Nowadays, the biggest advantage of remote communication is the possibility of transferring information quickly. The use of electronic means of communication is currently associated with the computerization of public administration. Today, one can use ICT tools not only for interpersonal contact, but also to handle administrative matters. Public administration bodies willingly use new technologies, thus implementing the postulate of public utility. However, it should be remembered that the performance of public tasks within e-government must be preceded by a number of activities of the following nature:

– organizational (structural and personnel changes),

– legal (introduction of legal provisions regulating both the basic competences of the authorities, specifying activities that can be performed using ICT systems and issues regarding system security), - technological (adaptation of hardware, software, system tools, use of new information and communication technologies). The definition of appropriate procedures and mechanisms is undoubtedly associated with the growing demand for the use of e-information and provisions of e-services [CELAREK 2013, 43].

Therefore, information has become a value and a good that should be subject to special legal protection. The introduction of modern information and communication technologies has changed the rules of using information, as since then it has become possible to perform various types of system operations involved in processing it. Information is being made available on a regular basis not, undergoes numerous modifications, and is also archived as part of e-collections. In addition, information is related to the fact that the entity that uses it has specific knowledge on a given topic. Public, central and local government authorities willingly use new technologies, entering state and economic information into electronic catalogues or using modern solutions for the purposes of the functioning of critical infrastructure or key segments of the state's operation. It can therefore be concluded that the amount of data contained in ICT systems is so great that the government must introduce special safeguards, thus preventing information leakage, network disruptions or in extreme cases its complete breakdown [CAVELTY 2012, 362-377]. Moreover, the constant desire to download and use information is an indication of an information society. A society for which constant access to information, at any place and time, is a basic value. Entering a new era of digitization has forced a number of changes in innovation and new technologies. Processing, storage and sharing has become easier, thanks to the use of so-called information and communication technologies. The development of IT and computerization have enabled an easier and faster way to distribute information, mainly through external telecommunications networks. The implementation of broadband connections and full networking are the main tasks that public administration is facing in the 21st century [WEBSTER 1995, 7-8]. The communication revolution, and above all the processes of international integration, had an impact on the final definitional shape of the information society. Today, it is characterized its features, which are:

– high level of information exchange,
– wide application of information and communication technologies,
– intensity of data processing,
– developed network infrastructure [DIJK 2006, 19-20].

There are many definitions of the information society, of which one collective definition may be created which includes designations of the name of this term: it is a society based on knowledge and information, of a global nature, because the flow of data and services is unrestricted both locally and temporarily. Clarity, precision and speed of communication are important to it. Due to the value of the text contained in specific information, particular attention is paid to the medium and manner of the message. The information society recognizes ITC solutions as an asset, which is why it willingly uses electronic means of communication [ISAZADEH 2004, 1-4]. An interesting position was presented by Yoneji Masuda, who noted that the development of the information society is qualified on the basis of the current state of knowledge and the scope of the use of information and communication systems and technologies and other electronic tools. The goal then involves achieving results of socio-economic importance. Information society is therefore an important link necessary for the proper functioning of e-government [YONEJI 2004, 15-16]. Its activity embodies the principle of a democratic rule of law.

1. CYBERSECURITY IN CYBERSPACE. THREATS TO NETWORK SECURITY

The role of information society, and thus the legitimacy and necessity to use electronic means of communication, is highlighted by many EU law documents. Already the document entitled "Europe and the global information society: recommendations to the European Council", commonly known as the Bangemann Report [EUROPEAN COMMISSION, 1994], emphasized the impact of new ICT tools on the economic sector, on the European services market operating on the basis of information and communication, on the free flow of information and the use of electronic services, construction of electronic public administration, as well as equal access to electronic devices and infrastructure. The area of interest in the subject of electronic communication and the information society is evident in many acts of international rank, initiatives, plans or strategies, as well as in those acts covering a specific field of knowledge. Particular attention should be paid to the Lisbon Strategy, which closely refers to the concept of the information society, promoting, among others: modern solutions for regulating telecommunications, intensification of activities in the field of e-economy, innovation, e-health, intelligent transport, and above all e-administration [GANCZAR 2009, 21-23]. Inevitably referring to the aspect of providing services by electronic means and of performance of information society services, individual European Union countries adopt optimal legal solutions. Poland, aware of its technological and economic potential, is also trying to create a uniform legal framework improving the mechanisms of functioning of the society and public administration on the web. However, this is not a simple task due to threats to network security. The process of full computerization is ongoing, which is why it is important that actions in terms of interoperability and networking at the cross-border level are not only sufficient, but at least efficient and effective.

Currently, information and communication technologies are widely used not only among Internet users, but also in the sphere of public law. Thus, public administration bodies and other administrative entities use modern IT solutions as part of their electronic administration. Technological transformations have changed the style of management and the transition from the so-called traditional model, in which information is processed on paper, there is no automatic data transmission, access is often limited, excessive bureaucratization of tasks occurs and so does often an information blockade for the electronic administration model. This style of management is also dictated by non-technological factors such as: globalization, socio-economic development or increased awareness of the right to information in the information society [JASTRZĘBSKA 2018, 61,65]. ITC solutions are primarily to serve the effectiveness and efficiency of performing public administration tasks. Electronic administration, along with a typical management function, implements the postulate of public utility. Digitalization of documentation is conducive to the classification and analysis of data, facilitates searching for it, ensures accessibility and transparency, streamlines the procedure and facilitates and accelerates the handling of official matters. The use of electronic means of communication strengthens the foundations of the functioning of a democratic rule of law. It makes communication with the organ friendly and effective. It also enables citizens to express their views on public authority through electronic voting or e-consultations. It is pointed out that e-government is raising the level of interaction in terms of sharing information online, remote communication and making the so-called electronic transactions or deliveries as part of e-services [RADU and PÓLKOWSKI 2014, 187-188].

The use of ICT tools is important in the aspect of international communication, understood not only through the prism of interpersonal communication, but above all as a possibility of sending information or providing services on a transnational scale. This makes it all the more important to protect networks and systems from harmful effects of third parties, which may not only cause short-term incidents but, above all, reduce or completely prevent the provision of public services. Because the whole world uses ICT, each country is exposed to ever newer cyber attacks. It is therefore not surprising the dynamism of changing regulations. The cyberspace of EU Member States and countries intending to join the EU is extremely vulnerable to hacking attacks. Probably the most famous cases: Estonian (2007), Georgian (2008) and Ukrainian (2014, 2015) only confirm this assumption. Russia seems to be particularly active, which in each of the above mentioned cases has tried to destabilise, the internet services of public and private sectors, websites, governmental and media infrastructure not infrequently linked to a physical attack (such as, for example, the Russian government's own internet service, the governmental and media infrastructure in Ukraine). The aggression is both cybernetic and kinetic. Cyber measures can also threaten NATO's security, and this already determines the need for global network protection [ILVES et al. 2016, 128].

The free flow of goods and services, and the need for innovation in the socio-economic sector are emphasized by EU legislation. The emphasis is on, among others, the definition of information society services, understood as any services normally provided for remuneration, at a distance, by means of electronic devices for data processing (including digital compression) and storage, at the individual request of a recipient, where at a distance means a service provided without the parties being simultaneously present; by electronic means entails that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; at the individual request of a recipient of services means that the service is provided through the transmission of data on individual request [Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC][1]. The basic issues of freedom to provide e-services are regulated by the Directive on electronic commerce [Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000][2]. In reference to it, but also to other EU legislation, the Polish legislator also adopted legal regulations regarding the principles of computerization and provision of services by electronic means.

The Digital Single Market Strategy promotes optimal solutions to ensure a high level of consumer protection in the functioning of the internal market. This applies mainly to sales contracts concluded between the seller and the consumer, including the rules on the conformity of goods with the contract, the remedies for lack of conformity, the means of exercising those remedies and the commercial guarantees [Article 1 Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC][3]. Competitiveness, free movement of goods and services, is a priority for the European Union, in particular as regards the development of cross-border e-commerce, between businesses and consumers.

[1] Journal of Laws of 1998, item 217.

[2] Journal of Laws of 2000, item 178.

[3] Journal of Laws of 2019, item 136.

Issues relating to removing barriers to the development of cross-border e-commerce within the Union, in terms of access to digital content and services, are also important. The case study should address the protection of consumers with regard to access to such services, but primarily in the framework of establishing common rules on certain requirements for contracts concluded between traders and consumers, e. g. the conformity of the digital content or service with the contract, or changes to the digital content or the digital service [Article 1 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services][4].

In the Act on the computerization of the activities of entities performing public tasks [Act of February 17, 2005][5], in addition providing definitions of such important concepts as: electronic document 1, electronic platform of public administration services 2, trusted profile 3 or trusted signature 4, the Polish legislator emphasized the importance of electronic administration for the efficient and effective functioning of the entire public administration. Accordingly, special attention was paid to the requirements for ICT systems used to perform public tasks, including public registers, and the way information is exchanged in electronic form with public entities. The need to provide the so-called National Interoperability Framework for ICT systems was noted so that it is possible to introduce appropriate standards of e-government operation while maintaining sufficient transparency of registers.

However, exchanging information electronically between the parties to an administrative relationship and maintaining the interoperability of information society services is not a simple task. Cyberspace threats are the basic problem of e-services implementation by e-administration. The popularization of the provision of electronic services has resulted in the emergence of cyber culture law, more specifically cyberspace law. Cyber Law covers the characteristics of new tools, including ICT systems and electronic means of communication in the context of legal regulations. Treating modern technologies and electronic services as the basic conditions for the development of a new field of law is a sign of new times, times in which the most important issues are a combination of law and computerization. Moreover, cyberspace highlights the importance of public information in a global sense. This information is unfortunately exposed to various types of interference and threats.

[4] Journal of Laws of 2019, item 136.

[5] Journal of Laws of 2019, items 700, 730, 848, 1590.

Therefore, the primary duty is to safeguard its integrity as well as availability and confidentiality of the data it contains [JANOWSKI 2012, 304-305].

What is the Internet's strength, i.e. the capacity for unlimited access to and transmission of data, can translate into network users' negative behaviors in the form of criminal incidents. In the Polish legal order, the concept of cyberspace is widely emphasized. Cyberspace threats can be a reason for the imposition of martial law on part or the entire territory of a state [Act of August 29, 2002 on martial law and on the competences of the Supreme Commander of the Armed Forces and the principles of its subordination to the organs of the Republic of Poland, Article 2(1)][6], a state of emergency [Act of June 21, 2002 on the state of emergency, Article 2(1)][7] or the state of natural disaster in the event of a technical failure caused by an event occurring in cyberspace [Act of April 18, 2002 on the state of natural disaster, Article 2][8]. As Grażyna Szpor points out, the concept of cyberspace is important from the point of view of the sovereignty of the state, which, taking into account the dynamism and development of technology and communication as well as the information infrastructure itself, must achieve lasting coherence of political and organizational systems, in particular regarding transparency and coherence of legal regulations [SZPOR 2016, 138-139].

Currently, the international community, governments of certain countries, and organizations and institutions are constantly using the Internet as a basic tool for exchanging information and providing services. Therefore, they need to know how to ensure or use economic and communication freedom so that secure and continuous provision of e-services is possible. Therefore, the identification of threats that may cause disruptions in the proper functioning of both individual means of electronic communication and the entire ICT system seem the most important. Hacker attacks do not only have their specific names or scope of occurrence, but they also cause smaller or bigger problems in terms of network operation. Specific methods are also proposed to combat cyber-attacks depending on the area in which they take place. In the US in 2010, the fight against online threats was defined as the Cold War on the Internet. The fight against cybercrime is obviously a supranational matter because cyberspace is an international space [O'CONNELL 2012, 187-189].

Cybersecurity involves maintaining certain standards for the proper functioning of the network, the most important of which are: confidentiality,

[6] Journal of Laws of 2017, item 1932.

[7] Journal of Laws of 2017, item 1928.

[8] Journal of Laws of 2017, item 1897.

integrity and availability of information. Depending on who will be affected by the protection, it can be determined individually (protection of personal data, privacy) or collectively (protection of citizens, ICT systems and critical infrastructure). Therefore, protective tasks related to ensuring security concern all structures, all legal entities and a huge number of information resources. The global range of services and information, with technological advancement, makes the issue of network threats not uniform but diverse in the number and types of occurring threats [HOFFMANN 2018, 19-20]. Hackers' taking control over the network can take the form of:

– activism – non-destructive activity, where the network serves to support terrorist activities,

– hacktivism – using the network for activities aimed not so much at criminal activities as at disrupting the proper operation of the Internet,

– cyberterrorism – an attack or threat of attack on ICT systems or critical infrastructure in order to destroy it, possibly intimidate or enforce specific behavior, including destabilization, disinformation or propaganda, most often for political or financial reasons. The most common network threats include Trojan horses, the use of unknown, often illegal sources or software, viruses, worms and bacteria, destruction of authorization tools, redirection of information to people other than the data administrator, the so-called logic bombs, the activation of which causes the creation of additional computer functions interfering with its operation, gaining access to the network by installing chips, impersonating the network user, the so-called hijacking – involving the transmission of data between systems, the so-called sniffing – tracking user's movements, so-called DOS – blocking the service or functioning of the entire server, or blocking e-mail [LIEDEL and PIASECKA 2008, 40-42].

It is worth emphasizing that potential threats constitute the basis for introducing appropriate preventive and remedial measures in the event of their occurrence in the future. One cannot disagree with the statement that cyber security should be seen as an extension of information security, and cyber security should consist not only in protecting information or resources of information systems of a person or organization, but also in protecting Internet users [SOLMS and NIEKERK 2013, 101]. Thus, the issue of assessing the threats to the proper functioning of e-services and e-administration as well as the effective exchange of e-information should be a priority task for public authorities.

The effects of cybersecurity breaches include both threats to the functioning of critical infrastructure and services considered critical to national and economic development and those involving breaches of network users' privacy. In the case of the first group, the risks may be of an organisational and technological nature. The prevalence of ICT tools and general access to applications, installations or Internet platforms without adequate security, user identification and data authentication may result in situations where this occurs:

– unauthorised (unauthorised) access to data,

– intentional sabotage of public Internet platforms through which key services are provided,

– assumption of control over critical infrastructure,

– limiting, preventing the proper use of the infrastructure, in the worst case, its destruction,

– disruption of continuity of service,

– paralysis of the functioning of the State and the economy [PONIEWIERSKI 2014, 68-69].

The possibility of destabilisation of the country should also be assessed from the perspective of the so-called blackout network. The occurrence of network failures may lead to certain technical parameters being exceeded, thus preventing the optimal functioning of critical infrastructure and ICT systems used for its operation. That is why it is so important to define the requirements of the network, frequency and volume of data transmission, thus implementing an appropriate policy to enable continuous and stable operation of systems. Perhaps it is worthwhile in this case to introduce the so-called rolling blackout, i. e. previously planned shutdown and maintenance of the technical infrastructure, and carry out a safety assessment of the system equipment [ZYCH and FÓRMANIAK 2017, 660-663].

As regards threats directly affecting the network user, it should be noted that these relate directly to privacy and the protection of personal data processed in information and communication systems. The transmission of personal data to which a hacker has gained unauthorised, unauthorised, illegal access can therefore be considered a threat. Taking control of the system in which personal data is collected makes it possible to obtain it and, consequently, to use it in order to carry out illegal flows of financial transactions or identity theft. That is why it is so important to analyze and assess the possible threat and introduce optimal protective measures against cyberattacks [TARABASZ 2018, 68-69].

The danger of hacking is that it can only consist in gaining access to the ICT system and e-data (sensu stricto) and can aim at total disruption and destabilization of the system, destruction or modification of data (sensu largo). All the above activities may constitute a prelude to committing a specific type of computer crime against information protection [RADONIEWICZ 2013,122]. The most serious of these are in Criminal Code:

– Article 267 § 1 CC 5 – unauthorised access to information,

– Article 267 § 2 CC – unauthorised access to the information system,

– Article 267 § 3 CC – illegal eavesdropping through computer devices and programs,

– Article 267 § 4 CC – disclosure to another person of information obtained illegally,

– Article 268 § 2 and 3 CC – destroying, damaging, deleting or altering the recording of relevant information on an IT storage medium,

– Article 268a CC – damage to databases,

– Article 269 CC – computer sabotage,

– Article 269a CC – network disruption,

– Article 269b CC – unlawful use of programmes and data (Act of 6 June 1997 – Criminal Code)[9].

Filip Radoniewicz, as the most important challenge in ensuring the security of cyberspace, raises the issue of computer crime. The problems related to identification of the perpetrator in relation to the scale of the phenomenon are significant. The global transmission of information makes it very difficult both to take preventive action and to find the source (perpetrator) of the crime. Bearing in mind that users are unaware of the potential threat, the anonymity of the attack and the processing of countless amounts of information in electronic databases, the Internet is becoming an easy place to carry out criminal activities on a mass scale [RADONIEWICZ 2016, 128]. Technological advances seem to facilitate the development of computer crime.

2. ADMINISTRATIVE POWER OF PUBLIC ADMINISTRATION BODIES. CYBERSECURITY OBLIGATIONS

The number and type of threats in the cyberspace sphere implies the need to protect it. The greatest responsibility in the implementation of appropriate network and system security measures lies with public administration bodies and other entities performing public tasks. This is because it is public administration and other entities operating within public administration, acting on

[9] Journal of Laws of 2019, item1950.

behalf of and on account of the state, have the right to use the so-called administrative authority. This power gives them the opportunity to use specific authority, called coercive measures, to enforce the law. The creation of appropriate legal regulations and their subsequent implementation is both a right and an obligation of the authorities. However, it is worth remembering that the essence of public administration is to focus tasks on public interest and protect public goods and services. On the other hand, the executive character is manifested in the concretization of the applicable law, i.e. adaptation to the changing rules of reality, in particular when it comes to public security [ZIMMERMANN 2006, 29-31]. It should be admitted that public administration in the context of regulatory tasks strengthens the standards, indicating the preservation of the value of a democratic state ruled by law. Placing relevant legal provisions in statutory documents guarantees, among others, protection of the internal and external security of the state, respect for human rights and freedoms, harmonious human functioning in a society, while ensuring conditions for the development and use of available resources, including modern means of electronic communication [KRAWCZYK 2016, 208-209].

Poland is one of the fastest developing countries of the Old Continent. Economic growth is undoubtedly associated with the use of modern communication and information technologies by entrepreneurs themselves, private individuals and public administration. The introduction of system solutions and digitization in the administrative procedure, as well as the use of new technologies in such areas as: health protection, transport, energy industry, the banking and financial sector or digital infrastructure, have highlighted the need for legal changes. It should be mentioned that the Polish cybersecurity system is largely based on or derived from European regulations, in particular the EU law. The construction of the European cybersecurity system imposed on individual EU Member States the obligation to shape their own legal framework in the field of security. While the European Union Network and Information Security Agency operates at the European level and is responsible for the security of ICT networks and systems in the EU and the introduction of appropriate security standards, due to the nature of the threats and their type, each country should have its own cybersecurity strategy. One can find the following statement on the Agency's official website: “In a constantly changing cyber threats environment, EU Member States need to have flexible and dynamic cybersecurity strategies to meet new, global threats”. Particular emphasis is given to the aspect of national cybersecurity strategies and the introduction of appropriate legal regulations due to the potential threats to the functioning of the network and critical infrastructure [ENISA 2019]. The high level of cybersecurity concerns many areas and services, in particular ITC infrastructure, transport, industry, public and government administration, finance and health care. Taking into account the free flow of goods and services, current communication opportunities, and other globalization processes within the EU, a Directive concerning measures for a high common level of security of network and information systems across the Union was adopted [Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016][10]. The NIS Directive indicates the following assumptions:

– adopting or maintaining provisions to achieve a higher level of security of network and information systems (Article 3),

– implementation of the so-called national strategies for the security of network and information systems, ensuring strategic goals and priorities for the security of network and information systems at the national level,

– designation of the competent authority or authorities for the protection of network and information security,

– identification of operators of essential services and digital service providers,

– ensuring the protection of personal data and ICT systems against network threats, assessment of potential threats, preventive actions and actions taking place after the occurrence of the event [BANASIŃSKI and NOWAK 2018, 154-157].

The emergence of threats to the proper functioning of cyberspace had a significant impact on the appearance of a special type of law in the Polish legal order. The Act, which prioritized tasks in determining the functioning of ICT networks and the use of supervision and control measures in the event of a network incident. The Act on the National Cybersecurity System [Act of July 5, 2018][11] defines cybersecurity as resilience of information systems to activities that violate the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems (Article 2(4). It indicates numerous incidents that may hinder or interrupt the implementation of a public task or key service. Particular attention is devoted to organizing the structures of the national cybersecurity system, which include: operators of essential services, digital service providers, CSIRT MON 5, CSIRT NASK 6, CSIRT GOV 7, as well as, among others: entities providing services in the field of cybersecurity, competent authorities

[10] Journal of Laws of 2016, item 194.

[11] Journal of Laws of 2018, item 1560.

for cybersecurity, Single Contact Point for cybersecurity, Government Plenipotentiary for Cybersecurity, Cybersecurity Committee (Article 4 of the Act on the National Cybersecurity System). From the ministerial side it follows that CSIRT MON, CSIRT NASK and CSIRT GOV coordinate activities in the field of handling incidents reported by individual entities, e.g. local government units and citizens are served by CSIRT NASK, public authorities, including government administration bodies, state control and law protection bodies as well as and courts and tribunals are supported by CSIRT GOV, entities subordinate to or supervised by the Minister of National Defense, including entities whose ICT systems or ICT networks are entered in the uniform list of facilities, installations, devices and services forming critical infrastructure are supported by CSIRT MON [MINISTRY OF DIGITAL AFFAIRS 2019].

The role of operators of essential services and digital service providers in the aspect of actual incident management also seems to be indispensable. According to Annex 1 to the Act on the national cybersecurity system, key sectors in Poland include: energy (e.g. extraction of minerals, electricity, heat, oil and gas), transport (air, rail, water and road), banking and financial market infrastructure, drinking water supply and distribution, health care and digital infrastructure. In turn, Annex 2 specifies digital services as online trading platforms, cloud computing services and internet search engines [Annexes 1 and 2 to the Act on the National Cybersecurity System][12]. Therefore, the array of obligations lying with suppliers or operators of essential services is not surprising. Their tasks include:

– as regards operators of key services: construction and implementation of a security management system in the information system through which the key service is provided, estimation of an incident occurrence risk, risk management attempts, provision of technical and organizational measures in the field of cyber security and system security, access control, continuity of supply, documenting the action strategy, monitoring system threats, incident management – the use of appropriate cybersecurity measures and mechanisms, ensuring nationwide communication [CHAŁUBIŃSKA-JENTKIEWICZ 2019, 101-103],

– for digital service providers: the use of appropriate and proportionate technical and organizational measures to manage risk due to the security of information systems and facilities, network incident management, ensuring

[12] Journal of Laws of 2018, item 1560.

the continuity of digital service provision, as well as monitoring, auditing and testing of ICT systems [TACZKOWSKA-OLSZEWSKA 2019, 142-144].

The Act on the National Cybersecurity System assigns a special role to public administration bodies, that is individual ministers managing specific government administration activities (e.g. for the energy sector – minister competent for energy) or central units (e.g. for the banking sector and financial market infrastructure—the Financial Supervision Authority). Because of their attributes of authority and broad statutory competences, they are required to act in a certain way before an incident occurs and to take certain remedial actions in the event of its occurrence. In accordance with Article 42 of the Act on the National Cybersecurity System, these are tasks in the field of: recognizing the entity as an operator of essential services and issuing a relevant decision on the basis of which the operator will be included in the ministerial list of operators of essential services, preparing recommendations jointly with CSIRT NASK, CSIRT GOV, CSIRT MON and sectoral cybersecurity teams to strengthen cybersecurity, ongoing monitoring of the application of the provisions of the Act, calls for removal, within a prescribed period, of vulnerabilities which led or could lead to a serious, significant or critical incident, auditing and supervision of operators of essential services and digital service providers, international cooperation and protection of personal data. The scale and importance of cybersecurity was emphasized by Marek Zagórski, Minister of Digital Affairs, at the last Congress 590, which took place on October 7-8, 2019 in Jasionka near Rzeszów, He said that the participation of citizens in the use of digital services is constantly increasing. The government and the Ministry of Digital Affairs are striving to ensure that most official matters in Poland can be dealt with online. In addition, he emphasized the growing number of users of the trusted profile, which is currently used by over 4,350,000 people [MINISTRY OF DIGITAL AFFAIRS 2019]. The potential of public administration bodies in the case of cyberspace protection is extremely important, because only they can actually conduct ongoing monitoring and use authority measures for effective system protection.

Security in cyberspace should be treated very widely, due to the maintenance of an appropriate level of protection for all network users. Public institutions and public administration bodies play an important role, because they are responsible for introducing proper standards of compliance with the law in the network. However, internet users should also try to protect their computers and online platforms they use. Cybercriminals use increasingly new methods of operation. Therefore, protection is needed both in the legal aspect (with particular emphasis on human rights and freedoms) and in technology [CZYŻAK 2018, 118].

It is worth mentioning that a particular type of solution in the context of cybersecurity is contained in the so-called Cybersecurity Strategy of the Republic of Poland for 2019-2024 [Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019-2024][13]. Its adoption is based on Article 68 of the Act on the National Cybersecurity System. The strategy shall define strategic objectives and appropriate policy and regulatory measures to achieve and maintain a high level of cybersecurity, including, inter alia actors involved in the implementation and enforcement of the Strategy, the approach to risk assessment or actions relating to cybersecurity education, information and training programmes (Article 69, The Act on the National Cybersecurity System).

The current Strategy, which replaced the previous National Cybersecurity Policy Framework of the Republic of Poland for the years 2017-2022, contains 5 specific objectives of the cybersecurity policy, which are: to develop the national cybersecurity system, to increase the level of resilience of information systems of public administration and the private sector and to achieve the ability to effectively prevent and respond to incidents, to increase national capacity in the field of cybersecurity technologies, to build awareness and social competence in the field of cybersecurity and to build a strong international position of the Republic of Poland in the field of cybersecurity. The strategy aims to contribute both to the implementation of the Act on the National Cybersecurity System and to a real increase in cybersecurity, especially in digital services, critical services and critical infrastructure protection.

CONCLUSIONS

The importance of legal mechanisms is most clearly demonstrated when a network attack occurs. In Poland, as shown in the report from F-Secure, the number of cyberattacks increased significantly in 2018. The report demonstrates that in 2018 Poland was the target of as many as 6 million cyberattack attempts, with the largest number coming from the United States

[13] Monitor Polski of 2019, item 1037.

(about 1.5 million), France (900,000) and the Russian Federation (830,000). Attacks come from different parts of the world, including from China, Finland, Singapore, Ukraine, Argentina, Germany or Great Britain. Analyzing the results, it can be seen that cyber security is important in both large cities and smaller suburban agglomerations [KOSIELSKI 2018]. The strength of domestic hacker attacks needs to be remembered. Cybercriminals often use here greater knowledge in terms of taking control over a given operating system or critical infrastructure. Technological progress is inevitable. The manner of carrying out attacks and types of network threats are changing. Which is why the role of public administration bodies and other entities performing security-related public tasks is so essential. In particular, when it comes to the protection of personal data or the functioning of critical infrastructure. The role of the state, in the individual sense, boils down to protection of the confidentiality, integrity and availability of data belonging to individuals and protection against cybercrime [HARLEY, MYERS, COBB and AMAYA 2019]. As for the macroeconomic situation, the authorities assume obligations ensuring stable and sustainable socio-economic development.

Cyberattacks can affect critical infrastructure and administrative facilities, continuity of service or information security. The Polish legislator has read the intention of the EU legislation very well in terms of protecting both the collective and private interests of cyberspace users.Secondly, it was pointed out that the most important objective is not to handle incidents that have already occurred, but first and foremost to prevent them from occurring, i. e. the application of appropriate preventive and protective measures. The most effective protection is one in which not only public administrations but also key service providers and operators themselves are directly involved. Cyberprotection activities should include not only the proper functioning of services, but the continuous improvement of systems, while keeping information secure. Ensuring proper legislation and implementing it can protect both European and Polish ICT networks from many cyber threats.

For the sake of the order in the paper, it is worth mentioning the basic legal acts and other documents addressing cybersecurity that are in force in the Polish legal order:

– Act on the provision of electronic services [Act of July 18, 2002][14],

– Personal Data Protection Act (Act of May 10, 2018)[15],

[14] Journal of Laws of 2019, items 123 and 730.

[15] Journal of Laws of 2019, item 1781.

– 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[16],

– Regulation of the Council of Ministers of September 11, 2018 on the list of essential services and materiality thresholds for the disruptive effect of an incident for the provision of essential services[17],

– Integrated State Computerization Program,

– National Framework of Cybersecurity Policy of the Republic of Poland.

Unfortunately, due to the layout of the work, one should limit themselves to stating that each of the above-mentioned documents requires a separate explanation as to the basic rules and method of operation in the event of a network threat. Nevertheless, the Polish authorities want to ensure the proper functioning of cyberspace and, knowing the value and importance of electronic communication, assume responsibility for the digital security of the country. It can be said with certainty that Polish legal regulations are a response to potential threats to the network's proper functioning. However, changes in the style of public administration management, the arrangement of international relations between countries, the use of ITC as the basic method of archiving documents and the progressing computerization of public life will once again be verified by the current legal status. It will also be verified by network users and cyberterrorists.

REFERENCES

BANASIŃSKI, Cezary and Włodzimierz NOWAK. 2018. „Europejski i krajowy system cyberbezpieczeństwa." In: *Cyberbezpieczeństwo. Zarys wykładu*, edited by Cezary Banasiński, 154-157. Warszawa: Wydawnictwo Wolters Kluwer.

CAVELTY, Myriam Dunn. 2012. „Cyber-security." In: *Contemporary Security Studies*, edited by Alan Collins, 362-377. Oxford: Oxford University Press.

CELAREK, Krystyna. 2013. *Prawo informacyjne. Problem badawczy teorii prawa administracyjnego.* Warszawa: Wydawnictwo Difin.

CHAŁUBIŃSKA-JENTKIEWICZ, Katarzyna. 2019. „Obowiązek wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej." In: *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, edited by Waldemar Kitler, Joanna Taczkowska-Olszewska, and Filip Radoniewicz, 101-103. Warszawa: Wydawnictwo C.H. Beck.

CZYŻAK, Mariusz. 2018. „Bezpieczeństwo w cyberprzestrzeni." *TEKA Commission of Legal Sciences, Volume XI, Polish Academy of Sciences Branch in Lublin* 2:118.

[16] Journal of Laws 119/1.

[17] Journal of Laws of 2018, item 1806.

DIJK, Jan A.G.M. van. 2006. *The Network Society. Social Aspects of New Media.* London, Thousand Oaks, New Delhi: SAGE Publications Ltd.

EUROPEAN COMMISSION. 1994. „Europe and the Global Information Society." *Recommendations to the European Council, Bangemann Report.* In http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf [accessed: 8.10.2019].

ENISA, European Union Agency For Cybersecurity. 2019. *National Cybersecurity Strategies.* In https://www.enisa.europa.eu/topics/national-cyber-security-strategies [accessed: 15.10.2019].

GANCZAR, Małgorzata. 2009. *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*. Warszawa: Wydawnictwo CeDeWu.

HARLEY, David, Lysa MYERS, Stephen COBB and Camilo GUTIÉRREZ AMAYA. 2019. *Cybersecurity Trends 2019: Privacy And Intrusion In The Global Village.* In https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET_Trends_Report_2019.pdf. [accessed: 15.10.2019].

HOFFMANN, Tomasz. 2018. *Wybrane aspekty cyberbezpieczeństwa w Polsce.* Poznań: Wydawnictwo FNCE.

ILVES, Luukas K., Timothy J. EVANS, Frank J. CILLUFFO, Alec A. NADEAU 2016. „European Union and Nato Global Cybersecurity Challenges. A Way Forward." *Prism Security Studies Journal* 6 (2): 128.

ISAZADEH, Ayaz. 2004. „Information Society: Concepts and Definitions." *WSEAS Transactions on Systems* 6(3): 1-4. In https://www.researchgate.net/publication/254476368_Information_Society_Concepts_and_Definitions [accessed: 15.10.2019].

JANOWSKI, Jacek. 2012. *Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa.* Warszawa: Wydawnictwo Difin.

JASTRZĘBSKA, Karolina. 2018. *Elektroniczna administracja jako narzędzie wdrażania zmian organizacyjnych*. Warszawa: Wydawnictwo CeDeWu.

KOSIELSKI, Mateusz. 2018. *Ponad 6 milionów cyberataków na Polskę. Jest gorzej niż rok temu.* In https://www.cyberdefence24.pl/ponad-6-milionow-cyberatakow-na-polske-jest-gorzej-niz-rok-temu [accessed: 15.10.2019].

KRAWCZYK, Mariusz. 2016. *Podstawy władztwa administracyjnego,* Warszawa: Wydawnictwo Wolters Kluwer SA.

LIEDEL, Krzysztof and Paulina PIASECKA. 2008. *Jak przetrwać w dobie zagrożeń terrorystycznych. Elementy edukacji antyterrorystycznej.* Warszawa: Wydawnictwo Trio Collegium Civitas.

MINISTRY OF DIGITAL AFFAIRS. 2019. *Cyfryzacja w służbie zrównoważonego rozwoju, bezpieczeństwo sieci 5G – minister cyfryzacji na Kongresie 590.* In https://www.gov.pl/web/cyfryzacja/cyfryzacja-w-sluzbie-zrownowazonego-rozwoju-bezpieczenstwo-sieci-5g---minister-cyfryzacji-na-kongresie-590 [accessed: 15.10.2019].

MINISTRY OF DIGITAL AFFAIRS. 2019. *Krajowy System Cyberbezpieczeństwa.* In https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa [accessed: 15.10.2019].

MIR, Usman Riaz, SYEDA MAHNAZ HASSAN and MUBASHIR MAJEED QADRI. 2014. „Understanding Globalization and its Future: An Analysis." *Pakistan Journal of Social Sciences* 34(2): 611-612.

O'CONNELL, Mary Ellen. 2012. „Cybersecurity without Cyber War." *Journal of Conflict & Security Law* 187 (2012): 187-189.

PONIEWIERSKI, Aleksander. 2014. „Zagrożenia dla bezpieczeństwa infrastruktury krytycznej w kontekście zaawansowanego zastosowania rozwiązań teleinformatycznych – wyzwania dla państwa." In: *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, edited by Joanna Świątkowska, 68-69. Kraków: Wydawnictwo Instytut Kościuszki.

RADONIEWICZ, Filip. 2016. *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*. Warszawa: Wydawnictwo Wolters Kluwer Polska.

RADONIEWICZ, Filip. 2013. „Odpowiedzialność karna za przestępstwo hackingu." *Prawo w Działaniu*, t. 13: *Sprawy Karne* 122.

RADU, Ana Maria and Zdzisław PÓLKOWSKI. 2014. „Theoretical, technical and practical aspects of e-administration." *Studia z Nauk Społecznych,* 7: 187-188.

SOLMS, Rossouw von and Johan VAN NIEKERK. 2013. „From information security to cybersecurity." *Computers & Security* 38: 97-102.

SZPOR, Grażyna. 2016. *Jawość i jej ograniczenia,* t. I: *Idee i pojęcia.* Warszawa: Wydawnictwo C.H. Beck.

TACZKOWSKA-OLSZEWSKA, Joanna. 2019. „Status i obowiązki dostawcy usługi cyfrowej." In: *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, edited by Waldemar Kitler, Joanna Taczkowska-Olszewska and Filip Radoniewicz, 142-144. Warszawa: Wydawnictwo C.H. Beck.

TARABASZ, Anna. 2018. „Cybersecurity and Internet of threats – new challenges in customer behavior." *Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach* 360 (16): 68-69.

YONEJI, Masuda. 2004. „Image of the future information society." In: *The Information Society Reader*, edited by Frank Webster, 15-16. London: Routledge Taylor & Francis Group.

WEBSTER, Frank. 1995. *Theories of the information society.* London and New York: Taylor & Francis Group.

ZIMMERMANN, Jan. 2006. *Prawo administracyjne.* Kraków: Wydawnictwo Zakamycze.

ZYCH, Jan and Cezary FÓRMANIAK. 2017. „Źródła Blackoutów w Polsce z perspektywy zarządzania kryzysowego." *Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa* 1 (34): 660-663.

ENDNOTES

1. CC – Act of 6 June 1997 – Criminal Code.
2. electronic document in accordance with the Act is a separate set of semantic data stored in a specific internal structure and saved on an IT data carrier
3. electronic platform of public administration services, treated as an ICT system in which public institutions provide services through a single access point on the Internet.
4. trusted profile – means of electronic identification containing a set of data identifying and describing a natural person who has full or limited legal capacity
5. trusted signature – an electronic signature, the authenticity and integrity of which are ensured using the electronic seal of the minister competent for computerization, containing: data identifying the person, identifier of the electronic identification means with which it was deposited, and the time of its submission.
6. CSIRT MON – Computer Security Incident Response Team operating at the national level, led by the Minister of National Defense.
7. CSIRT NASK – Computer Security Incident Response Team operating at the national level, run by the Scientific and Academic Computer Network – National Research Institute.
8. CSIRT GOV – Computer Security Incident Response Team operating at the national level, led by the Head of the Internal Security Agency.

THE ACT ON THE NATIONAL CYBERSECURITY SYSTEM AND OTHER LEGAL REGULATIONS IN THE CONTEXT OF ENSURING STATE CYBERSECURITY

SELECTED ISSUES

Summary

The article presents changes in the Polish legal order in the aspect of ensuring the security of ICT systems and system tools with which data processing and remote services are performed. The issues related to potential threats to the proper functioning of the network and the obligations of public administration bodies in the field of cybersecurity were analyzed. Particular attention was paid to the administrative authority of entities, thanks to which they can apply appropriate protective measures. In addition, EU law is presented in relation to the Digital Single Market Strategy for Europe. The aim of the work will be to identify potential threats to cyberspace and to try to counteract them, on the example of regulations adopted by Poland. In the first part of the thesis, the matter of network security threats will be discussed, in the second — obligations of entities in the field of cybersecurity arising from legal acts. Research methods include the analysis of legal acts using the literature on the subject.

Key words: administrative authority; cybersecurity; cybercrime; globalization; system threats

USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA I INNE REGULACJE PRAWNE W KONTEKŚCIE ZAPEWNIENIA CYBERBEZPIECZEŃSTWA PAŃSTWA

ZAGADNIENIA WYBRANE

Streszczenie

Artykuł przedstawia zmiany w polskim porządku prawnym, w aspekcie zapewnienia bezpieczeństwa systemów teleinformatycznych oraz narzędzi systemowych, za pomocą których odbywa się przetwarzanie danych oraz świadczenie usług na odległość. Analizie zostały poddane zagadnienia odnoszące się do potencjalnych zagrożeń prawidłowego funkcjonowania sieci oraz obowiązki organów administracji publicznej w zakresie cyberbezpieczeństwa. Szczególną uwagę zwrócono na władztwo administracyjne podmiotów, dzięki któremu mogą zastosować właściwe środki ochronne. Ponadto przedstawiono regulacje prawa unijnego w odniesieniu do strategii jednolitego rynku cyfrowego Unii Europejskiej. Celem pracy będzie wskazanie potencjalnych zagrożeń cyberprzestrzeni oraz próby przeciwstawienia się nim, na przykładzie regulacji przyjętych przez Polskę. W pierwszej części pracy omówiona zostanie materia zagrożeń bezpieczeństwa sieciowego, w drugiej – obowiązki podmiotów w kwestii cyberbezpieczeństwa, wynikające z aktów prawnych. Metody badawcze obejmują analizę aktów prawnych z wykorzystaniem literatury przedmiotu.

Słowa kluczowe: władztwo administracyjne; cyberbezpieczeństwo; cyberprzestępczość; globalizacja; zagrożenia systemowe