Articles

Studia Iuridica Lublinensia vol. 31, 3, 2022
DOI: 10.17951/sil.2022.31.3.31-43

Małgorzata Czuryk
University of Warmia and Mazury in Olsztyn, Poland
ORCID: 0000-0003-0362-3791
malgorzata.czuryk@uwm.edu.pl

Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues

Ograniczenia w zakresie korzystania z wolności i praw człowieka i obywatela ze względu na cyberbezpieczeństwo

ABSTRACT

Human rights and freedoms may be restricted in particular circumstances. The restrictions in question are not general, as they may be applied only exceptionally for the protection of more significant interests. One interest which provides grounds for the imposition of restrictions is cybersecurity. The legislator does not explicitly define cybersecurity as a premise for restrictions on human and civil rights and freedoms, but it does permit such limitations for the sake of State security, the component parts of which include cybersecurity, which is particularly important today, in the Internet era. Threats in cyberspace can result in the enforcement of a state of exception (martial law, state of emergency, or state of natural disaster), under which the exercising of constitutional freedoms and rights may be restricted. In this event, the legislator explicitly states that actions in cyberspace which threaten certain legally protected interests are permitted to result in curbing the freedoms and rights of individuals for the purpose of restoring cybersecurity.

Keywords: cybersecurity; cyberspace; human rights and freedoms

CORRESPONDENCE ADDRESS: Małgorzata Czuryk, PhD, Dr. habil., Associate Professor, University of Warmia and Mazury (Olsztyn), Faculty of Law and Administration, Obitza 1, 10-725 Olsztyn, Poland.

INTRODUCTION

Human and civil rights and freedoms derive from inherent and inalienable human dignity, which is inviolable, and its respect and protection are the obligation of public authorities.[1] Nevertheless, this fact does not make freedoms and rights of individuals absolute. Although there are circumstances under which they may be restricted, such limitation might only be temporary, and should not violate human dignity.[2]

Article 30 of the Polish Constitution highlights, on the one hand, the importance of the principle of dignity as a link between natural law and positive (codified) law, and, on the other hand, as an axiological basis and premise for the entire constitutional order. Subsequently, the normative nature of the principle of dignity is defined, imposing on public authorities the obligation to respect and protect it against any infringements.[3]

The tendency to treat any unjust or even merely unsatisfactory event as an infringement of human dignity should be avoided. Otherwise, the constitutional protection of human dignity would be at risk of being degraded by diminishing. Constitutionally protected dignity,[4] which should be related to humanity itself (and not to the colloquial use of the term "dignity"), could be violated in a situation which is truly drastic, and which objectifies the human being.[5] Therefore, restrictions on the exercising of constitutional freedoms and rights, including those due to cybersecurity, should not be too radical, so that human dignity is not thereby infringed. Radicalness of restrictions, inadequate to the objective pursued, can lead to the transgression of human dignity, but each such case should be treated individually, taking into account the pertaining circumstances.

The possibility of restricting certain human and civil rights and freedoms is an expression of a compromise between the public interest and the interests of the individual. The legislator has defined a catalogue of fundamental rights and freedoms which may not be restricted in states of exception, and constitutes

---

[1] Article 30 of the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws 1997, no. 78, item 483, as amended), hereinafter: the Polish Constitution. By protecting human dignity, Article 30 of the Polish Constitution protects humanity. See judgment of the Supreme Court of 30 June 2021, I NSNc 191/21, LEX no. 3192196.

[2] O. Lyubchik, P. Korniienko, Z. Dzeiko, N. Zahrebelna, V. Zavhorodnii, *On the Definition, Content, and Essence of the Term "Human Rights"*, "Krytyka Prawa. Niezależne Studia nad Prawem" 2022, vol. 14(1), p. 176.

[3] L. Garlicki, *Komentarz do art. 30*, [in:] *Konstytucja Rzeczypospolitej Polskiej*. *Komentarz*, eds. L. Garlicki, M. Zubik, vol. 3, Warszawa 2016.

[4] M. Bożek, M. Karpiuk, J. Kostrubiec, K. Walczuk, *Zasady ustroju politycznego państwa*, Poznań 2012, p. 31.

[5] Judgment of the Supreme Court of 25 November 2020, I NSNc 57/20, LEX no. 3093105.

a closed list which guarantees the protection of the rights and freedoms upheld by the Polish Constitution.[6]

The author of this paper used the dogmatic-legal method. According to this approach, the legal regulations on the issues in question have been analysed. The analyses comprise both constitutional and statutory regulations. The author also uses the theoretical-legal method, according to which the restrictions of human and civil freedoms and rights are assessed. The issues discussed herein are looked into by, among others, M. Karpiuk, J. Kostrubiec, and K. Chałubińska-Jentkiewicz. The purpose of this paper is to discuss the principles for the imposition of restrictions on the exercising of freedoms and rights by individuals, due to the need to ensure the protection of cybersecurity.

CYBERSECURITY

Cybersecurity, according to the legal definition, means the resilience of information systems against any action which compromises the confidentiality, integrity, availability, or authenticity of its processed data, or of the related services provided by those systems.[7] According to the EU legislator, the security of network and information systems means the ability of network and information systems to resist, at a given level of confidence, any action which compromises the availability, authenticity, integrity, or confidentiality of stored or transmitted or processed data, or the related services offered by, or accessible *via*, those network and information systems. Hence, a network and information system should be construed as an electronic

[6] R. Kostrubiec, *Ograniczenia wolności i praw człowieka i obywatela w czasie stanów nadzwyczajnych w polskim porządku konstytucyjnym*, [in:] *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej. Wybrane zagadnienia prawne*, eds. M. Karpiuk, K. Orzeszyna, Warszawa 2014, p. 49.

[7] Article 2 (4) of the Act of 5 July 2018 on national cybersecurity system (consolidated text, Journal of Laws 2020, item 1369, as amended), hereinafter: the NCSA. For more on cybersecurity, see K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021; *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022, p. 5; M. Czuryk, *Supporting the Development of Telecommunications Services and Networks through Local and Regional Government Bodies, and Cybersecurity*, "Cybersecurity and Law" 2019, vol. 2(2), pp. 39–50; I. Hoffman, K. Cseh, *E-administration, Cybersecurity and Municipalities – the Challenges of Cybersecurity Issues for the Municipalities in Hungary*, "Cybersecurity and Law" 2020, vol. 4(2), pp. 199–211; M. Kelemen, V. Polishchuk, Ma. Kelemen, A. Polishchuk, *Reflection on the Act on Cybersecurity in Aviation Education*, "Cybersecurity and Law" 2021, vol. 5(1), pp. 129–138; I. Hoffman, M. Karpiuk, *E-administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues*, "Lex localis – Journal of Local Self-Government" 2022, vol. 20(3), pp. 628–629; O. Evsyukova, *Political Digitalisation for Ukrainian Society – Challenges for Cyber Security*, "Cybersecurity and Law" 2021, vol. 5(1), pp. 139–144; I. Hoffman, *Cybersecurity and Public Administration in the Time of Corona(virus) – in the Light of the Recent Hungarian Challenges*, "Cybersecurity and Law" 2021, vol. 5(1), pp. 145–158.

communications network; any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs the automated processing of digital data; or digital data stored, processed, retrieved, or transmitted over electronic communications networks or any device or group of interconnected or related devices for the purpose of its operation, use, protection, and maintenance.[8] So, cybersecurity protection involves counteracting threats which occur within information systems, removing any such threat, and any effects thereof.

Countering threats and removing their effects help to ensure security as a basic human need. Security is extremely important, not only in terms of satisfying social needs, but also for the undisrupted functioning of public institutions.[9] Today, one of the basic human needs encompasses cybersecurity as one of the spheres of security.

Cybersecurity is of currently major importance, and the effects of actions detrimental to it are noticeable not only in the public space, but also in the social or economic spheres. Considering the foregoing, the State must respond to cyber-attacks quickly and resolutely, constantly seeking newer protection mechanisms. Responding to the increasingly frequent threats to cyberspace, the legislator has recognized the need for the appropriate legal regulations, stipulating both proper diagnosis and effective response in the event of cyber-attacks.[10]

A system-based approach and a clearly defined purpose was adopted for cybersecurity in the NCSA, as far as the national aspect is concerned. According to Article 3 of the NCSA, the purpose of the national cybersecurity system is to guarantee cybersecurity at the national level, including the uninterrupted provision of essential services and digital services, by achieving a satisfactory level of security within the information systems used to provide these services, and ensuring incident handling.[11] Cybersecurity should guarantee an adequate level of protection of information systems, and in view of the need to ensure such a level, the freedoms and rights of individuals may be restricted in cyberspace, when such protection cannot be achieved otherwise.

---

[8] Article 4 (1–2) of the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016).

[9] M. Karpiuk, *The Provision of Safety in Water Areas: Legal Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(1), p. 82.

[10] Idem, *Organisation of the National System of Cybersecurity: Selected Issues*, "Studia Iuridica Lublinensia" 2021, vol. 30(2), p. 234.

[11] See also idem, *The Local Government's Position in the Polish Cybersecurity System*, "Lex localis – Journal of Local Self-Government" 2021, vol. 19(3), p. 611. The national cybersecurity system is an integral part of the national security system and of the European system of network and information-systems security, separated for the effective (efficient, undisrupted) performance of public tasks, essential services, and digital services through the establishment and implementation of the strategy in which the entities covered by the system fulfil the statutory duties assigned to them for the protection of the public interest. See G. Szpor, *Komentarz do art. 3*, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gruszczyńska, G. Szpor, Warszawa 2019.

THE PREMISES FOR RESTRICTIONS ON THE FREEDOMS AND RIGHTS OF INDIVIDUALS

In Article 31 (3) of the Polish Constitution, the legislator explicitly provides that restrictions on the exercising of constitutional freedoms and rights may be imposed only by statute, and only when necessary in a democratic state for the protection of its security or public order, or to protect the natural environment, health, or public morals, or the freedoms and rights of other persons. Such restrictions shall not violate the essence of freedoms and rights.[12] The premises take the form of values (interests) competing with the scope in which an individual exercises his or her freedoms and rights.[13]

It should be noted that the basic principle determining the limits of interference by public authorities in the sphere of the constitutional freedoms and rights of the human being and citizen is the principle of proportionality, which requires that this interference be moderate. This principle is expressed in Article 31 (3) of the Polish Constitution, and at the same time comprises one of the standards of a State under the rule of law. Restrictions on constitutional rights are consistent with the principle of proportionality if: 1) they facilitate the effective realization of the assumed goals; 2) they are necessary, and it is not possible to realize the given goals with less restrictive measures; 3) their effects are proportionate to the burdens they impose on the individual.[14]

When interpreting the provisions which form the legal basis of the principle of proportionality, it is assumed that the essence of this principle is the typical three-element model of the proportionality test, according to which the legal actions or measures taken are verified through the prism of the following components:[15] appropriateness (adequacy) – the action or measure is appropriate for the achievement of that objective, whereby appropriateness is achieved by stating that the measure pursues the objective imposed or protected by law, and this objective must be a public objective of significant importance; necessity (indispensability) –

---

[12] See M. Karpiuk, T. Włodek, *Wygaśnięcie mandatu wójta na skutek skazania na karę grzywny za niedopełnienie obowiązków z zakresu zarządzania kryzysowego. Glosa do wyroku Sądu Rejonowego w P. z dnia 18 kwietnia 2019 r. (II K 1164/14)*, "Studia Iuridica Lublinensia" 2020, vol. 29(1), p. 284.

[13] Judgment of the Constitutional Tribunal of 19 May 1998, U 5/97, OTK 1998, no. 4, item 46.

[14] Judgment of the Constitutional Tribunal of 20 February 2008, K 30/07, OTK-A 2008, no. 1, item 6. The requirement of necessity, as expressed in Article 31 (3) of the Polish Constitution, is satisfied when the established limitations are in accordance with the principle of proportionality. This means that: 1) the measures used by the legislators must lead to the intended purposes; 2) they must be necessary for the protection of the interest they are connected with; 3) their effects must be in proportion to the burdens imposed on the citizens. See judgment of the Constitutional Tribunal of 9 June 1998, K 28/97, OTK 1998, no. 4, item 50.

[15] M. Michalska, *Zasada proporcjonalności w orzecznictwie TK i ETPC – analiza prawno-porównawcza*, "Krytyka Prawa. Niezależne Studia nad Prawem" 2022, vol. 14(2), pp. 85–89.

meaning a situation in which actions or measures, as compared to other available means, interfere the least with the sphere of the rights of the individuals to whom they are addressed, and at the same time they pursue the objective to the greatest extent; and proportionality – in the strict sense, meaning a situation in which the relationship between the value of the effects of the application of a legal action or measure interfering with the rights of individuals, and the value of the objectives which will be pursued by that action or measure, indicates a supremacy of the value of the objectives.[16]

In the case of restrictions on human and civil rights and freedoms in the name of cybersecurity, attention should also be paid to artificial intelligence, which is closely related to cybersecurity.[17] Cyberspace is one of the domains in which artificial intelligence is prioritized, and can be used to protect it, but it can also be a source of threats. These threats might result in the necessity to restrict the rights and freedoms of individuals in cyberspace when it is impossible to ensure cybersecurity otherwise.

In the case of artificial intelligence, it is crucial that the solutions created in this field always serve the human purpose, putting human dignity and rights first.[18] Artificial intelligence is meant to serve the human purpose, and never to violate the essence of humanity. Its improper use can lead to a number of infringements, including the infringement of the right to privacy.

Article 31 (3) of the Polish Constitution indicates in a general way the possibility of restricting human and civil rights and freedoms, without specifying to which rights and freedoms it relates. It should therefore be assumed that this provision relates to all freedoms and rights of individuals. In certain cases, however, the international lawmaker clearly indicates which human rights and freedoms may be restricted, and in which situations.[19]

All people have the right to respect their private and family life, their home, and their correspondence. There shall be no interference by a public authority with the exercising of this right, except when in accordance with the law, and when it is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and

[16] Judgment of the Supreme Administrative Court of 3 September 2019, II FSK 3474/17, LEX no. 2751941.

[17] For more about artificial intelligence and its impact on cyberspace, see J. Kostrubiec, *Sztuczna inteligencja a prawa i wolności człowieka*, Warszawa 2021, pp. 18–29.

[18] Appendix to the Resolution No. 196 of the Council of Ministers of 28 December 2020 on establishing the Policy for the Development of Artificial Intelligence in Poland from 2020 (Official Gazette of the Republic of Poland 2021, item 23).

[19] A. Ponta, *Legal Instability in Cyberspace and OSCE's Mitigation Role*, "Juridical Tribune" 2021, vol. 11(3), pp. 417–418.

freedoms of others.[20] Cybersecurity (as a constituent of State and public security) constitutes a premise permitting interference by public authorities with the exercising of the right to privacy.

According to Article 10 of the Convention, everyone has the right to freedom of expression. This right shall include the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities, and regardless of frontiers. The exercising of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions, or penalties as are prescribed by law, and are necessary in a democratic society, in the interests of national security, territorial integrity, or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for the prevention of the disclosure of information received in confidence, or for the maintenance of the authority and impartiality of the judiciary. Therefore, State security, public safety, and also cybersecurity, justify the restriction of the freedom of speech.

Under Article 61 of the Polish Constitution, a citizen shall have the right to obtain information on the activities of public authority bodies, as well as persons discharging public functions. Such a right shall also include the receipt of information on the activities of self-governing economic or professional bodies, and other persons or organizational units relating to the field in which they perform the duties of public authorities and manage communal assets or property of the State Treasury. Restrictions on the right of access to public information may be imposed by statute, solely to protect the freedoms and rights of other persons and economic entities, public order, security, or important economic interests of the State. Cybersecurity, as a premise restricting access to public information, becomes particularly important in the case of the right to obtain public information where the information flow is carried out through network and information systems, especially when certain information is subject to legal protection.

Restrictions on the right of access to public information may be imposed by statute to protect security (cybersecurity); such protection is provided for classified information. Classified information is data whose unauthorized disclosure would or could cause damage to the Republic of Poland or would or could be detrimental from the point of view of its interests, including in the course of their preparation,

[20] Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, drawn up in Rome on 4 November 1950, amended by Protocols Nos. 3, 5, and 8, and supplemented by Protocol No. 2 (Journal of Laws 1993, no. 61, item 284, as amended), hereinafter: the Convention. According to Article 47 of the Polish Constitution, all persons shall have the right to the legal protection of their private and family life, of their honour and good reputation, and to make decisions about their personal life.

and regardless of the form and manner of their expression.[21] Restriction on access to such information is dictated by the protection of interests important from the point of view of the functioning of the State, which include: independence, sovereignty, the territorial integrity of Poland; security or constitutional order in the State; alliances or its international position; and the defence preparedness of the Republic of Poland. Due to the category of legally protected interests, classified information carries an appropriate confidentiality clause: "highly classified", "classified", "confidential", "proprietary". Access to such classified information allows one to know how to conduct cyber-attacks. Attacks of this type can also be carried out against ICT systems in which classified information is processed.

It should be emphasized that classified information can be made available only to a person who provides a guarantee of confidentiality, and only to the extent necessary for that person to perform work or duty in the position held, or to perform outsourced activities, as provided for in Article 4 (1) of the APCI, whereas the guarantee of confidentiality, according to Article 2 of the APCI, is the ability of a person to meet the statutory requirements to protect classified information against unauthorized disclosure, as determined under the verification procedure.

According to Article 51 of the Polish Constitution, no one may be obliged, except on the basis of statute, to disclose information concerning his or her person. Public authorities shall not acquire, collect, nor make accessible, information on citizens other than that which is necessary in a democratic state of law. However, the right of protection of personal data is affected by, among others, cybercrime. Personal data may be processed by competent authorities for the purpose of the recognition, prevention, detection, or suppression of a criminal offense, including threats to safety and public order, as well as pre-trial detention, punishments, penalties for breaches of orders, and coercive means resulting in the deprivation of liberty.[22] However, personal data may be processed only to the extent necessary for the competent authority to pursue the objective provided for by the legislator.

Personal data may also constitute criminal information, and be processed for the purposes of detecting and prosecuting offenders, and preventing and combatting crime. Criminal information shall be processed without the knowledge and consent of the data subject, and in compliance with the principles of protecting them, as laid down in the regulations on the protection of classified information. Criminal information shall be provided to authorized entities, for purposes other

[21] Article 1 (1) of the Act of 5 August 2010 on the protection of classified information (consolidated text, Journal of Laws 2019, item 742, as amended), hereinafter: the APCI.

[22] Article 1 (1) the Act of 14 December 2018 on the protection of personal data processed in connection with preventing and combatting crime (Journal of Laws 2019, item 125, as amended). See also K. Chałubińska-Jentkiewicz, M. Nowikowska, *Ochrona danych osobowych w cyberprzestrzeni*, Warszawa 2021, p. 93.

than detecting and prosecuting offenders and preventing and fighting crime, to the extent necessary to fulfill their statutory duties, in particular for the purpose of protecting safety and public order, preventing and counteracting incidents, and threats of a terrorist nature, or conducting counterterrorist activities, if these entities are authorized to process information, including personal data, included in the scope of criminal information for the purpose of fulfilling a specific duty.[23]

Personal data, including those which are processed without the knowledge and consent of the data subject, must be: 1) processed lawfully, fairly, and in a transparent manner; 2) collected for specified, explicit, and legitimate purposes, and not further processed in a way incompatible with those purposes; 3) sufficient, relevant, and restricted to what is necessary for the purposes for which they are processed; 4) correct and updated when necessary; 5) kept in a form which permits the identification of the data subject for no longer than is necessary for the purposes for which the data were processed; 6) processed in a way which ensures adequate security of personal data, including protection against unauthorized or unlawful processing, and accidental loss, destruction, or damage, by means of appropriate technical or organizational measures.[24] The restriction of the right to the protection of personal data does not release their processors from exercising due diligence and securing the data adequately; on the contrary, they are obliged to apply the best possible security measures to prevent unauthorized persons from becoming familiar with any such data, including preventing any leakage thereof through a cyber-attack.

In the case of states of exception, their implementation may be an effect of threats occurring in cyberspace.[25] Therefore, in order to restore cybersecurity, the legislator permits the introduction of certain restrictions on the exercising by individuals of their constitutional freedoms and rights, which are in force during the state of exception (martial law, state of emergency, state of natural disaster).

[23] Article 2 of the Act of 6 July 2001 on the processing of criminal information (consolidated text, Journal of Laws 2019, item 2126, as amended). See also M. Czuryk, *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015, p. 139.

[24] Pursuant to Article 5 (1) of the Regulation of the European Parliament and of the Council (EU) 2016/679 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) (OJ L 119/1, 4.5.2016).

[25] Article 2 (1) of the Act of 29 August 2002 on martial law, and on the powers of the Commander-in-Chief of the Armed Forces and the rules for his or her subordination to the constitutional authorities of the Republic of Poland (consolidated text, Journal of Laws 2017, item 1932); Article 2 (1) of the Act of 21 June 2002 on the state of emergency (consolidated text, Journal of Laws 2017, item 1928); Article 3 (2) of the Act of 18 April 2002 on the state of national disaster (consolidated text, Journal of Laws 2017, item 1897). See also M. Czuryk, *Activities of the Local Government During a State of Natural Disaster*, "Studia Iuridica Lublinensia" 2021, vol. 30(4), pp. 114–116.

CONCLUSIONS

Restrictions on the exercising of freedoms and human rights, regardless of the circumstances which justify them, should be treated as extraordinary measures. The principle is to protect the freedoms and rights of individuals; they may be restricted only under specific circumstances, with the observance of the constitutional requirements. They may not be imposed arbitrarily as a mechanism of political struggle, or as a remedy for the system's inefficiency.[26]

One of the circumstances which justifies the authoritative encroachment into the sphere of human and civil rights and freedoms is cybersecurity. Article 31 (3) of the Polish Constitution does not explicitly mention cybersecurity as a value whose safeguarding permits interference with the freedoms and rights of individuals, but this regulation refers to State security, of which cybersecurity is a constituent part, and which must be a priority now, in the world of widespread computerization. Today the Internet not only enables rapid communication, but also constitutes a source of information, or a platform for the provision of services. The protection of its users is therefore very important. The Internet brings not only the possibility of quick, easy, and cheap contact, but also threats, including those related to criminal activities, including cyberterrorism. Consequently, ensuring network security will determine the need to restrict the exercising of freedoms and rights by individuals.

Currently, network and information systems are used not only for searching for information, but also for conducting business activities, providing various services, communication, and performing public tasks; their importance for the State and the economy is in some cases strategic. Therefore, they must be duly protected, sometimes at the cost of human rights and freedoms.

REFERENCES

Literature

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

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

Chałubińska-Jentkiewicz K., Nowikowska M., *Ochrona danych osobowych w cyberprzestrzeni*, Warszawa 2021.

Czuryk M., *Activities of the Local Government During a State of Natural Disaster*, "Studia Iuridica Lublinensia" 2021, vol. 30(4), **DOI: http://dx.doi.org/10.17951/sil.2021.30.4.111-124**.

[26] See I. Hoffman, J. Kostrubiec, *Political Freedoms and Rights in Relation to the COVID-19 Pandemic in Poland and Hungary in a Comparative Legal Perspective*, "Bialystok Legal Studies" 2022, vol. 27(2), pp. 50–51.

Czuryk M., *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015.
Czuryk M., *Supporting the Development of Telecommunications Services and Networks through Local and Regional Government Bodies, and Cybersecurity*, "Cybersecurity and Law" 2019, vol. 2(2), **DOI: https://doi.org/10.35467/cal/133839**.
Evsyukova O., *Political Digitalisation for Ukrainian Society – Challenges for Cyber Security*, "Cybersecurity and Law" 2021, vol. 5(1), **DOI: https://doi.org/10.35467/cal/142199**.
Garlicki L., *Komentarz do art. 30*, [in:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, eds. L. Garlicki, M. Zubik, vol. 3, Warszawa 2016.
Hoffman I., *Cybersecurity and Public Administration in the Time of Corona(virus) – in the Light of the Recent Hungarian Challenges*, "Cybersecurity and Law" 2021, vol. 5(1), **DOI: https://doi.org/10.35467/cal/142201**.
Hoffman I., Cseh K., *E-administration, Cybersecurity and Municipalities – the Challenges of Cybersecurity Issues for the Municipalities in Hungary*, "Cybersecurity and Law" 2020, vol. 4(2), **DOI: https://doi.org/10.35467/cal/142201**.
Hoffman I., Karpiuk M., *E-administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues*, "Lex localis – Journal of Local Self-Government" 2022, vol. 20(3), **DOI: https://doi.org/10.4335/20.3.617-640(2022)**.
Hoffman I., Kostrubiec J., *Political Freedoms and Rights in Relation to the COVID-19 Pandemic in Poland and Hungary in a Comparative Legal Perspective*, "Bialystok Legal Studies" 2022, vol. 27(2), **DOI: https://doi.org/10.15290/bsp.2022.27.02.02**.
Karpiuk M., *Organisation of the National System of Cybersecurity: Selected Issues*, "Studia Iuridica Lublinensia" 2021, vol. 30(2), **DOI: http://dx.doi.org/10.17951/sil.2021.30.2.233-244**.
Karpiuk M., *The Local Government's Position in the Polish Cybersecurity System*, "Lex localis – Journal of Local Self-Government" 2021, vol. 19(3), **DOI: https://doi.org/10.4335/19.3.609-620(2021)**.
Karpiuk M., *The Provision of Safety in Water Areas: Legal Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(1), **DOI: http://dx.doi.org/10.17951/sil.2022.31.1.79-92**.
Karpiuk M., Kostrubiec J. (eds.), *The Public Dimension of Cybersecurity*, Maribor 2022, **DOI: https://doi.org/10.4335/2022.1**.
Karpiuk M., Włodek T., *Wygaśnięcie mandatu wójta na skutek skazania na karę grzywny za niedopełnienie obowiązków z zakresu zarządzania kryzysowego. Glosa do wyroku Sądu Rejonowego w P. z dnia 18 kwietnia 2019 r. (II K 1164/14)*, "Studia Iuridica Lublinensia" 2020, vol. 29(1), **DOI: http://dx.doi.org/10.17951/sil.2020.29.1.273-290**.
Kelemen M., Polishchuk V., Kelemen Ma., Polishchuk A., *Reflection on the Act on Cybersecurity in Aviation Education*, "Cybersecurity and Law" 2021, vol. 5(1), **DOI: https://doi.org/10.35467/cal/142198**.
Kostrubiec J., *Sztuczna inteligencja a prawa i wolności człowieka*, Warszawa 2021.
Kostrubiec R., *Ograniczenia wolności i praw człowieka i obywatela w czasie stanów nadzwyczajnych w polskim porządku konstytucyjnym*, [in:] *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej. Wybrane zagadnienia prawne*, eds. M. Karpiuk, K. Orzeszyna, Warszawa 2014.
Lyubchik O., Korniienko P., Dzeiko Z., Zahrebelna N., Zavhorodnii V., *On the Definition, Content, and Essence of the Term "Human Rights"*, "Krytyka Prawa. Niezależne Studia nad Prawem" 2022, vol. 14(1), **DOI: https://doi.org/10.7206/kp.2080-1084.514**.
Michalska M., *Zasada proporcjonalności w orzecznictwie TK i ETPC – analiza prawno-porównawcza*, "Krytyka Prawa. Niezależne Studia nad Prawem" 2022, vol. 14(2), **DOI: https://doi.org/10.7206/kp.2080-1084.524**.
Ponta A., *Legal Instability in Cyberspace and OSCE's Mitigation Role*, "Juridical Tribune" 2021, vol. 11(3), **DOI: https://doi.org/10.24818/TBJ/2021/11/3.01**.
Szpor G., *Komentarz do art. 3*, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gruszczyńska, G. Szpor, Warszawa 2019.

Legal acts

Act of 6 July 2001 on the processing of criminal information (consolidated text, Journal of Laws 2019, item 2126, as amended).
Act of 18 April 2002 on the state of national disaster (consolidated text, Journal of Laws 2017, item 1897).
Act of 21 June 2002 on the state of emergency (consolidated text, Journal of Laws 2017, item 1928).
Act of 29 August 2002 on martial law, and on the powers of the Commander-in-Chief of the Armed Forces and the rules for his or her subordination to the constitutional authorities of the Republic of Poland (consolidated text, Journal of Laws 2017, item 1932).
Act of 5 August 2010 on the protection of classified information (consolidated text, Journal of Laws 2019, item 742, as amended).
Act of 5 July 2018 on national cybersecurity system (consolidated text, Journal of Laws 2020, item 1369, as amended).
Act of 14 December 2018 on the protection of personal data processed in connection with preventing and combatting crime (Journal of Laws 2019, item 125, as amended).
Appendix to the Resolution no. 196 of the Council of Ministers of 28 December 2020 on establishing the Policy for the Development of Artificial Intelligence in Poland from 2020 (Official Gazette of the Republic of Poland 2021, item 23).
Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws 1997, no. 78, item 483, as amended).
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016).
European Convention for the Protection of Human Rights and Fundamental Freedoms, drawn up in Rome on 4 November 1950, amended by Protocols Nos. 3, 5, and 8, and supplemented by Protocol No. 2 (Journal of Laws 1993, no. 61, item 284, as amended).
Regulation of the European Parliament and of the Council (EU) 2016/679 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) (OJ L 119/1, 4.5.2016).

Case law

Judgment of the Constitutional Tribunal of 19 May 1998, U 5/97, OTK 1998, no. 4, item 46.
Judgment of the Constitutional Tribunal of 9 June 1998, K 28/97, OTK 1998, no. 4, item 50.
Judgment of the Constitutional Tribunal of 20 February 2008, K 30/07, OTK-A 2008, no. 1, item 6.
Judgment of the Supreme Administrative Court of 3 September 2019, II FSK 3474/17, LEX no. 2751941.
Judgment of the Supreme Court of 25 November 2020, I NSNc 57/20, LEX no. 3093105.
Judgment of the Supreme Court of 30 June 2021, I NSNc 191/21, LEX no. 3192196.

ABSTRAKT

Ograniczenie korzystania z wolności i praw człowieka może mieć miejsce w szczególnych okolicznościach. Nie ma ono charakteru powszechnego, może być stosowane wyjątkowo dla ochrony dobra oczywiście ważniejszego. Takim dobrem, które uzasadnia wprowadzenie stosownych ograni-

czeń, może też być cyberbezpieczeństwo. Ustrojodawca nie określa wprost cyberbezpieczeństwa jako przesłanki ograniczenia wolności i praw człowieka i obywatela, lecz dopuszcza takie ograniczenie ze względu na bezpieczeństwo państwa, którego elementem składowym jest też cyberbezpieczeństwo, mające zwłaszcza dzisiaj, w dobie Internetu, szczególne znaczenie. Zagrożenia w cyberprzestrzeni mogą skutkować wprowadzeniem stanu nadzwyczajnego (stanu wojennego, wyjątkowego czy też klęski żywiołowej), w ramach którego dopuszcza się ograniczenie korzystania z konstytucyjnych wolności i praw. W tym przypadku ustawodawca wprost stanowi, że działania w cyberprzestrzeni zagrażające określonym dobrom prawnie chronionym mogą skutkować wprowadzeniem ograniczeń wolności i praw jednostki, a celem będzie przywrócenie cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo; cyberprzestrzeń; wolności i prawa człowieka