Przegląd Prawa Konstytucyjnego
-----ISSN 2082-1212-----
DOI 10.15804/ppk.2019.05.21
-----No. 5 (51)/2019-----

Katarzyna Chałubińska-Jentkiewicz[1]

Cybersecurity as a Premise for Restrictions of the Right to Privacy as a Constitutional Value

Keywords: security, right to privacy, Constitutional values, public order, cybercrime
Słowa kluczowe: bezpieczeństwo, prawo do prywatności, wartości konstytucyjne, porządek publiczny, cyberprzestępstwo

Abstract

In this article the author analyzes various legal aspects necessary for maintaining the rights of citizens to live in a free, safe and democratic state of contemporary digital era. She presents philosophical and legal origins of the rights to privacy and the development of the concept in different countries with a particular emphasis of its place in the digital world of modern democracies. She tries to show the importance of this concept as the premise for national security and compares legal solutions in different countries all over the world. It makes the article important because her interests go into comparing and finding not only the best examples and legal cases but practical knowledge which may be used in academic work and research.

Streszczenie

Cyberbezpieczeństwo jako przesłanka ograniczeń prawa do prywatności jako wartości konstytucyjnej

W artykule autor analizuje różne aspekty prawne niezbędne do utrzymania prawa obywateli do życia w wolnym, bezpiecznym i demokratycznym państwie współczesnej ery

[1] ORCID ID: 0000-0003-0188-5704, Ph.D., D.Sc., Department of Media Law, Intellectual Property and New Technologies, Institute of Law and Defense Administration, Faculty of National Security, The War Studies University, e-mail: kasiachalubinska@gmail.com.

cyfrowej. Przedstawia filozoficzne i prawne źródła prawa do prywatności oraz rozwój koncepcji w różnych państwach, ze szczególnym uwzględnieniem jej miejsca w cyfrowym świecie współczesnych demokracji. Próbuje pokazać znaczenie tej koncepcji jako przesłanki bezpieczeństwa narodowego i porównuje rozwiązania prawne w różnych państwach na całym świecie. To sprawia, że artykuł jest ważny, ponieważ jego treścią jest porównywanie i wskazywanie nie tylko najlepszych przykładów i spraw prawnych, ale praktycznej wiedzy, którą można wykorzystać w pracy naukowej i badaniach.

*

I. Introduction

The right to privacy is not an absolute freedom. The specificity of restrictions on the right to privacy includes, first of all, the concept of openness of public life, referring to persons who perform public functions or have public welfare at their disposal. The Constitutional Tribunal pointed out this fact in its judgment of March 5, 2013, file reference number U 2/11[2]. According to the Tribunal, this means that even such exceptional and extreme conditions do not allow the legislator to soften the premises under which one can enter the sphere of private life, thus not risking the accusation of unconstitutional arbitrariness. The above led the Constitutional Tribunal to the conclusion that this freedom must be limited by an act having the legal rank, especially in the reality of criminal proceedings, which interferes most deeply with constitutional freedoms and civil rights. It should be mentioned that the catalog of such persons should include all persons performing the so-called "public service". This was also clearly emphasized by the Constitutional Tribunal, stating that privacy of such persons is subject to less protection due to the fact that information related to performing public functions is not excluded from the scope of the said right to the public information.

It should be noted that any right or freedom expressed in the Constitution of the Republic of Poland may be subjected to restrictions resulting from the Article 31 clause 1 of the Constitution of the Republic of Poland. It should

[2] Dz.U. 2013, item 375.

be emphasized that in addition to the Article 31 clause 3 of the Constitution of the Republic of Poland, restrictions on freedom and rights may be introduced in the state of emergency, based on the regulation of the Article 233 of the basic act (and possibly based on special provisions usually accompanying the regulation of a very specific right or freedom, i.e. for example the Article 48, 49, 50 of the Constitution of the Republic of Poland). It is also worth to note other restrictions on the right to privacy which result from the Article 45 of the Constitution of the Republic of Poland. This provision states the right to court proceedings and, i.a., provides an open consideration of the case.

Restrictions on the rights and freedoms of an individual – a citizen – may be introduced in the situation of specific premises. These include security, public order, health, environmental protection, public morality, and freedoms and rights of others. In the judgment of June 29, 2001[3], the Constitutional Tribunal stated that the Article 31 clause 3 of the Constitution of the Republic of Poland formulates the cumulative premises for the admissibility of restrictions in exercising constitutional rights and freedoms, and the limits of interference with constitutional rights and freedoms are determined by the principle of proportionality and the concept of the essence of individual rights and freedoms. "To say that restrictions may only be set if they are necessary in a democratic state, we must consider: whether the introduced regulation is capable of achieving its intended effects; whether this regulation is necessary to protect the public interest with which it is connected; whether the effects of the introduced regulation are in proportion to the burdens it imposes on a citizen". The provision of the Article 31 clause 3 of the Constitution of the Republic of Poland, introduces the obligation of a statutory regulation. This means that restrictions may only be established in the form of an act and the permissible interference of the public authority with fundamental rights must be based on a statutory regulation. This does not mean, however, that the limitation of constitutional rights and freedoms is to result from the law. It should also be emphasized that the restrictions relate to the exercise of rights and freedoms itself, and the provision of the Article 31 clause 3 of the Constitution of the Republic of Poland does not sanction the general liquidation of these rights and freedoms in a specific situation in which

[3] File ref. No. K 23/00, OTK ZU No. 5/2001, item 124.

there occur premises for the restrictions. The restrictions on rights and freedoms, however, require an assessment of their necessity. It should be noted that in the light of the foregoing judicial decisions of the Constitutional Tribunal, more strict standards for assessing the admissibility of restrictions should be applied to the regulation of personal and political rights and freedoms than to economic and social rights. Therefore, this applies in particular to the right to privacy expressed in the Article 47 of the Constitution of the Republic of Poland.

II. The right to privacy

Luis D. Brandeis and Samuel D. Warren are two the most frequently mentioned names in publications devoted to the right to privacy. In the famous article *the Right to Privacy*, published in issue No. 4 of "Hardward Law Review", which was published on December 15, 1890, these authors had set the framework for the subject under examination for the first time. Sources of privacy may be sought in various types of messages or philosophical and legal concepts. Depending on the adopted concept of privacy – some attribute privacy as a trait inseparable from a man, accompanying him always, although not always in a conscious way. Other concepts of privacy refer to the genesis in the seventeenth and eighteenth-century considerations on the law of freedom and nature. And so, the supporters of the first position point out that the first sources of privacy can already be found in the Hammurabi code and the Bible, while others believe that the right to privacy stemmed from the ideas presented by Hobbes, Grotius, Locke, Montesquieu and J.J. Rousseau. The formal and legal protection of privacy does not have a long tradition, because it was born in the last 100 years. Privacy can be defined in many different ways. In narrow terms, it is a state within which an individual decides about the range and scope of information shared and communicated to others. In a broader sense, it is a state in which an individual makes decisions which relate to the very person without the interference of third persons. M. Jabłoński describes privacy as the sum of various values which make up the understanding of the autonomy of individual that lives in a given reality in relation to other individuals, as well as their communities and the state itself and its officers.

J. Braciak, in turn, notes that privacy is closely connected with the concept of self-interest of an individual, its welfare and with the activity undertaken by an individual for the protection of such a welfare, contrary to the activity undertaken for the public welfare[4]. K. Motyk distinguished four basic types of defining privacy, which are reflected in the positions mentioned above: privacy as the right to control information about oneself, privacy as the right to be left alone, privacy as the autonomy of an individual, and privacy as the control of access to a person[5]. The concept of privacy is associated with such concepts as: protection of identity, immunity of residence, confidentiality of correspondence, personal immunity, protection of property, etc. In the literature it is argued that the right to privacy has been valued as an expression of an increasingly widespread sense of individuality, uniqueness and distinctness of an individual. The issue of privacy is also subject to restrictions justified by cyber security.

III. The premise of security

Public security, to which a number of ordinary acts refer, which is also mentioned in the Constitution of the Republic of Poland, is a state in which the society and its interests, as well as the state together with its goals, are protected against damage threatening them from any source. According toW. Kawka, public security includes the security not only of the citizens of a given state and representatives of a particular nation, but also refers to the interests, tangible and intangible assets of foreign entities covered with the protection of a given state. This concept includes a positive state which experiences protection consisting in reversing damages threatening from any source, thus it is a welfare protected by law. Nowadays, we talk about national security as a system covering a number of different types of security, which includes public security in its scope and in this aspect, it also includes protection of the representatives of national minorities. The legislator, referring to the restrictions on the rights and freedoms of an individual – citizen, referring to the

[4] Ibidem, pp. 59–61.

[5] M. Vall, E. Nowińska, *The Act on combating unfair competition. Commentary,* Warsaw 2013, pp. 78–80.

premise of security, did not specify in detail the kind of security concerned. It should be assumed, however, that the legislator intentionally used the concept of "security" without limiting himself to the concept of "the public security" or "the state security", giving this value a general character. Thus, in the catalog of this concept we may use a definition. According to the definition of J. Marczak "the national security is the highest need and value of the nation and the main purpose of the activities of a state", while the national defence performs the function of protecting and defending national values against external and internal, military and non-military[6] threats, ensuring material and cultural development. Based on this definition, it is easy to draw a thesis that the national security is a condition in which a state, as part of its defence and protection functions, has a duty to ensure security by counteracting external and internal threats, public order and peace, including an individual peace. W. Kitler emphasizes that the national security as a national value (and also a national goal) permeates other goals according to the principle that goals become impossible to achieve without not feeling threatened. "Possessing even the most valuable material or intellectual value loses its importance if there is no security"[7]. In this definition, we can say that the primary purpose of the state is to ensure security also by ensuring peace and public order. For this reason, the words of W. Kawka should be recalled that "security, peace and public order present a kind of connection with each other, similarity of nature and mutual dependence, as a result of which they form a whole; therefore, the state's activity regarding the protection of security, peace and public order may, from the practical point of view, be considered a separate branch of the state activity, especially if it is taken into account as a necessary requirement for human coexistence. Maintaining and protecting these states requires systematic supervision and vigilance"[8].

In this context, the definition of the security premise should be extended to include all conditions that enable proper functioning of the state and

[6] J. Marczak, *Universal protection and national defence,* [in:] *Fundamentals of Poland's national security in the era of globalization*, eds. R. Jakubczak, J. Marczak, K. Gąsiorek, W. Jakubczak, Warsaw 2008, p. 164.

[7] W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system,* Warszawa 2011, p. 29.

[8] W. Kawka, *Policja w ujęciu historycznym i współczesnym*, Wilno 1939, p. 21.

an individual, and their proper development. The degree of the national security will be affected by the degree of protection of the public morality, national identity, cultural heritage and all other values important for the protection of the nation, state and the individual, including health protection, environment and provision of education, and the right to work. This protection sphere includes all the rights and freedoms of the individual – a citizen with the right to dignity at the forefront. The need to ensure security justifies the need to protect values such as public morality, fundamental rights and freedoms, the national heritage, etc. This approach includes protection of all other values as the superior value. Ensuring security remains in the public interest as an overriding goal. It is an unchanging value, however, as it has already been presented while discussing the scope of protection of fundamental rights and freedoms, the legal system itself, i.e. a protection tool that depends on the adopted state system, is subject to change. Protection is closely related to the police function of the state, because it was introduced, among others, to protect public peace and security[9]. Therefore, it should be assumed that the protection of fundamental rights and freedoms is an objective in ensuring security, while security can be a premise for restrictions on these rights and freedoms in accordance with the concept of a democratic rule of law. This relationship is closely related to the conflict regarding the relationship between an individual – citizen and the public authority. Ensuring security is aimed at protecting rights and freedoms while, at the same time, limiting rights and freedoms to protect security. However, the opposite cannot be the case, since the protection of rights and freedoms is included in an unspecified and non-exhaustive catalog of security-related objectives. It should be emphasized that the restrictions refer to the issue of exercising rights and freedoms. The principle of proportionality defined in the Article 31 clause 3 of the Polish Constitution, formulates cumulative premises for the admissibility of restrictions on exercising constitutional rights and freedoms. These are: the statutory form of restriction, existence of the need to introduce it in a democratic state, the functional relationship of restriction with the implementation of such values as: state security, public order, environment protection, public health and morality, freedom and rights of others. An important

[9] Ibidem, p. 23.

premise is the prohibition of violating the essence of a given right and freedom. The catalog of premises for the limitation of freedoms and rights listed in the Article 31 clause 3 of the Constitution of the Republic of Poland is closed and cannot be interpreted broadly. The Article 31 clause 3 of the Constitution expresses the principle of proportionality, which becomes the basis for determining the framework of the regulatory freedom of the ordinary legislator. In case of a conflict between two constitutionally protected rights, it is necessary to balance the protected interests in accordance with the principle of proportionality[10].

IV. The premise of public order

Public order should be understood as all forms enabling the normal development of life in a state[11]. The notion of public order consists of a number of legal and moral norms which guarantee the proper functioning of the state.

According toW. Kawka, ethics, customs, decency, aesthetics, etc. are shaped in every society, with political, religious, ethnic and economic moments and a degree of cultural development playing an important role. According to this author, "a collective whole with all its properties is reflected in the social views. The development of the human spirit changes the conditions of living and with them the law and the social views, therefore, the content and public order cannot be determined once and for all, it does not remain the same forever, that is it is variable. A place, circumstances, environment and similar circumstances have a decisive influence on the content of the notion of public order". As a vague term, it can be defined by referring to the policy adopted in the state, the legal norms as well as rules and principles governing a given community. It should be emphasized that an attribute of public order is effective functioning of public authorities.

The use of the term public security, which under the national law is used interchangeably or jointly and referred to as public security and order, guar-

[10] Judgments of the Constitutional Tribunal dated: April 19, 2005, file ref. No. K 4/05, OTK ZU No. 4/A/2005, item 37; dated January 10, 2012, file ref. No. SK 25/09, OTK ZU No. 1/A/2012, item 1.

[11] W. Kawka, op.cit. p. 67.

antees the individual's right to safe living conditions, while determining an undisturbed functioning of the state and its institutions. Public security is a condition enabling the normal functioning of institutions carrying out tasks which purpose is to protect the interests of the state, protection of the human life, health and property, while ensuring respect for the constitutionally granted rights and freedoms of an individual. Public order is adherence by the citizens to the adopted behavior patterns in generally accessible (public) places. Both defined concepts are closely related, as the protection of public security is conducive to forming principles ensuring order. However, enforcement by the state of behaviors consistent with the accepted legal norms and principles of social coexistence is conducive to maintaining public security.

The national security is about successful existence and development, and the protection of values close to all members of a given community, including i.a. the quality of life, social solidarity, human rights, culture, customs, traditions and national identity. According toW. Kitler, the national security is the most important value, the national need and the priority objective of the activities of the state, individuals and social groups, and, at the same time, a process encompassing various means which guarantee lasting, interference-free existence and national (state) development, including protection and defence of the state as a political institution and protection of individuals and the whole society, their goods and the natural environment against threats that significantly limit its functioning or threaten goods subject to special protection[12].

The issue of legal restrictions on the protection of personal data looks slightly different. Admittedly, as in the case of the Article 47 of the Constitution of the Republic of Poland, this right is not listed in the catalog of the Article 233 of the Constitution of the Republic of Poland and thus is subject to the general rules established pursuant to the Article 31 clause 3 of the basic act (the rights and freedoms of third parties), but at the same time the Article 51 clause 2 of the Constitution of the Republic of Poland cannot be overlooked. As indicated byA. Mednis, the system-former regulates in this provision the issues of data processing both by private entities and public authorities. Clauses 2 and 3 of this Article are addressed to public authorities. They define the

[12] Ibidem, p. 23.

entitlement of public authorities toward the Polish citizens, related to the opportunity to acquire, collect and share information about them. For it may only be the information which is necessary in a democratic state ruled by law. The existence of such a special regulation is important because it constitutes an access barrier to the information about an individual convenient for the public authority, because of the collection of which it can confirm its dominant position in relation to the individual. Normative separation, establishment in the Article 51 clause 2 of the Constitution of the Republic of Poland of a separate ban – it facilitates noticing this violation and simplifies the subject of evidence that such violation has occurred. For the subject of evidence is only whether obtaining of the information was necessary or only convenient or useful to the authority. Therefore, the Constitution of the Republic of Poland has two types of restrictions here. First, regarding the form – the obligation to provide data must be introduced in the form of an act. Second, as regards the matter – the obligation is justified only to the extent to which it is necessary in a democratic state ruled by law. It may be problematic to indicate the information that should be considered necessary. It may be assumed that it will be such information, without which public authorities will not be able to take (terminate) actions regarding the competences assigned to them. It is also necessary to refer here to the values that were indicated in Article 31 clause 3132. Thus, the assessment whether the legislator observed the normal principle of proportionality regarding the chance of obtaining information about citizens by public authorities or not should and may be carried out on the basis of co-applied provisions of the Article 51 clause 2 and Article 31 clause 3 of the Constitution. In addition to the need to indicate the interest included in the catalog, which is contained in the Article 31 clause 3 of the Constitution, the premise for the legality of encroachment on the information autonomy of the individual is the statement that the introduced legislative regulation may lead to the intended effects (the principle of usefulness), it is necessary to protect the public interest with which it is associated (the principle of necessity), and its effects remain in proportion to the burdens that it imposes on the citizen (that is, the principle of proportionality in the strict sense of the word). The position expressed through the Constitutional Tribunal must be approved. Although the necessity clause itself in a democratic state of law certainly includes in itself also all the values expressed in the

Article 31 clause 31 of the Constitution of the Republic of Poland. Ultimately, it should also be stated that Article 51 clause 2 also constitutes a premise in respect to the restriction of the right to privacy. The relationship between the right to privacy and the law regulating the protection of personal data should also be indicated.

The network availability provides many opportunities for development. A perception of communication and information network as a place of implementation of aspects of everyday life. The myth of being anonymous is always alive in the minds of the users. One has to realize that being anonymous on the web is virtually impossible. One may use masking software or data encryption, but the human in the network – the user – will always leave a trail behind, which will enable to prove signs of activity. There is a real danger of surveillance by criminals as well as by services responsible for ensuring security and protection of important state interests and respect for the established law. Of course, the line between the need to ensure security and unlawful interference in the rights and freedoms of an individual is in this case incredibly thin. The network users are very sensitive to attempts of tracking their activities, however, the question is how to properly ensure security without being able to collect information about the possibility of its occurrence. The judgment of the Polish Constitutional Tribunal on data retention regulates an important, from the point of view of the natural law, issue of informing concerned entities about the control undertaken against them. Tampering without proper authorization is prohibited, additionally, the user should be informed about the carried-out activities, immediately after their completion. It is not allowed to use these data as evidence in court cases without the user's knowledge. The efforts taken to obtain information have always been on a thin line between the necessity and lawlessness. The process of fighting cybercrime using secret services is a very complex process, in which one balances on the fine border of the user's privacy and the need to ensure security. It should also be taken into account that operational activities do not gain legitimacy if they detect a crime and at the same time violate the rights and freedoms of an individual.

Secret services and other organizations established to fight cybercrime derive their powers from the possibility given to them to undertake operational activities in this area. Interpol gave the foundations for the legal regulations in

this respect, becoming the first international organization to notice a dynamically developing cybercrime market. The law established so far does not give police clear guidelines and specified mechanisms to fight cybercrime. Additionally, the penal and procedural regulations developed so far are not gathered in one systemic and comprehensive legal act. These regulations are scattered, which additionally hinders efficient operation and detection of crimes committed online. Interpol and national services must cooperate closely, exchange information and experience, create a common and consistent system of protection against online threats.

It should be noted that these data can be made available only on the basis of a legitimate request, i.e. through court proceedings to which they are relevant. Such access must usually be made on the basis of an order or request from the party concerned. Otherwise the service provider is obligated to protect these data. In compliance with the provisions of the act, these data are to be kept for a period of 12 months from the moment they were obtained. The process of collecting and storing telecommunications data, commonly known as *data retention*, raises a lot of controversy because it is inevitably connected with the concept of web anonymity and literally refutes it. Data retention is a process in which a telecommunications service provider is required by law to store information about connections made by the user. *In fact,* it collects information on the use of the network by its recipients. These data must by law be made available to the authorized bodies as need be to detect and combat cybercrime[13].

The problem of data retention found its way in the form of a judgment passed by the Constitutional Tribunal on July 30, 2014, file reference number K23/11. This judgment deals directly with two key features of the web anonymity. Firstly, collecting data about the user, the scope and manner of their acquisition, i.e. retention, and secondly, with the type of data collected and their destruction if they do not correspond to the profile of the case in process[14]. Additionally, the need to inform the network user about the *ex post surveillance,* i.e. upon its completion, has been stated. The judgment refers direct-

[13] The Article 180 of the Act of July 16, 2004 – Telecommunications Law (Dz.U. 2018, item 1954).

[14] Judgment of the Constitutional Tribunal of July 30, 2014 file ref. No. K23/11 (Dz.U. 2014, item 1055).

ly to the provisions contained in the Telecommunications Law, acts regarding secret services, police and the Military Police, regarding the possibility of obtaining data on the entity against which the services conduct operational activities aimed at determining the commitment of crime. Until now, the Act did not stipulate the need to inform the entity under surveillance about the surveillance process it underwent.

After careful analysis of the raised objections, the Constitutional Tribunal has determined several key points[15]: one cannot freely create a law which interferes with constitutionally protected freedoms and rights, the concept of "an operational surveillance" is too vague when it comes to restrictions on the way data are obtained and what data can be obtained, provisions should be created to guarantee independent control over the sharing of data coming from retention, immediate destruction of the data subject to evidence bans should be guaranteed collectively and under a protocol. This judgment touches a very sensitive matter which is privacy and the fight against crime carried out by secret services. The Constitutional Tribunal was favourable toward the applicant in this case. It is true that some of the powers granted to secret services are controversial, especially if they affect the sphere of privacy and freedom of an individual. The discrepancy between what the secret services may do to fight crime and how they do it has always been the subject of controversy. On the one hand, the legislator has equipped the secret services with several tools to execute tasks in the field of crime detection. On the other hand, the Constitutional Tribunal stated that the powers conferred were contrary to the Constitution. One should remember that secret services and other police units act as if automatically within the limits and in accordance with the law. Their activities are based on the laws and restrictive clauses created especially for them[16], The Constitutional Tribunal does not seem to notice this dependence. Of course, the fact that protection of citizens' rights is a constitutional priority is not to be disputed.

Operational surveillance, which will be discussed later in this study, is the main tool for the secret services in question so that they can best ensure protection and respect for security. The Constitutional Tribunal has found

[15] Ibidem.

[16] M. Bożek, *Normative aspects of the state security system in emergency situations of political and military nature,* Lublin 2004.

a great deal of vagueness and freedom given by the operational surveillance. The catalog of measures which can be taken as part of the operational surveillance carried out by the services is a closed catalog. Secret services operate only within the limits and in accordance with the law. Sometimes their actions may raise various controversies. It should be taken into account that the secret services must be governed by the principle of proportionality when it comes to the actions taken.

Apart from the legal aspect, the conflict raised by the Constitutional Tribunal in this judgment concerns a very delicate area of ethics. Secret services have always balanced on the border when it comes to respecting the right to privacy. Looking at the activities undertaken by secret services, one should always ask the question whether the security of the state or peace and privacy of its citizens are more important. This topic is under constant discussion.

The problem of mass surveillance, which characterizes the functioning of the modern media, especially social media, which affects an unspecified group of people has been discussed in the ETPC/ECtHR judgment in the case of Klass and others vs. Germany[17], in which the plaintiffs were five German lawyers. The ruling in the Klass and others case has retained its precedent nature for the last almost twenty years. The subject of the consideration was the definition of the victim of a violation of the Convention entitled to lodge a complaint; admissible limits of violation of the right to privacy and the notion of the right to effective means of protecting the rights protected in the Convention. In that judgment, the tribunal acknowledged that an individual may, under certain conditions, claim to be a victim of a violation caused by the mere existence of the secret measures or legislation which authorize the use of the secret means – without having to prove that such measures have actually been used against them. The Tribunal emphasized that when the state orders the use of covert surveillance measures and when it is to re-

[17] Publications de la Cour européenne des droit de l'homme. Série A: Arretts et décisions, vol. 28. Affairre Klass et autres: 1. decision du 18 Novembre 1977; 2. Arret de 6 Septembre 1978. Greffe de la Cour. Conseil de l'Europe, Carl Heymanns Verlag: Cologne, Bonn, Munich 1978, pp. 36; Cour européenne des droit de l'homme. Affairre Klass et autres. Arret, Conseil de l'Europe: Strasbourg 1978, pp. 30; Application No. 5029/71: Gerhard Klass and others v/the Federal Republic of Germany, in: Decisions and Reports, vol. 1, Council of Europe, European Commission of Human Rights: Strasbourg 1975, pp. 20–30.

main a secret to the persons under surveillance and when they are not entitled to a legal remedy against such an order, the content of the Article 8 of the Convention protecting the right to privacy would largely be fiction. In such a situation, an individual may be treated in a manner contrary to Article 8 or even may be deprived of the right guaranteed in this provision without being aware of this fact and therefore, without the ability to use a legal remedy, whether at the national level or before the bodies of the Convention. As long as the decision of the authority entitled under the act to apply and adjust surveillance of correspondence, mail or telecommunications, remains bindingly secret toward the person concerned, this decision is excluded, under the protection guaranteed by the Article 6 of the Convention, from the judicial control undertaken at the request of that person and – as a consequence – it slips out, out of necessity, from the requirements specified in this provision.

The German Government raised the need for an effective action while justifying the rule of keeping confidential the fact of ordering control of the correspondence, mail and communication of certain persons "[...] therefore notification of such a person is not an option". At the same time, the government admitted that a person's unsatisfactory appeal to the Committee gave him/her the opportunity to lodge a complaint with the Constitutional Tribunal. The Tribunal may refuse to consider the complaint as unfounded but may also ask the Government to provide data or documents relevant to the case. The authorities are required to respond to such a request, even if the message requested is confidential. It is therefore at the discretion of the Tribunal to decide whether such a message or document may be used in the case; it may declare with two-thirds of the votes that this would not be compliant with state security and dismiss the complaint on this basis (Article 26 § 1 of the Act on the Constitutional Tribunal)[18].

The Federal Constitutional Court (BVG) has ruled that the provision of Article 1 § 5 clause 5 of the said Act is contrary to the Article 10 § 2 of GG[19]

[18] Basic Law for the Federal Republic of Germany (GG) Federal Law Gazette I, p. 2438. Neither entry into force on May 24, 1949 of the Basic Law (Grundgesetz – GG) of the Federal Republic of Germany, nor the establishment of this state on September 20, 1949, changed this state of affairs.

[19] Gesetz zur Beschhränkung des Brief, Post- und Fernmeldgeheimnisses, in Germany known as G 10 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses in Ger-

because it prohibits informing the person concerned of the measures taken against him/her, even if this would not affect the interests of the investigation. The remaining parts of the applicants' complaint were dismissed. BVG assumed that the remaining provisions of the Act were justified by the protection of the Federal Republic and its independence, democratic constitutional order and that they do not violate basic constitutional principles. The Tribunal acknowledged that: "Constitutional provisions should not be interpreted in isolation, but rather in a manner consistent with the basic principles of the GG and its system of values". [...] In the context of this case, it is particularly important that the Constitution favours protecting the concept of a "militant democracy", and therefore does not protect attacks against fundamental rights or the liberal order of the state.

The European Commission of Human Rights has also stated in its opinion in response to the question whether there has been violation of the Article 8 of the Convention. This is the key question of this matter. The Tribunal emphasizes that when the State orders the use of covert surveillance measures and when it is to remain a secret to the surveyed persons and when they are not entitled to a legal remedy against such an order, the content of Article 8 would be largely a fiction. In such a situation, an individual may be treated in a manner contrary to Article 8 or even be deprived of the right guaranteed in this provision without being aware of this fact and thus without the ability to use a legal measure, whether at national level or before the Convention bodies. The Court finds that it is not acceptable to ensure that the exercise of the right guaranteed in this Convention could be repealed by the mere fact of keeping the person concerned ignorant of its violation. As to the alleged violation of Article 8 in the applicants' opinion, the appealed Act, without providing for informing the person concerned about the surveillance measures and has no right of recourse to the court when they are no longer applied, violates the Article 8 of the Convention, according to which: "1. Everyone has the right to respect for his private and family life, his home and correspondence. 2. There shall be no interference by a public authority with the exercise of this right except those cases provided for by the act and nec-

man, is a German federal law that regulates the surveillance powers of Germany's intelligence agencies. The Act limited the confidentiality of correspondence, mail and telecommunications (pursuant to the authorization conferred by the provision of the Article 10 of GG).

essary in a democratic society on account of the state security, public security or the economic welfare of the country, prevention of order and counteracting crime, protection of health and morality or protection of rights and freedoms of others". Pursuant to provision 10 § 2 of the GG, restrictions on restricting confidentiality of correspondence, mail and telecommunications may only be imposed in accordance with an act. The Article 1 § 1 of G10 allows specific authorities to open and check correspondence and postal items, read telegrams, and control and record telephone conversations. Therefore, the Tribunal's examination was limited to these measures and not, for example, to covert surveillance carried out in accordance with the Code of Criminal Procedure. The Commission stated in its report that covert surveillance provided for in the German legislation system constitutes interference with the exercise of the right specified in Article 8 § 1. Furthermore, the very existence of such legislation is relevant to all those who are threatened with its application; this threat inevitably violates the freedom of communication between users of postal and telecommunications services, thus constituting "interference by public authorities" in the applicants' exercise of their right to private life, family life and correspondence. While assessing the scope of protection offered by Article 8, the Tribunal must consider two important facts. The first one is the technical progress made in both espionage and surveillance; the second is the development of terrorism in Europe in the recent years. Modern democratic societies are threatened with sophisticated forms of espionage and terrorism. Consequently, the state must be able to effectively oppose such threats and must be able to carry out undercover control of subversive elements operating on its territory. The Tribunal must therefore accept that the existence of provisions conferring powers to an undercover surveillance of correspondence, postal items, telephone calls is – in exceptional situations – necessary in a democratic society in the interest of the national security and/or to prevent riots or crime. The surveillance system created by Act No. 10 excludes judicial supervision, replaced by the initial supervision by an official with judicial qualifications combined with the supervision by the Commission and the Committee. The Tribunal is of the opinion that in the area where, in specific cases, abuse can be extremely easy and where such abuse may have extremely harmful consequences for a democratic society as a whole, the solution desirable as a rule is to entrust the supervision

to a judge. Nevertheless, given the nature of the supervisory and other guarantees provided for in the Act No. 10, the Tribunal concludes that the exclusion of the judicial supervision does not exceed the limits of what may be considered necessary in a democratic society. The Bundestag Commission and the Committee are independent of the authorities applying communication surveillance, and have sufficient powers and competences to exercise effective and continuous supervision. Furthermore, their democratic nature is reflected in the balanced composition of the Commission. This body represents an opposition, which may thus participate in the supervision of the measures applied by a competent minister responsible to the Bundestag. Given the circumstances of the present case, it can be assumed that both bodies have sufficient independence to be able to issue objective decisions. Furthermore, the Tribunal states that an entity convinced of subjecting it to surveillance may submit a complaint to the Committee and apply to the Constitutional Tribunal. However, as the Government acknowledges, these measures are admissible only in exceptional circumstances. Regarding *a posteriori* supervision, it should be determined whether the judicial supervision – in particular involving an individual – should be excluded after cessation of surveillance.

The Tribunal is of the opinion that in the circumstances of the case under consideration, the challenged Act is not contrary to Article 8 in authorizing the use of undercover surveillance of correspondence, mail and telecommunications, as already stated above. Since the Tribunal has already come to such a belief, the question whether the decisions authorizing such surveillance under the challenged Act are included in the judicial guarantee as defined in Article 6 – assuming that this provision applies here – it must be examined by removing a distinction between two stages: this procedure – before and after notification of the end of applying the surveillance. As long as it remains bindingly secret, the decision to subject someone to surveillance is excluded from the judicial control undertaken at the motion of a person concerned – under the provisions of Article 6; as a consequence, it slips out, out of necessity, from the requirements specified in this provision. The decision may fall within the protection of Article 6 only after discontinuing the surveillance. According to the information provided by the Government, an individual concerned has, at the time when he/she is notified of the cessation of surveillance, a number of legal remedies against possible violations of his/

her rights; these measures meet the requirements stipulated in this provision. Bearing this in mind, the Court recognizes [unanimously] that even if the provision of Article 6 applies here, it has not been violated in the present case.

A different position was adopted in the USA. The US Supreme Court in a precedent ruling by Amnesty v. Clapper[20] concluded that failure to demonstrate the fact that the plaintiff had been subject to surveillance measures effectively resulted in the inability to determine that he had suffered damage. The new procedures allow electronic governmental surveillance of persons outside the United States for foreign intelligence purposes. Various groupings argue that the procedures violate the fourth amendment, the first amendment, of the Article III of the Constitution and the principle of separation of powers. The new regulations would force these groups to take costly measures to ensure the confidentiality of their international communications. The Supreme Court's point of view met with criticism of part of the doctrine, which resulted in a judgment of the Federal Court of Appeals for the Fourth District in the case of Wikimedia v. NSA[21], in which the court overturned the first-instance judgment and referred the case back to the court. In the case of the Wikimedia Foundation and others vs. National Security Agency and others[22] in justification of the decision, the adjudicating panel stated that the plaintiff Wikimedia Foundation, the operator of Wikipedia, sufficiently substantiated its claim, which in this case means that it demonstrated that it could have been the subject of surveillance by the National Security Agency. Wikimedia Foundation and others vs. National Security Agency and others, is a lawsuit

[20] Article 702 – Clapper v. Amnesty – which was filled less than an hour after President Bush signed Article 702 in 2008.

[21] The original plaintiffs of the statement of claim were: Wikimedia Foundation, National Association of Criminal Defense Lawyers, Human Rights Watch, Amnesty International USA, PEN American Center, Global Fund for Women, The Nation Magazine, The Rutherford Institute and The Washington Office on Latin America.

[22] Wikimedia Foundation, National Association of Criminal Defense Lawyers, Human Rights Watch, Amnesty International USA, PEN American Center, Global Fund for Women, The Nation, Rutherford Institute, Washington Office on Latin America Versus National Security Agency/Central Security Service, US Department of Justice, Adm. Michael S. Rogers as an official as the Director of the National Security Agency and the Head of the Central Security Service, the Office of the National Intelligence Director, Daniel R. Coats as the official director of the National Intelligence and Jefferson B. Sessions III as the official US Attorney General.

knowledge from numerous known facts forms the basis of Big Data analytics, which is widely used in mass surveillance programs. As a result, the measures of this type can not only provide detailed data on individuals, but can also be used to predict behavior of selected social groups or the entire society.

It is difficult to find a more obvious confirmation that unlimited eavesdropping of millions of citizens does not only lead to a distortion of the idea of privacy protection, but also does not support the purpose for which it was established – to increase public security. The fact of recording data concerning electronic communications of hundreds of thousands of housewives, workers, officials, children, lawyers, politicians or clergy does not increase defensive capabilities of the state. On the contrary, it engages public services to analyze huge data sets, worthless from the point of view of state security, but forming an inexhaustible source of information and control over the society.

Literature

Bożek M., *Normative aspects of the state security system in emergency situations of political and military nature*, Lublin 2004.

Kawka W., *Policja w ujęciu historycznym i współczesnym*, Wilno 1939.

Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Warszawa 2011.

Marczak J., *Universal protection and national defence*, [in:] *Fundamentals of Poland's national security in the era of globalization*, eds. R. Jakubczak, J. Marczak, K. Gąsiorek, W. Jakubczak, Warsaw 2008.

Vall M., Nowińska E., *The Act on combating unfair competition. Commentary,* Warsaw 2013.