DOI : 10.14746/pp.2021.26.3.1

Remigiusz ROSICKI
Adam Mickiewicz University in Poznań
ORCID ID: 0000-0002-1187-5895

State security and individual security as exemplified by operational surveillance used by the Polish counter-intelligence service

Abstract: The material scope of the research problem presented in the text encompasses the issues concerned with operational surveillance that the Polish civilian counter-intelligence service, i.e. the Internal Security Agency (in Polish abbreviated as ABW – Agencja Bezpieczeństwa Wewnętrznego), is authorised to. The main purpose of the analysis is to assess the changes introduced as a result of the passing of the so-called *Surveillance Act* in 2016. The Act was supposed to introduce new regulations with regard to the powers concerning operational surveillance and obtaining of ICT data, granted to particular secret and police services. The said changes were enforced by the judgment of the Constitutional Tribunal, which in 2014 found numerous violations of the provisions of the Constitutions of the Republic of Poland caused by the existing regulations authorising the services to engage in particular operational and investigative actions.

In order to elaborate the material scope of the research problem, and to present the conclusions, the following research questions have been presented in the text: *Do the legal regulations concerning the powers vested in the Polish civilian counter-intelligence service within operational surveillance infringe individual rights and freedoms (e.g. the right to privacy, protection of personal information, privacy of correspondence), and if so, then to what extent?*

Functional and pro-constitutional interpretations have been applied to assess the provisions regulating the powers of the Internal Security Agency with regard to operational surveillance and obtaining of ICT data. The functional interpretation focuses on the function of selected legal solutions, whereas the pro-constitutional interpretation focuses on the assessment of legal solutions in the context of the principles of a democratic state ruled by law, as well as human rights and freedoms. As regards the pro-constitutional interpretation, the tool used for assessment is the test of proportionality, i.e. the rule used for interpreting legal norms according to the degree and legitimacy of the interference in individual rights and freedoms.

Key words: secret services, Internal Security Agency, operational and investigative actions, operational surveillance, surveillance, individual rights and freedoms

Introduction

The material scope of the analysis performed in the text is concerned with the problematic of operational surveillance that the Polish civilian counter-intelligence service is authorised to in the context of the Act of 24 May 2002 on the *Internal Security Agency and the Foreign Intelligence Agency* (Journal of Laws 2002, no. 74, item 676, as amended). Therefore, the scope of the analysis encompasses the problematic of operational surveillance as a power vest in the Internal Security Agency (in Polish abbreviated as ABW – *Agencja Bezpieczeństwa Wewnętrznego*). The reason for choosing such a research problem is willingness to evaluate the changes made as a result of the passing of the so-called *Surveillance Act* of 2016, the main purpose of which was proper

adjustment of the regulations in the acts concerning particular services in the scope of operational surveillance and access to ICT data (Journal of Laws 2016, item 147). The need for changes to be made by the Polish legislator was enforced by the 2014 judgment of the Constitutional Tribunal, which established unconstitutionality of numerous legal solutions concerning surveillance of the citizens, and serving as powers of the police and secret services, including the Polish civilian counter-intelligence (*Judgment of the Constitutional Tribunal* of 30 July 2014, ref. no. K 23/11).

The main remarks which were made by the Constitutional Tribunal in 2014, and which point to the violation of the norms and provisions of the Constitution include the following legal theses: (1) collecting, storing and processing of data on individuals without an explicit and precise statutory provision is unlawful, (2) it is necessary to precisely determine what organs of the state are authorised to carry out operational surveillance, (3) legal provisions must specify grounds for carrying out operational and investigative activities, and limit them to prevention and detection of serious offences only, (4) it is necessary to specify not only covert measures for obtaining information, but also the kinds of information collected with particular measures, (5) legal provisions must specify a maximum period of time for carrying out operational and investigative activities, which in turn should not infringe the principle of necessity related to the constitutional principle of proportionality, (6) legal provisions must specify a procedure for ordering operational and investigative activities, including the obligation to obtain permission from an independent organ for covert obtaining of information, (7) legal provisions must specify a procedure for handling data stored during operational and investigative activities, (8) legal provisions must specify a procedure for *ex post facto* notification of citizens of covert obtaining of information related to them, (9) the activities serving as operational surveillance and consisting in collecting data must be a subsidiary measure for obtaining information or evidence, (10) legal provisions must specify a procedure for challenging operational and investigative activities (*Judgment of the Constitutional Tribunal* of 30 July 2014, ref. no. K 23/11; *The Ombudsman’s application submitted to the Constitutional Tribunal* on 18 February 2016; Rosicki, 2014, pp. 63–75). The same theses were repeated by the Ombudsman in the application to the Constitutional Tribunal in 2016, which, however, the Ombudsman withdrew because of, *inter alia*, the defective composition and the violation of the provisions regulating the activity of the Constitutional Tribunal (*The Ombudsman’s application to the Constitutional Tribunal* of 18 February 2016; *Procedural Writ by the Ombudsman* of 14 March 2018).

Both in democratic and non-democratic states, the authorities tend to justify their interference in the citizens’ rights and freedoms by raising the argument of security, more often than not collective security, with a view to protecting both collective and individual interests. Thus, the argumentation which under normal conditions is used to protect democracy, here is invoked to dismantle the mechanisms that protect the individual against the state (cf. Loewenstein, 1935a, pp. 571–593; Loewenstein, 1935b, pp. 755–784; Loewenstein, 1937a, pp. 417–432; Loewenstein, 1937b, pp. 638–658; Lerner, 1938; Barber, 2003; Jovanović, 2016, pp. 745–762; Malkopoulou, Norman, 2018, pp. 442–458; Bäcker, Rak, 2019, pp. 63–82; Maddox, 2019). However, it is noteworthy that it is in the case of democratic states ruled by law and liberal democracies that interference in citizens’ rights and freedoms becomes a serious problem, because it acts as their gradual and

deliberate diminution. At the same time, by creating insufficiently specified legal regulations and norms, the authorities acquire a special kind of competence authorising them to use their own discretion while making decisions that remain outside social control. The logic behind the argumentation is quite simple, and it is predicated on demonstrating that the common good (the good of the community, the good of the state) becomes more important than the individual good, e.g. the right to privacy (individual security). A conflict between these two values intensifies insofar as the state makes use of – in its opinion – more effective means of eliminating real, created or imaginary threats.

In order to elaborate the material scope, the following research questions have been presented in the text: Do the legal regulations concerning the powers vested in the Polish civilian counter-intelligence service within operational surveillance infringe individual rights and freedoms (e.g. the right to privacy, protection of personal information, privacy of correspondence), and if so, then to what extent? The analysis of possible infringement of individual rights and freedoms with regard to operational surveillance encompasses the context of the relationship between individual security and state security. Undoubtedly, the very context of political and legal changes that took place in Poland after 2015 is of considerable relevance for the analysis.

Functional and pro-constitutional interpretations have been applied in the analysis of the content of the legal regulations concerning operational and investigative activities. The functional interpretation focuses on the function of selected legal solutions so that the presented norms are provided with proper axiological justification. The pro-constitutional interpretation focuses on the assessment of legal solutions in the context of the principles of a democratic state ruled by law, as well as human rights and freedoms. Of great significance in the pro-constitutional interpretation is the rule whereby interpretation of legal norms is performed with regard to the degree and legitimacy of the interference in individual rights and freedoms, i.e. with regard to the principle of proportionality. These interpretations have been used to assess the correctness of the solutions concerning operational surveillance, as special powers exercised by the Polish counter-intelligence service, on the basis of the Act of 2002 on the *Internal Security Agency and the Foreign Intelligence Agency*, and the so-called *Surveillance Act* of 2016 (cf. Wronkowska, Ziembiński, 1997, pp. 147–179; Zieliński, 1998, pp. 1–20; Wronkowska, 2005, pp. 76–91; Zieliński, 2009, pp. 23–39; Wiatrowski, 2013, pp. 1–34; Nowacki, Tabor, 2016, pp. 293–312).

1. Theoretical and normative issues

1.1. State security

The content of Art. 5 of the Constitution of the Republic of Poland indicates that the state is obliged to ensure the security of the citizens, and so security is one of the most important legal interests in the state legal system. Security, as a legal interest, is most often equated with the collective entity, i.e. the state, nation and community. Thus, in a situation where it is necessary to weigh interests, e.g. in extreme situations, it is polit-

ical practice to oppose the security of the community to individual rights and freedoms. However, it is noteworthy that security is not the only legal interest, nor is it as such positioned above or below other interests or values in the Constitution of the Republic of Poland. One cannot consider the problem of security without referring to the content of Art. 31(3) of the Constitution. The provision contained therein indicates that any limitation upon the exercise of constitutional freedoms and rights may be imposed only by statute, and only when necessary in a democratic state, *inter alia*, for the protection of its security or public order (cf. Jabłoński, 2010; Garlicki, 2020, pp. 121–136).

Therefore, one may conclude that in democratic states ruled by law and liberal democracies the problem that remains unresolved is the relationship between two values, i.e. security of the state (community) and security of the individual (individual rights and freedoms). While Art. 5 of the Constitution stipulates the obligations of the state towards the citizens and the community, Art. 31 of the Constitution stipulates grounds for restricting civil liberties and rights for the sake of, *inter alia*, security as well as liberties and rights of other individuals. In the case of the restrictions for the sake of the security of the community, the legislator indicates the limit, i.e. the inviolability of the essence of individual rights and freedoms. Hence, one can conclude that both the afore-mentioned constitutional provisions present a conflict between two values, i.e. the interest of the community and the interest of the individual. In situations where it is necessary for the executive to weigh interests, e.g. in extreme situations, this kind of conflict can be instrumentally used in political and legislative practice. This kind of instrumental practice is frequently associated with limitation of individual rights and freedoms, which become the object of fear management in the face of threats, e.g. acts of terrorism; this is commonly met with the passivity or acceptance on the part of the society. Apparently, the logic behind these processes is identical with the logic behind the processes related to penal populism (cf. Gardocki, 1990; Pratt, 2007; Szafrańska, 2015, 21–71; Kulesza, 2017; Widacki, 2017, pp. 7–13; Mounk, 2018; Płatek, 2019, pp. 125–217).

1.2. Security of the individual (individual rights and freedoms)

A crucial mechanism for verifying whether we are dealing with the authorities’ excessive interference in individual rights and freedoms is the test of proportionality. Proportionality itself is a rule to be used for interpreting legal norms on the basis of the evaluation of the degree of their interference, and so it establishes the excess or indispensability of such interference on the part of the legislator. The main element in the evaluation of the proportionality of the legislator’s interference is its necessity, as well as the preservation of the balance between the public interest and the individual interest. Therefore, in the first place the legislator ought to justify the functionality of the norm, its usefulness with regard to the accomplishment of the goal, as well as to demonstrate its necessity in the context of the goal that the legislator wants to accomplish with it. This test undoubtedly aims at evaluation of the consequences of the conflict of interests such as individual rights and freedoms, and the interests that the legislator wishes to protect (Garlicki, 2020, pp. 121–136).

Therefore, the proportionality is about the balance between various interests, established on the basis of axiological criteria and argumentation. Pursuant to the above-mentioned Art. 31 of the Constitution, the principle of a democratic state ruled by law is both the limit and the axiological criterion used in the assessment of proportionality. This is because it becomes a measure for the necessity of interfering in individual rights and freedoms in the legal system. Therefore, the legislator is justified in making use of special instruments only when the desired goal cannot be achieved in any other way. Even though state or public security as interests in themselves do not exclude protection of individual rights and freedoms, they are a foundation justifying their restriction. By the same token, the right to respect for private life and correspondence is not absolute in character. Legitimized by security, the degree of interference in rights and freedoms should not, however, be arbitrary or incommensurate with possible threats. Special measures used for interference should be subject to real control by democratic institutions. In the case of interference in individuals’ private lives and privacy of correspondence by means of surveillance, one should bear in mind that there is often no compensation for infringement or attendant abuse. (See *Judgment of the Constitutional Tribunal of 12 January 1999*, ref. no. P 2/98; *Judgment of the Constitutional Tribunal of 9 October 2001*, ref. no. SK 8/00; *Judgment of the Constitutional Tribunal of 12 December 2005*, ref. no. K 32/04).

The lack of real compensation for real infringement or rule of law infringement with regard to individual rights and freedoms requires special control of the surveillance used by various secret or police services. The European Court of Human Rights in Strasbourg has presented rules for exercising control and using surveillance in numerous judgments. By referring to theses in selected judgments of the ECHR, one can present the requirements to be met by regulations concerning surveillance activities. Therefore, in order to find surveillance measures legitimate, i.e. remaining within the law, it is necessary to precisely indicate, in the legal regulations: (1) the category of persons that may be subject to surveillance measures, (2) the essence of the cases or offences justifying employing surveillance measures, (3) the category and forms of surveillance measures, (4) the entities performing procedures of surveillance measures, (5) procedures of surveillance measures, (6) the time frame in which surveillance measures are to be applied, (7) a manner of collected information retention, (8) manners and scope of redress for damage done as a result of improper surveillance or data retention (cf. *Huvig v. France*, 1990; *Kruslin v. France*, 1990; *Prado Bugallo v. Spain*, 2003; *Weber & Saravia v. Germany*, 2006 ; *D. Popescu v. Romania, No. 2*, 2007; *AEI&HR and Ekimdzhiev v. Bulgaria*, 2008; *Iordachi and Others v. Moldova*, 2009; *Kennedy v. the United Kingdom*, 2010; Szuniewicz, 2016, pp. 214–224). The indicated requirements do not only fall within the compass of proportionality, but they also serve as institutional protection of rights and freedoms, and by extension security, of the individual. Next to these requirements, one should bear in mind the constitutional rights that directly pertain to the protection of the individual. Undoubtedly, of greatest significance are the rights concerning legal protection of private and family life, making decisions about one’s personal life, as well as rights safeguarding against the public authorities collecting information about citizens on account of its relevance and usefulness, including the right to freedom and privacy of communication (cf. Art. 47, art. 49, art. 51(2), *Constitution of the Republic of Poland*; Garlicki, 2020, pp. 126–138).

2. Operational and investigative activities, and operational surveillance

2.1. The procedure and scope of operational surveillance

The operational and investigative work undertaken by police and secret services comprises a set of overt, confidential and classified operational methods, measures and tactical actions (Hanausek, 2009, pp. 112–128). Of greatest significance are activities undertaken in a confidential or covert manner, and so they arouse the greatest interest on the part of civil rights and liberties organisations. In a democratic state ruled by law, operational methods may be used in operational and investigative work in accordance with the law and criminological knowledge in order to accomplish certain tasks concerned with identification, prevention and counteraction of specific threats or offences. In a democratic state ruled by law, operational work constitutes special powers vested in secret services that pose a certain risk which should not, however, surpass the state of higher necessity, or be characterized by features of prohibited acts specified in criminal law. Besides, the material scope of their use as well as methods should be in accordance with the principles of subsidiarity and proportionality (cf. Hanausek, 2009, pp. 112–128; Chrabkowski, 2013, pp. 186–202; Falenta, 2020). This results from the fact that in a legal and political system creation of special powers and competences for particular state institutions may, in exceptional situations, result in the institutions themselves creating exceptional situations to break the law.

One function of operational and investigative work is to provide evidence concerning offences and the offender. Therefore, operational work should produce evidence material that enables investigative bodies to conduct procedural acts, e.g. instituting criminal proceedings or performing other special acts during ongoing proceedings. It is worth drawing attention to the fact that the material or information obtained in the course of operational and investigative activities may be included in the criminal proceedings once they have been granted a status of evidence, i.e. in the course of acts specified in procedural criminal law. This results from the fact that it is unacceptable to directly use, in the proceedings, material obtained in the course of operational and investigative activities. Hence, one of the main problems encountered by the civilian counter-intelligence in the domain of operational work is the ability to convert the results of its work into operational material fit for the proceedings, and ultimately into evidence (cf. Rosicki, 1993, pp. 1–19; Hanausek, 2009, pp. 112–128; Zdybel, 2016; Szumiło-Kulczycka, 2012; Gardocka, Jagiełło, 2017; Jagiełło, 2019). The threat that the citizens who have been subjected to operational and investigative activities are faced with is the fact that they are not covered by procedural criminal law.

One form of operational and investigative work is operational surveillance, which according to the *Act on the Internal Security Agency and the Foreign Intelligence Agency* consists in the following activities: (1) obtaining and recording the content of conversations conducted with technical measures, including telecommunications networks, (2) obtaining and recording audio and video of individuals in rooms, means of transport or places other than public ones, (3) obtaining and recording the content of correspondence, including correspondence carried on by means of electronic communication, (4) obtaining and recording data contained on IT data carriers, telecommunications end

devices, IT and ICT systems, (5) gaining access to and control of the content of parcels (Journal of Laws 2002, no. 74, item 676, as amended; Miłkowski, 2020, pp. 244–275). As can be seen, all of the above-mentioned activities substantially interfere in private lives of individuals, not least because of the fact that an increasingly important role is played by everyday objects connected to ICT and telecommunications networks (e.g. mobile phones, tablets, smartwatches).

Operational surveillance, as a special power of the ABW with regard to identification, prevention and counteraction of specific threats or offences, must fulfil the condition of subsidiarity, which means that consent to it can be granted in a situation where other measures have proved ineffective or will prove useless. Operational surveillance is founded on investigation, prevention and detection of the following offences: (1) espionage, terrorism, unlawful disclosure or use of secret information as well as other offences against national security, (2) corruption committed by particular persons performing public functions, whenever this is against national security, (3) production of and trade in goods, technologies and services that are of strategic significance for national security, (4) illegal production, possession and trade concerning weapons, ammunition and explosives, weapons of mass destruction as well as narcotic drugs and psychotropic substances on an international scale. This foundation also includes offences against the essential economic interests of the state, offences against property, offences against economic trading and offences against money and securities trading in the context of the criminal code, as well as fiscal misdemeanours and offences against tax obligations, and subsidy and subvention settlements, as well as fiscal misdemeanours and offences against customs obligations and rules of trading in goods and services with foreign countries in the context of penal fiscal code. Moreover, the legislator includes in the foundation for operational surveillance selected offences against the administration of justice, but only when they are related to the above-mentioned offences. Next to the purpose of operational surveillance, which is investigation, prevention and detection of specified threats and offences, the legislator includes obtaining and recording of the evidence of the said offences, disclosure of property subject to forfeiture on account of the said offences and prosecution of the offenders (cf. art. 27, Journal of Laws 2002 no. 74, item 676, as amended; Bożek, 2014, pp. 125–133; Opaliński, Rogalski, Szustakiewicz, 2017, pp. 92–120; Miłkowski, 2020, pp. 249–250).

The act regulating the operation of the ABW provides for two modes of ordering and granting consent to operational surveillance – the full mode and the emergency mode. In the full mode, the ABW Head, having received a written permission from the Public Prosecutor-General, submits an application for operational surveillance with full documentation (material justifying the surveillance) to the Circuit Court in Warsaw. At every stage, i.e. with the Public Prosecutor-General and the Court, consent to operational surveillance may be refused. As regards the emergency mode, the ABW Head may order, having received a written permission from the Public Prosecutor-General, operational surveillance, applying to the Circuit Court in Warsaw for a decision to be issued in the case. If under this mode the court does not grant consent within 5 days of the ordering of operational surveillance, the ABW Head is obliged to discontinue the operational surveillance. As a result of the discontinuation of the surveillance, the ABW Head orders witnessed and recorded destruction of material that has been collected during the surveillance. The grounds for using the emergency mode are predicated on the risk of loss of

information, or covering up or destroying the proof of an offence. (cf. art. 27, Journal of Laws 2002, no. 74, item 676, as amended; Rogalski, 2019, pp. 180–197).

The act regulating the operation of the ABW indicates the duration for which operational surveillance may be ordered. In the first place, the court issues a decision about operational surveillance for a period of 3 months, which can be prolonged for no more than another 3 months. However, in justified cases, when during the operational surveillance new circumstances relevant to the prevention or detection of an offence, or identification of an offender, and obtaining of the proof of an offence emerge, the court may issue subsequent decisions, prolonging the operational surveillance for consecutive periods, none of which can last longer than 12 months. Thus, the total period of operational surveillance cannot last longer than 18 months, and cannot be prolonged more than the total period in relation to a given person or telephone number (cf. art. 27, Journal of Laws 2002, no. 74, item 676, as amended; Miłkowski, 2020, pp. 262–263).

Applications for the ordering of operational surveillance are processed by one judge under the conditions provided for the transfer, storage and disclosure of confidential information, and regarding the necessity to ensure proper protection of the secret against unauthorised disclosure. It is noteworthy that with every prolongation of the operational surveillance the application for prolongation is subject to approval from the Public Prosecutor-General and the Circuit Court in Warsaw. Only a competent prosecutor and a representative of the ABW Head can participate in a hearing before the court. The issuance of a decision about operational surveillance results in obligations on the part of telecommunications companies, postal services and electronic communication service providers. These entities are obliged to ensure, at their own expense, technical and organisational conditions enabling the ABW to conduct operational surveillance (cf. art. 27, Journal of Laws 2002, no. 74, item 676, as amended; art. 181 § 2, Journal of Laws 1997, no. 89, item 555, consolidated text).

Of essential significance are the regulations concerning the proceedings in the case when operational surveillance has produced information that is protected in the context of the Code of Criminal Procedure, as subject to absolute inadmissibility of evidence. This group includes information concerning confidentiality that binds advocates and legal advisers, i.e. information that the legal representative became aware of while providing legal advice or pleading the case. The same exclusion applies to information passed under the seal of confession that the clergyman is bound to observe. As regards this type of collected material, the ABW Head is obliged to order its immediate, witnessed and recorded destruction (cf. art. 27, Journal of Laws 2002, no. 74, item 676, as amended; art. 178, Journal of Laws 1997, no. 89, item 555, consolidated text).

“Lesser protection” is enjoyed by information the content of which pertains to professional confidentiality that binds notaries public, advocates, legal advisers, tax advisers, as well as to medical, journalistic and statistical confidentiality, and confidentiality that binds the Public Prosecutor-General’s Office, but the obtaining of which is necessary for the proper administration of justice, and a given circumstance may not be determined on the basis of any other evidence. However, this scope excludes prohibitions concerning the mediator’s privilege and reporter’s privilege, unless the information in question constitutes evidence of the acts enumerated in the offence specified in the criminal code as punishable failure to report a prohibited act (e.g. genocide, a terrorist offence, homicide,

espionage, rape). As regards information with “lesser protection,” the Public Prosecutor-General – having become familiar with the material collected and submitted by the ABW, and having recognised that its content pertains to particular types of confidentiality – is to immediately refer it to the court that has previously ordered operational surveillance or granted consent thereto. The court is to immediately decide about its possible use in criminal proceedings, having verified whether the provided material contains information pertaining to particular types of confidentiality, and whether it pertains to information constituting evidence of the acts enumerated in the offence specified in the criminal code, as failure to report an offence. However, whenever such information is inadmissible, the court is to immediately order destruction of the material, and the ABW Head is obliged to execute the order (cf. art. 27, Journal of Laws 2002, no. 74, item 676, as amended; art. 178a, art. 180 § 2 and 3, Journal of Laws 1997, no. 89, item 555, consolidated text; art. 240, Journal of Laws 1997, no. 88, item 553, consolidated text; Opaliński, Rogalski, Szustakiewicz, 2017, pp. 118–119).

2.2. The procedure and scope of ICT data obtaining

Obtaining ICT data needs to be distinguished from operational surveillance concerning, inter alia, obtaining and recording the content of conversations conducted with technical measures, the content of correspondence, including electronic correspondence, data contained on electronic devices and in ICT systems. ICT data includes telecommunications, postal and IT data, the scope of which is regulated by separate acts, i.e. the Telecommunications Act, the Act – Postal Law, and the Act on Providing Services by Electronic Means (Journal of Laws 2004, no. 171, item 1800, as amended; Journal of Laws 2021, item 576, as amended; Journal of Laws 2012, item 1529, as amended).

As regards telecommunications data, obtaining concerns details about the end of network, a telecommunications end device, the end user – both the entity that initiates a connection, and the entity to whom the connection is directed (e.g. a telephone number owner). Besides, the said data include information about the data and time of the connection, as well as its duration, the type of connection, and the location of the telecommunications end device. This means, *inter alia*, that information about the location of the device can be obtained, the indirect effect being the obtaining of the information about the location of the telephone owner. Moreover, companies are obliged to ensure access and record conditions, and to grant access to the processed data on users, transmission data (including data indicating the geographic location of the device), location data and data on attempts at establishing connections or on interrupted connections. The scope of telecommunications data *sensu largo* should also include the data made accessible to the telecommunications operator by virtue of the agreement concluded with the services user (e.g. a telephone owner) (art. 159, art. 161, art. 179, art. 180c, 180d, Journal of Laws 2004, no. 171, item 1800, as amended).

As regards postal data, the postal operator is obliged to ensure, free of charge and as part of the postal activity they conduct, technical and organisational conditions allowing, *inter alia*, the counter-intelligence service to perform their tasks. As regards the ABW, the scope of access and obtaining of postal data concerns information on postal opera-

tors, and information on the postal services provided and enabling identification of those who use the postal services (art. 82, Journal of Laws 2012, item 1529 as amended).

As regards IT data, the ABW is authorised to obtain, from operators, personal data that they process by virtue of the agreements concluded with the users of their services. The scope of these data includes the following information: PESEL number, passport number, national ID number, number of any identity card, permanent abode address, correspondence address, verification data for the services user’s electronic signature (art. 18, Journal of Laws 2002, no. 144, item 1204, as amended; Journal of Laws 2020, item 344).

The grounds for the ABW Head, or persons authorised by the ABW Head, to turn to operators for IT data are tasks set out by statute, but it is noteworthy that in this case the catalogue of these tasks is broader than the catalogue of the tasks enabling the application of operational surveillance. Apart from the above-analysed tasks, it is worth pointing to, *inter alia*: (1) identifying, preventing and counteracting threats undermining the internal security of the state and its constitutional order, and in particular undermining its sovereignty and international position, the sovereignty and inviolability of its territory, as well as the defence system of the state, (2) obtaining, analysing, processing and transferring, to competent organs, information that may be vital for the protection of the internal security of the state and its constitutional order, (3) identifying, preventing and detecting threats undermining the security of ICT systems and critical infrastructure that are vital from the viewpoint of the uninterrupted functioning of the state (cf. art. 5, Journal of Laws 2002, no. 74, item 676, as amended).

The manner of judicial review marks a big difference between the procedure for obtaining information in the context of operational surveillance and the procedure for obtaining telecommunications, postal and IT data. In the first case, a crucial element in the procedure is the necessity to obtain *ex ante* permission to conduct operational surveillance, whereas in the second case the procedure for obtaining ICT data does not require such permission. Still, this does not mean that the procedure for obtaining this type of data is beyond all review, but in this case review is *ex post facto* in character. The ABW Head is obliged to report to the court on a six-monthly basis, providing the number of cases in which data were obtained, and the legal category of the acts justifying their obtaining. Thus, it can be clearly seen that the scope of *ex post facto* review is different, or even meagre compared with the judicial review of the applications by the ABW Head within the scope of operational surveillance (cf. art. 28a, Journal of Laws 2002 no. 74, item 676, as amended; Opaliński, Rogalski, Szustakiewicz, 2017, pp. 132–134). A situation like this can hardly be regarded as one not open to doubt, given the principle of proportionality and possible violation of human rights and freedoms.

3. Practical issues

3.1. Characteristics of the legal and political context

A practical analysis of the significance of the regulations concerning operational surveillance, as a power vested in the ABW, should include the context of the political and

legal situation in Poland. In the first place, attention should be drawn to the destabilization of the legal system due to the unconstitutional changes in the Polish judiciary that were begun after 2015. In the view of some analysts and institutions assessing the rule of law, the changes result in, *inter alia*, a lack of effective and transparent system of judicial review of the constitutionality of law, which serves as an indication of the breach of the standards of a democratic state ruled by law. Ewa Łętowska, a former Ombudsman, goes as far as to speak about destruction and erosion of the rule of law in Poland after 2015. Besides, the fact that the Public Prosecutor’s Office is not really independent of political influence results in the fact that the institutions involved in the process of granting permission to operational surveillance may potentially fail to fulfil their functions in a proper manner that would not raise doubts (cf. *Opinia Naczelnej Rady Adwokackiej*…, 2016; CDL-AD/2016/012-e; Bodnar, 2019; *O wygaszaniu państwa prawa…*, 2020; *Case of Xero Flor w Polsce sp. z o.o. v. Poland*, 2021; *Reczkowicz v. Poland*, 2021). Furthermore, account should be taken of the critical remarks concerning a lack of real supervision over the activity of the Polish secret services, as exercised by independent state institutions. In addition, of no little importance are critical remarks presented in research and opinion publications on politicization and partisanship of secret services, and their instrumental use for short-term political gains (cf. Grochowski, 2013, pp. 195–206; Chuchowski, 2016; Rosicki, 2016, pp. 165–176; Laskowski, 2017; Rosicki, 2017; Panoptykon, 2018; Rzeczkowski, 2018; Itrich-Drabarek, 2019; Rzeczkowski, 2019; Rzeczkowski, 2020; Piński, Szwejgiert, 2021; Rzeczkowski, 2021, pp. 37–39; Zalewski, 2021). It is worth drawing attention to the fact that according to independent institutions as well as Polish and foreign means of social communication, in 2018 the Polish authorities purchased a powerful system of cyber-surveillance, commercially known as “Pegasus.” This gives rise to justified fear of the potential use of the surveillance system by secret services in breach of the law, and by extension of citizens’ rights and freedoms (cf. Marczak, 2018; Bodnar, 2019; Kaili, 2019, *Applications by the Ombudsman*..., VII.519.2.2019.AG).

It is also noteworthy that the presented solutions with regard to operational surveillance and obtaining of ICT data, i.e. selected elements in operational and investigative activity, do not concern activities conducted within criminal proceedings, and hence they are not regulated in the Code of Criminal Procedure. Therefore, they are not subject to procedural review until they are converted to evidence. Another noteworthy fact is that in Poland the majority of operational surveillance and data obtaining takes place at the pre-trial activities stage on the basis of special statutes that grant special powers to particular services, including the ABW (cf. Rosicki, 2017; Bodnar, 2019).

3.2. Characteristics of the proportionality of operational surveillance

The assessment of the constitutionality – chiefly with regard to the principle of proportionality – of legal solutions concerning the application of operational surveillance and ICT data obtaining, includes: (1) the procedure for applying for operational surveillance, (2) the duration of operational surveillance, (3) the scope of information obtained.

In the first place, it is worth drawing attention to the verification of the ABW applications for operational surveillance by the Circuit Court in Warsaw at the final stage. Both

in the full mode and the so-called mode “of the utmost urgency,” this court is one of last instance, and so considerable responsibility lies with it. However, one cannot speak about effective verification of this type of applications due to the fact that it is carried out by neither a specialised court department, nor specialised judges. Applications are verified by a judge under the conditions provided for the transfer, storage and disclosure of confidential information, and regarding the necessity to ensure proper protection of the secret against unauthorised disclosure. However, the verification takes place alongside other professional responsibilities encumbering the judge, and so it presents additional work. In a time of work overload, which can be caused by the number of cases conducted by the judge, s/he may not be in a position to become sufficiently familiar with the grounds and justification for the application submitted by the ABW. Due to the growing politicization of the judiciary, the review system may be doubtful on account of the constitutional principle of citizens’ trust in the state.

In the case of the applications for operational surveillance in the mode “of the utmost urgency,” there can be some doubt about the five-day period in which – provided the Circuit Court in Warsaw does not grant permission to ordering it – it should be discontinued, and the collected material should undergo witnessed destruction. There can also be doubt about the potential use of the five-day period for deliberate institution of review in this mode, so that the time can be used for collecting information, thereby interfering in the privacy of communication and citizens’ private lives. Besides, it is noteworthy that the witnessed destruction of material, whenever the court denies permission, does not preclude the violation of the rights and freedoms of the individual, because it is impossible to obliterate the knowledge acquired by the ABW functionaries who have acquainted themselves with the content of the recorded telephone conversations, nor is it possible to eliminate the knowledge in the form of memos written by the ABW functionaries.

Another crucial issue is the duration of operational surveillance, which can be prolonged whenever new circumstances emerge. Noteworthily, a prolonged application of operational surveillance violates at least the constitutional principles of citizens’ trust in the state, legal protection of private life, and the proportionality of restrictions on individual rights and freedoms. Therefore, it appears that granting the Polish services authorization to carry out surveillance for a period of 18 months is inordinate and lacking in justification grounded on necessity. Besides, legal regulations do not provide for the possibility of effective supervision over the obtained, collected and shared information on the citizen. There is no possibility of *ex post facto* review that the citizen could effect on an individual basis with the benefit of the feedback from the ABW as to the operational surveillance actions taken in relation to him/her. This type of review is of particular significance in a situation where no circumstances that might substantiate the original suspicions serving as the grounds for submitting an application for operational surveillance have been ascertained (cf. *Ombudsman’s application to the Constitutional Tribunal* of 18 February 2016).

Also, the scope of the information obtained by the ABW on the citizen remains beyond real control. Even though the individual has a right to protect their personal data, particularly data concerning their health, family and economic situation, as well as data on their political views, the control is impossible due to the lack of institutional solutions in this regard, as well as the lack of the transparency of the Polish counter-intelligence

service’s operation. As a result, there is quite a high risk of violation of the individual’s private life. And so from the constitutional viewpoint, the unlimited scope of collected information on the individual may be in breach of the principle of usefulness, indispensability and proportionality (cf. *Judgment of the Constitutional Tribunal of 30 July 2014*, ref. no. K 23/11; *Ombudsman’s application to the Constitutional Tribunal* of 18 February 2016).

The mode of the so-called “lesser protection” is questionable – in respect of the protection of individual rights – in the case where the information obtained during an ABW operational surveillance procedure is protected in the context of the Code of criminal procedure, and is connected with performance of specific functions or practice of specific professions, and the obtaining of which is necessary for the proper administration of justice. It seems that the statutory obligation under which courts are to issue decisions concerning admission of this type of material containing information covered by professional (e.g. attorney’s) confidentiality requirement in criminal proceedings violates rights of the individual. It is noteworthy that obtaining this type of information may take place without permission from the court, during on-going operational surveillance, and the legalisation of the material by the court will be *ex post facto*. Nor is it possible to appeal against such a decision issued by the court, which constitutes the material as evidence. The procedure followed by the Public Prosecutor-General, who at the same time performs a political function, in assessing the material obtained and collected by the ABW, before it is verified by the court, is a poor solution, which excessively extends access to material bound by professional secrecy. The solutions that enable collection and recording, as well as *ex post facto* legalisation of material bound by professional secrecy should be regarded as violation of the principles of a democratic state ruled by law. A similar judgment should be passed on the lack of clear criteria specifying the significance of information revealed in criminal proceedings, as the proper administration of justice can hardly be regarded as such a criterion. Such an imprecise and abstract criterion may result in considerable latitude enjoyed by enforcement authorities and the judiciary with regard to the legitimisation of the obtained material bound by professional secrecy. Perforce, juxtaposing the collective interest – in the form of proper administration of justice – with another interest, i.e. professional secret, will result in the former one being favoured by courts (cf. *Ibidem*).

Another problematic issue is the one of obtaining the so-called ICT data and data of other types in a manner circumventing preliminary review at the prosecutor’s office and court level, and without regard for the principle of subsidiarity and proportionality. The data scope encompasses telecommunications, postal and IT data, but the said data may not constitute the content of telecommunications message, a postal letter or parcel, or a message passed within the service provided by electronic means. This type of data includes, *inter alia*: personal data, data on the entity that initiates the connection, on the entity that receives the connection, on the duration of connections, on location and geolocation, and on the use of electronic services. The scope of these data has been included in the act regulating the activity of the Polish counter-intelligence and intelligence by referring to particular provisions of other specific acts of law. In consequence, use is made of categories that are quite general in character, and so are incongruent with the function, i.e. interference in individual rights and freedoms. The said solutions raise even

more doubts, if one takes into account the scope and degree of reconstruction of various aspects of the private life of the individual subjected to surveillance based on ICT data.

It should be noted that ICT data as well as data of other types may be obtained not only for the purpose of identification, prevention and detection of offences by the ABW. The legislator indicates that the said data may also be obtained for the purpose of accomplishment of other statutory tasks of the ABW, e.g. analysing, processing and transferring, to competent organs, information that may be vital for the protection of the internal security of the state and its constitutional order. Going beyond the catalogue of prohibited acts, and using the foundation – in obtaining ICT data and other data – of insufficiently specified and abstract phrases results in a lack of real possibility of verifying the legitimacy and scope of data to be obtained. Such legal solutions substantially interfere in the protection of the private life of the individual, and the use the ABW makes of them is questionable at best.

The last analysed solution that raises doubts is the necessity to provide the ABW with the data of telecommunications services providers, postal services providers and providers of services by electronic means. The data are provided directly to a designated ABW functionary, or via a telecommunications network. In the latter case this entails the necessity to develop an infrastructure of the so-called “dedicated lines” that enable access to the data without the agency of the employees of the above-mentioned providers. This solution results in obtaining data on private lives in an out-of-control manner, and with no regard for the principles of subsidiarity and proportionality. Therefore, the ABW powers clearly breach the fundamental rules that should characterize a democratic state ruled by law, thereby substantially violating individual rights and freedoms.

Conclusion

The subject of analysis in the present text is operational surveillance as a special power vested in the Polish civilian counter-intelligence, i.e. the Internal Security Agency. The analysis is performed in the context of the relationship between two interests, i.e. security of the individual and security of the state. In the latter case attention should be drawn to the instrumental use of the category of state interest with a view to introducing statutory solutions that substantially violate the principles of a democratic state ruled by law, including individual rights and freedoms. Of the greatest significance in the analysis are the solutions that can extraordinarily breach the right to privacy, the right to protection of personal information and the privacy of correspondence. The analysis is performed chiefly with the aid of functional and pro-constitutional interpretation. The subject of interpretation includes selected legal solutions in the context of the *Act of 2002 on the Internal Security Agency and the Foreign Intelligence Agency*, and the so-called *Surveillance Act* of 2016. Of no little significance for the reception of the solutions concerning operational surveillance are the changes in the Polish legal system introduced after 2015; these result in the destabilization of the legal system, a lack of effective constitutional review, as well as politicization and partisanship of the enforcement authorities and the judiciary. In order to elaborate the material scope of the analysis, and to present the conclusions in the text, the following research questions have been for-

mulated: *Do the legal regulations concerning the powers vested in the Polish civilian counter-intelligence service within operational surveillance infringe individual rights and freedoms (e.g. the right to privacy, protection of personal information, privacy of correspondence), and if so, then to what extent?*

It is noteworthy that the legislative changes made in 2016 by virtue of the so-called *Surveillance Act* by no means eliminated the possibility of infringing individual rights and freedoms with regard to the right to privacy, protection of personal information and the privacy of correspondence. The legal regulations concerning the ABW powers with regard to operational surveillance: (1) are not characterized by any considerable accuracy, (2) do not point to any precise grounds for application, (3) do not precisely indicate individuals that may become subject to surveillance, (4) do not precisely indicate the scope of information obtained, (5) do not precisely indicate the measures with which to obtain information, (6) do not indicate the surveillance time frame in a manner appropriate to the need, (7) do not provide for the procedure for challenging operational actions. Besides, it must be concluded that the legal solutions may substantially interfere in professional confidentiality, and by extension in the right to effective defence. Another issue, which is not addressed in the present text at length, is the question of the lack of real and effective supervision over the activity of the Polish counter-intelligence service, including operational actions, as exercised by independent institutions. The effect of the destabilization of the legal system is that the institutions involved in the legitimization of the applications for operational surveillance may not properly fulfil their functions. The very fact of the existence of legal provisions that may violate individual rights and freedoms proves the destabilization of proper administration of justice, which results in an extraordinarily privileged position of the state in relationship to the individual.

Next to the issues concerned with obtaining information in the context of operational surveillance, the text addresses the issues concerned with obtaining ICT data. According to the analysis, it is to be concluded that the regulations concerning the ABW powers with regard to ICT data obtained: (1) are not characterized by any considerable accuracy, (2) do not point to any precise grounds for obtaining, (3) do not precisely indicate individuals that may become subjects of data collection, (4) do not limit the scope of data depending on the need, (5) do not indicate the time frame within which to obtain the data, (6) do not indicate the period or manner of data retention. By way of general assessment, there is no real or effective control over the ABW procedure for obtaining the said data, which gives rise to a possibility of wide-ranging infringement by this service of the right to privacy and protection of personal information. As a result of the development of telecommunications and ICT technologies the collected data may be used for precise reconstruction of the private life aspects of the person subjected to surveillance.

Furthermore, it is noteworthy that the focus of analysis in the text is the ABW powers with regard to operational surveillance in the context of the *Act on counter-terrorism activities*, which granted extensive powers to the services with regard to surveillance of foreigners (Journal of Laws 2016, item 904; Gabriel-Węglowski, 2018). It seems that further studies of the issues of surveillance require comparative analysis of the ABW powers in the context of both the counter-terrorism act and the *Act on the Internal Security Agency and the Foreign Intelligence Agency*, so that the degree of interference in individual rights and freedoms can be presented in a systematic manner.

Bibliography

Act of 6 June 1997 – *The Code of Criminal Procedure* (Journal of Laws 1997, no. 89, item 555, consolidated text).

Act of 6 June 1997 – *The Criminal Code* (Journal of Laws 1997, no. 88, item 553, consolidated text).

Act of 24 May 2002 on the *Internal Security Agency and the Foreign Intelligence Agency* (Journal of Laws of 2002, no. 74, item 676, as amended).

Act of 18 July 2002 *on providing services by electronic means* (Journal of Laws 2002, no. 144, item 1204, as amended).

Act of 16 July 2004, *Telecommunications Act* (Journal of Laws 2004, no. 171, item 1800, as amended).

Act of 23 November 2012, *Postal Law* (Journal of Laws 2012, item 1529, as amended).

Act of 15 January 2016 *amending the Act on the Police, and certain other acts* (Journal of Laws, no. 2016, item 147) [the so-called *Surveillance Act*].

Act of 10 June 2016 *on counter-terrorism activities* (Journal of Laws 2016, item 904).

Announcement by the Speaker of the Sejm of the Republic of Poland of 6 February 2020 on publication of the consolidated text of the Act on providing services by electronic means (Journal of Laws 2020, item 344).

Announcement by the Speaker of the Sejm of the Republic of Poland of 23 February 2021 on publication of the consolidated text of the Telecommunications Act (Journal of Laws 2021, item 576, consolidated text).

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, (Application No. 62540/00), European Court of Huma Rights (2008), 30 January 2008.

Bäcker R., Rak J. (2019), *Trajektoria trwania opancerzonych demokracji*, „Studia nad Autorytaryzmem i Totalitaryzmem”, vol. 41, no. 3.

Barber B. R. (2003), *Strong Democracy. Participatory Politics for a New Age*, University of California Press, Berkeley–Los Angeles.

Bodnar A., *et al.* (2019), *How to Saddle Pegasus. Observance of civil rights in the activities of security services: objectives of the reform*, Commissioner for Human Rights, Warsaw.

Bożek M., *et al.* (2014), *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Kluwer, Warszawa.

Case of Xero Flor w Polsce sp. z o.o. v. Poland, (Application no. 4907/18), European Court of Huma Rights (2021), 7 May 2021.

CDL-AD(2016)012-e: *Poland – Opinion on the Act of 15 January 2016 amending the Police Act and certain other Acts, adopted by the Venice Commission at its 107th Plenary Session* (Venice, 10–11 June 2016).

Chrabkowski M. (2013), *Wykorzystanie metod pracy operacyjnej w czynnościach sprawdzających (uwagi do artykułu K. Chałubek)*, „Prokuratura i Prawo”, no. 7–8.

Czuchnowski W. (2016), *Bezpieczeństwo. Układ w specsłużbach*, https://wyborcza.pl/politykaekstra/1,132907,20092096,bezpieczenstwo-uklad-w-specsluzbach.html?_gl=1*m37qjh*_gcl_aw*R0NMLjE2MTUzNjQ0OTAuQ2owS0NRaUEtYUdDQmhDd0FSSXNBSERsNXhfelJtMDFLVFNKWk1Na2YxRG50NnRENkFZUnVYRE1JWm83RTBOZkNlZUp0MDJRX0VvR19UTWFBb3pnRUFMd193Y0I., 20.05.2016.

D. Popescu v. Romania, No. 2 (Application No. 71525/01), European Court of Huma Rights (2007), 26 July 2007.

Falenta P. P. (2020), *Uprawnienia operacyjne Policji o charakterze inwigilacyjnym*, Marszałek, Toruń.

Gabriel-Węglowski M. (2018), *Działania antyterrorystyczne. Komentarz*, Kluwer, Warszawa.

Gardocka T., Jagiełło D. (eds.) (2017), *Zagadnienie dowodowe w procesie karnym*, C.H. Beck, Warszawa.

Gardocki L. (1990), *Zagadnienia teorii kryminalizacji*, PWN, Warszawa.

Garlicki L. (2020), *Polskie prawo konstytucyjne*, Kluwer, Warszawa.

Grochowski R. (2013), *Rola służb specjalnych w demokratycznym państwie prawa*, „Środkoweuropejskie Studia Polityczne”, no. 4.

Gruszczak A. (2019), *Służby specjalne do naprawy. »Wymogiem skuteczności jest zespolenie«*, https://infosecurity24.pl/sluzby-specjalne-do-naprawy-wymogiem-skutecznosci-jest-zespolenie-komentarz, 14.10.2019.

Huvig v. France (Series A No. 176-B; Application No. 11105/84) European Court of Human Rights (1990), 12 EHRR 528, 24 April 1990.

Iordachi and Others v. Moldova (Application No. 25198/02), European Court of Huma Rights (2009), 14 September 2009.

Itrich-Drabarek J. (2019), *Etyka zawodowa funkcjonariuszy służb państwowych*, Difin, Warszawa.

Jabłoński M. (ed.) (2010), *Wolności i prawa jednostki w Konstytucji RP*, vol. 1: *Idee i zasady przewodnie konstytucyjnej regulacji wolności i praw jednostki w RP*, Beck, Warszawa.

Jagiełło D. (2019), *Taktyka kryminalistycznych czynności dowodowych*, C.H. Beck, Warszawa.

Jovanović M. (2016), *How to Justify »Militant Democracy«: Meta-ethics and the Game-like Character of Democracy*, „Philosophy and Social Criticism”, vol. 42, no. 8.

Judgment of the Constitutional Tribunal of 12 January 1999, ref. no. P 2/98.

Judgment of the Constitutional Tribunal of 9 October 2001, ref. no. SK 8/00.

Judgment of the Constitutional Tribunal of 12 December 2005, ref. no. K 32/04.

Judgment of the Constitutional Tribunal of 30 July 2014, ref. no. K 23/11.

Kaili E. (2019), *Question for written answer* E-005505/2020 *to the Commission* (Subject: Pegasus spyware).

Kennedy v. the United Kingdom (Application No. 26839/05), European Court of Huma Rights (2010), 18 May 2010.

Kruslin v. France (Series A No. 176-B; Application No. 11801/85), European Court of Huma Rights (1990), 12 EHRR 547, 24 April 1990.

Kulesza J. (2017), *Problemy teorii kryminalizacji. Studium z zakresu prawa karnego i konstytucyjnego*, UŁ, Łódź.

Laskowski D. (2017), *Polskie służby specjalne*, FNCE, Poznań.

Lerner M. (1938), *It Is Later Than You Think: The Need for a Militant Democracy*, The Viking Press, New York.

Loewenstein K. (1935a), *Autocracy versus Democracy in Contemporary Europe, I*, „The American Political Science Review”, vol. 29, no. 4.

Loewenstein K. (1935b), *Autocracy Versus Democracy in Contemporary Europe, II*, „American Political Science Review”, vol. 29, no. 5.

Loewenstein K. (1937a), *Militant Democracy and Fundamental Rights, I*, „American Political Science Review”, vol. 31, no. 3.

Loewenstein K. (1937b), *Militant Democracy and Fundamental Rights, II*, „American Political Science Review”, vol. 31, no. 4.

Maddox G. (2019), *Karl Loewenstein, Max Lerner, and militant democracy: an appeal to »strong democracy«*, „Australian Journal of Political Science”, doi: 10.1080/10361146.2019.1604943.

Malkopoulou A., Norman L. (2018), *Three Models of Democratic Self-Defence: Militant Democracy and Its Alternatives*, „Political Studies”, vol. 66, no. 2.

Marczak B., *et al.* (2018), *Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries*, „Citizen Lab Research Report”, no. 113, University of Toronto.

Miłkowski T. M. (2020), *Czynności operacyjno-rozpoznawcze a prawa i wolności jednostki*, Kluwer, Warszawa.

Mounk Y. (2018), *The People vs. Democracy. Why Our Freedom Is in Danger and How to Save It*, Harvard University Press, Cambridge.

Nowacki J., Tabor Z. (2016), *Wstęp do prawoznawstwa*, Kluwer, Warszawa.

The Ombudsman’s Application to the Constitutional Tribunal of 18 February 2016 (II.519.109.2015. KŁS/VV/AG).

The Ombudsman’s application to the Prime Minister of 9 September 2019 (VII.519.2.2019.AG).

The Ombudsman’s application to the chairperson of the Secret Services Committee of 9 September 2019 (VII.519.2.2019.AG).

Opaliński B., Rogalski M., Szustakiewicz P. (2017), *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, C.H. Beck, Warszawa.

Opinia Naczelnej Rady Adwokackiej dot. druków 550, 558 i 569 z dnia 10 czerwca 2016 (2016), http://orka.sejm.gov.pl/Druki8ka.nsf/0/5E5066F89108080CC1257FD5003AFDBC/%24File/550%2C558%2C569-001.pdf, 04.05.2021.

O wygaszaniu państwa prawa – wywiad z Prof. Ewą Łętowską i Prof. Jerzym Zajadło Rafała Kalukina (2020), https://palestra.pl/pl/aktualnosci/artykul/o-wygaszaniu-panstwa-prawa-wywiad-z-prof.-ewa-letowska-i-prof.-jerzym-zajadlo-rafala-kalukina, 25.11.2020.

Panoptykon (2018), *Czy ABW inwigilowała uczestników protestów? Wygrywamy w sądzie z Ministerstwem Cyfryzacji!*, https://panoptykon.org/wygrana-z-mc, 12.12.2018.

Piński J., Szwejgiert T. (2021), *Kamiński*, Penelopa, Warszawa.

Płatek M. (2019), *Kreowanie „groźnych, niebezpiecznych i złych”*, „Archiwum Kryminologii”, no. 1.

Prado Bugallo v. Spain (Application No. 58496/00), European Court of Huma Rights (2003), 18 May 2003.

Pratt J. (2007), *Penal Populism*, Routledge, London.

Procedural Writ by the Ombudsman of 14 March 2018 *re the case with ref. no. K 9/16*.

Reczkowicz v. Poland (Application no. 43447/19), European Court of Huma Rights (2021), 22 July 2021.

Rogalski M. (2019), *Podsłuch procesowy i pozaprocesowy. Kontrola i utrwalanie rozmów na podstawie kpk oraz ustaw szczegółowych*, Kluwer, Warszawa.

Rosicki L. (1993), *Possibilities of using operational material in preliminary proceedings* /a typescript – a graduate thesis/, University of Wrocław, Wrocław.

Rosicki R. (2014), *Surveillance and data retention in Poland*, „Public Policy and Economic Development”, no. 2.

Rosicki R. (2016), *Poland’s internal security as exemplified by the tasks and activities of the Internal Security Agency in the period 2007–2015*, „Przegląd Politologiczny”, no. 1.

Rosicki R. (2017), *Special services and surveillance of citizens in Poland (2015–2017)*, doi: 10.13140/RG.2.2.18880.23042.

Rzeczkowski G. (2018), *Służby w służbie partii (rozmowa z gen. Krzysztofem Bondarykiem)*, https://www.polityka.pl/tygodnikpolityka/kraj/1774718,1,sluzby-w-sluzbie-partii.read, 10.12.2018.

Rzeczkowski G. (2019), *Obcym alfabetem*, Arbitror, Warszawa.

Rzeczkowski G. (2020), *Służby bardzo polityczne*, https://www.polityka.pl/tygodnikpolityka/spoleczenstwo/1981870,1,sluzby-bardzo-polityczne.read, 20.12.2020.

Rzeczkowski G. (2021), *Szpiedzy przyjmą do pracy*, „Polityka”, no. 21.

Szafrańska M. (2015), *Penalny populizm a media*, Wydawnictwo UJ, Kraków.

Szumiło-Kulczycka D. (2012), *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, LexisNexis, Warszawa.

Weber & Saravia v. Germany (Application No. 54934/00), European Court of Huma Rights (2006), 29 June 2006.

Wiatrowski P. (2013), *Dyrektywy wykładni prawa karnego materialnego w judykaturze Sądu Najwyższego*, C.H. Beck, Warszawa.

Widacki J. (ed.) (2017), *Populizm prawny*, Akademia im. Andrzeja Frycza Modrzewskiego, Kraków.

Wronkowska S. (2005), *Podstawowe pojęcia prawa i prawoznawstwa*, Ars boni et aequi, Poznań.

Wronkowska S., Ziembiński Z. (1997), *Zarys teorii prawa*, Ars boni et aequi, Poznań.

Zdybel R. (2016), *Funkcja wykrywacza i dowodowa postępowania karnego*, C.H. Beck, Warszawa.

Zalewski S. (2021), *Kontrola służb specjalnych w Polsce*, Difin, Warszawa.

Zieliński M. (1998), *Wyznaczniki reguły wykładni prawa*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny”, no. 3–4.

Zieliński M., *et al.* (2009), *Zintegrowanie polskich koncepcji wykładni prawa*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny”, no. 4.

Bezpieczeństwo państwa i bezpieczeństwo jednostki na przykładzie kontroli operacyjnej stosowanej przez polski kontrwywiad

Sreszczenie

Zakres przedmiotowy problemu badawczego w tekście obejmuje tematykę kontroli operacyjnej, do której uprawniony jest polski kontrwywiad cywilny, czyli Agencja Bezpieczeństwa Wewnętrznego (pol. skrót: ABW – Agencja Bezpieczeństwa Wewnętrznego). Głównym celem podjętej analizy jest chęć oceny zmian, które dokonano w związku z przyjęciem tzw. *Ustawy inwigilacyjnej* w 2016 roku. Ustawa ta miała wprowadzić nowe regulacje w zakresie uprawnień dotyczących kontroli operacyjnej i pozyskiwania danych teleinformatycznych poszczególnych służb specjalnych i policyjnych. Zmiany te wymuszane zostały orzeczeniem Trybunału Konstytucyjnego, który w 2014 roku stwierdził liczne naruszenia przepisów Konstytucji RP przez dotychczasowe przepisy uprawniające służby do stosowania poszczególnych czynności operacyjno-rozpoznawczych.

W celu uszczegółowienia zakresu przedmiotowego problemu badawczego i prezentacji wniosków końcowych w tekście przedstawiono następujące pytanie badawcze: *Czy i w jakim stopniu regulacje prawne dotyczące uprawnień polskiego kontrwywiadu cywilnego w zakresie kontroli operacyjnej naruszają prawa i wolności jednostki (np. prawo do prywatności, ochronę informacji o sobie i tajemnicę korespondencji)?*

Do oceny przepisów regulujących uprawnienia Agencji Bezpieczeństwa Wewnętrznego w zakresie kontroli operacyjnej i pozyskiwania danych teleinformatycznych wykorzystano interpretację funkcjonalną i prokonstytucyjną. Interpretacja funkcjonalna skupia się na funkcji wybranych rozwiązań prawnych, natomiast interpretacja prokonstytucyjna na ocenie rozwiązań prawnych w kontekście zasad demokratycznego państwa prawa oraz praw i wolności człowieka. W przypadku interpretacji prokonstytucyjnej, narzędziem oceny jest test proporcjonalności, czyli reguła interpretacji norm prawnych wedle stopnia i zasadności ingerencji w prawa i wolności jednostki.

Słowa kluczowe: służby specjalne, Agencja Bezpieczeństwa Wewnętrznego, czynności operacyjno-rozpoznawcze, kontrola operacyjna, inwigilacja, prawa i wolności jednostki

Article submitted: 09.08.2021; article accepted: 29.08.2021
Data przekazania tekstu: 09.08.2021 data zaakceptowania tekstu: 29.08.2021