УДК: 355.40(438)(437.6)
DOI: https://doi.org/10.22182/pnb.1812020.3
Оригинални научни рад

Политика националне безбедности
Година XI, vol. 18
број 1/2020.
стр. 69-86

Mateusz Kolaszyński*

Jagiellonian University, Krakow, Poland

OVERSEEING SURVEILLANCE POWERS – THE CASES OF POLAND AND SLOVAKIA**

Abstract

The article aims to present the most important issues related to oversight over surveillance powers in Poland and Slovakia. The word „surveillance powers" used in the study refers particularly to covert techniques and practices of gathering personal data which occurs without the monitored subjects' knowledge or approval. Such surveillance powers are typically carried out by police services and intelligence agencies, and are more politically sensitive, as well as closely related to core issues of power and security. Oversight over these services and their surveillance powers is the standard in democratic states. Before 1989-1990, there was a similar model of security services in both analyzed countries. During Communism, there was no civil and democratic oversight over police services and intelligence agencies. Under the communist system control over security services was exercised by an inner circle representing the highest levels of the Communist party. Finally, since the early 1990s Poland and Slovakia had to build new systems of control and oversight over surveillance powers. Nowadays, both countries are members of the European Union and the Council of Europe. The basic issue of the paper is to describe how the systems of control and oversight look in Poland and Slovakia in the post-Snowden era.

Keywords: *surveillance, intelligence services, Poland, Slovakia*

* mateusz.kolaszynski@uj.edu.pl

** This work was supported by the National Scholarship Programme of the Slovak Republic for the Support of Mobility of Students, PhD Students, University Teachers, Researchers and Artists.

INTRODUCTION

Poland and Slovakia are very similar in terms of surveillance policy because a nonexistent public debate on surveillance characterizes both countries. One exception to this rule is the incidental debates over the activities of intelligence services **(**See e.g. Láštic, Kovanič 2017: 935) which are sparked off by the special status of these institutions in the political systems of both countries. Poland's and Slovakia's intelligence services have relatively broad powers in the surveillance field and at the same time are under the least control and oversight (Kolaszyński 2018; Svenonius, O., Björklund, F. and Waszkiewicz, P 2014; Završnik 2013).

On one hand, in recent years, the intelligence services of these countries have expanded their surveillance powers (Kolaszyński 2019; Kovanič 2019: 43). On the other hand, Poland and Slovakia continue to have significant problems with intelligence accountability. In political life, we can observe very often that formal accountability mechanisms are failing. That is why, in recent years, constitutional courts and NGOs have played a crucial role in limiting surveillance powers. However, there are many examples of unaccountable and illegitimate functioning of Polish and Slovak security services. In both countries, these agencies are politicized - the politicization is connected with personnel and institutional alternations in these services (Gruszczak 2017: 70; Aldrich, Richterova 2018: 1014).

Moreover, in both Central Europe countries, there are problems with intelligence services' legitimacy. Nonetheless, when it comes to the expansion of technological surveillance, these societies are characterized by greater support for technological surveillance mechanisms aimed at combating crime. Surveillance powers are considered to be a value-neutral solution to many security problems (Kovanič, Coufalova 2020: 115).

Poland and Slovakia have shared the experience with non-democratic intelligence agencies during the communist era. Under the communist system, secrecy was the norm in the state's surveillance policies (Persak, Kamiński 2005). The statutory basis did not regulate surveillance powers in a very comprehensive

way. Under the communist system control over intelligence and security services were exercised by an inner circle representing the highest levels of the communist parties - the Polish United Workers' Party (*Polska Zjednoczona Partia Robotnicza* – PZPR) and the Communist Party of Czechoslovakia (*Komunistická strana Československa* – KSČ). In fact, these structures were subject to the parties, not to the states - a trait common for most communist countries at that time (Caparini 2014: 500). Security and intelligence services were a part of the ministries which were highly centralized, hierarchized, and party-dependent. Sometimes the communist culture of secret services is mentioned (Medvecký, Sivoš 2016: 335). According to M. Kovanič and A. Coufalova this culture "was characterized primarily by the orientation of the intelligence agency inwards, on surveilling its own population and being an extension of the communist party, responsible for the maintenance of the non-democratic regime. In this sense, the legacy of communist intelligence, and the persistence of former officers, created a barrier to the creation of a democratic intelligence infrastructure" (Kovanič, Coufalova 2020: 118).

One of the consequences of democratic transformation was the need to create a system of control and oversight over intelligence services. Secret services also had to start respecting the rule of law. These requirements were opposite to the communist culture of intelligence. Intelligence services had to change the philosophy of their activity - become a service of the state and its citizens, not the ruling party (Williams, Deletant 2001: 17-20).

The article presents fundamental problems related to the control and oversight of surveillance in Poland and Slovakia. The first part characterizes the system of control and oversight over intelligence services in both countries. The rest of the article describes the most important changes in both systems after 2013. The article will examine the issue of overseeing surveillance powers from an institutional perspective. Particular attention was paid to the institutional mechanisms of oversight and control and its most vital elements: intelligence services, oversight institutions, and institutions of control.

POLAND AND SLOVAKIA BEFORE 2013

Poland's intelligence community is relatively complex and distinctly diversified. Intelligence is the main domain of special services. One of the most significant features of Polish intelligence is that it is referred to "special services" rather than intelligence services. The legal term "special service" includes intelligence agencies: the Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego* - ABW), the Foreign Intelligence Agency (*Agencja Wywiadu* - AW), CBA, the Military Counterintelligence Service (*Służba Kontrwywiadu Wewnętrznego* - SKW) and the Military Intelligence Service (*Służba Wywiadu Wojskowego* - SWW), but also police groups such as the Central Anti-Corruption Bureau (*Centralne Biuro Antykorupcyjne* - CBA). Indeed, there is a lack of clear division between intelligence services and police services in Poland (Gruszczak 2009). Currently, this problem applies to the CBA and the ABW (Kolaszyński 2017). Polish special services are institutions which undergo a specific process of oversight and control. Oversight and control solutions are supported by the Board for Special Services (within the executive branch) and the Sejm Committee for Special Services (within the legislative branch). Consequently, special services are located closer to the political centre and therefore are more exposed to political turmoil. It is the major difference between special services and other services, e.g., police agencies (Kolaszyński 2018).

Compared to Poland, Slovakia is characterized by integrated intelligence model, which means it covers both domestic and foreign intelligence. In this country, there are two intelligence services: the Slovak Information Service (*Slovenská informačná služba* - SIS) and the Military Intelligence (*Vojenské spravodajstvo* - VS). SIS is a civilian intelligence service, which is responsible for intelligence and counterintelligence - the Slovak Information Service is a general security and intelligence service of the Slovak Republic. The second intelligence service – VS was created on January 2013, as a result of merging two military intelligence services: Military Defence Intelligence (*Vojenské obranné spravodajstvo* - VOS) and Military Intelligence Service (*Vojenská spravodajská služba* – VSS). VS, as the name suggests*, is responsible for military*

intelligence.[1] *In Slovakia, t*he division of intelligence services and police agencies is more precise. Control and oversight institutions are, to a large extent, created for individual intelligence services, e.g., there are two parliamentary committees responsible for overseeing intelligence services - one for SIS and the other for VS (Kadlečíkovává, Rapošová 2016: 2-8).

The institutional frames of executive control over Polish special services are broad and flexible. The government enjoys a great deal of freedom as there are very few institutional limits. As a result, since 1990, special services have been controlled by many institutions of a different political character. In Poland, there are practically no permanent, institutionalized forms of executive control over services responsible for surveillance. Since there are so few institutional limitations, different governments enjoy considerable independence in exercising control. As a result, intelligence services have been supervised by several bodies of various structural and political status leading to a lack of permanent, substantive background, e.g., officials who would specialize in control over these institutions (Zybertowicz 2007).

Similarly to Poland, Slovakia also has many examples of the direct influence of politicians on the activities of intelligence services. This problem concerns, among other things, surveillance measures. In both cases, the politicization of intelligence services is characteristic. It can be said that the intelligence services are actors on the political scene. There are many political scandals related to eavesdropping of politicians, e.g., the Ground Scandal in Poland and the Gorilla Scandal in Slovakia (Láštic, Kovanič 2017: 937). On the other hand, they play a significant role in legislative changes related to the extension of surveillance powers.

When it comes to parliamentary oversight over intelligence services, it is quite similar in Poland and Slovakia. Parliamentary oversight is carried out primarily by special committees. In Poland, the Sejm Committee for Special Services (*Sejmowa Komisji ds. Służb Specjalnych*)[2] was appointed. In Slovakia, there are two par-

1 In Slovakia there is also National Security Agency (*Národný bezpečnostný úrad* – NBÚ). This agency is responsible for the protection of classified information, encryption services, and electronic signature. It also provides security clearances for dozens of state officials and civil and private employees and companies.

2 Article 95, second paragraph of the Constitution of the Republic of Poland of 2 April 1997

liamentary committees for intelligence services. Each intelligence service is the subject of work of a different parliamentary committee: Slovak Intelligence Service Oversight Special Committee (*Osobitný kontrolný výbor NR SR na kontrolu činnosti SIS*) for SIS and Military Intelligence Service Oversight Special Committee (*Osobitný kontrolný výbor NR SR na kontrolu činnosti Vojenského spravodajstva*) for VS. Oversight of the activities of SIS and VS shall be carried out by the National Council of the Slovak Republic, which shall establish for this purpose a special oversight body comprised of MPs of governmental political parties and opposition political parties.

The statutory basis of both special committees in Slovakia is very similar. In Poland, the statutory basis is minimal, and these issues are regulated in the Sejm regulations. In both countries, these committees are consisted of members of the parliament. The National Council of the Slovak Republic and the Sejm in Poland shall elect members to the committees, and determine the number of members, the organization and method of work of this body. The Slovak special committees are usually chaired by an opposition representative - in the past, this practice also applied in Poland.

The committees had the power to oversee numerous actions taken by the intelligence services.[3] However, the essential feature of the committees is not the wide subject field of its work but the fact that they are entitled to demand information from the government, the chiefs of services and their officers. The committees' power in that matter is limited. In Poland, disclosure of surveillance information requires the consent of the heads of intelligence services. The regulations do not point out to any particular grounds for either approval or rejection. That is why the committee might be denied access to information (Sarnecki 2010: 130). In Slovakia, these institutions have also limited powers to oversee intelligence surveillance. The committees review only internal regulations concerning conditions of use of intelligence services' surveillance measures.

(Journal of Laws, no. 78, item 483 as amended) states that the Sejm (the lower house of the parliament) is responsible for government oversight.

3 In Poland the Committee handles only some of services entitled to perform surveillance. Regulations refer to them as special services (*służby specjalne*) and they include: the Internal Security Agency (ABW), the Foreign Intelligence Agency (AW), the Central Anti-Corruption Bureau (CBA), the Military Counterintelligence Service (SKW) and the Military Intelligence Service (SWW).

The next element of the control and oversight system - the judicial oversight officially guarantees external, independent oversight over this area of secret surveillance which interferes with the human rights to the greatest extent. In both countries, courts play an essential role in approving some surveillance measures of intelligence services. However, in Slovakia, the mandate of the judiciary seems broader, e.g., the access to the telecommunications metadata was made conditional on obtaining a court-approved warrant. Moreover, court approval is necessary for a covert replacement of the object, a simulated object ownership transfer.

However, there is a lack of actual judiciary oversight in Poland. Polish judiciary oversight is exercised by criminal divisions of common courts of law and military courts which mostly deal with criminal cases. There are no other specially designed departments or other structures which would be responsible for giving consent to operational surveillance. For this reason, such duties are treated as peripheral or secondary tasks.

In Poland and Slovakia, remaining elements of formal oversight over secret surveillance play very important role. The Constitutional Courts played one of the significant roles in developing the statutory basis for secret surveillance. The sentences passed by the Courts often contributed to the changes in the regulations and, consequently, more excellent protection of human rights and liberties. In Poland, some aspects of secret surveillance work also used to be monitored by an independent constitutional body - the Supreme Audit Office (*Najwyższa Izba Kontroli* – NIK) which supervised methods of acquiring telecom data. Also, the Commissioner for Human Rights (*Rzecznik Praw* Obywatelskich - RPO) is in charge of dealing with human rights and violations of civil liberties. In case there are doubts about regulations regarding powers taken by intelligence services and law enforcement, the Commissioner's task is to commence procedures in front of the Tribunal to find such regulations unconstitutional. The Commissioner's interests also include the issue of wiretapping utilized by law enforcement and intelligence services.

To sum up, before the Snowden revelations, the Polish and Slovak systems of control and oversight were similar. Both systems were not institutionally developed, and discussion on this subject is very limited in these societies.

POLAND AFTER 2013

In Poland there were no significant surveillance reforms after Snowden revelations. The amendments to the Act[4] in 2016 implemented many recommendations included in the Constitutional Tribunal judgment of 30 July 2014.[5] However, the most essential principles formulated in the judgment, which had to be reflected in the process of revision of secret surveillance legislation, were not included. In this judgment, the Tribunal specified essential principles that must be jointly met by provisions which regulate obtaining information on individuals in secrecy by public authorities in a democratic state ruled by law. The Polish legislator has not introduced some of such principles to date. For example, according to the judgment, the law should provide for the right of the monitored person to be informed about surveillance once it is finished, and the right to initiate the judicial review thereof (however, in exceptional circumstances the departure from the notification rule should be possible).[6] Such a right has not been provided to citizens yet.

A number of recommendations from the Venice Commission have not been introduced in the Polish law. According to the Opinion of 2016, procedural safeguards and material conditions set in the police acts[7] on implementing secret surveillance are still

4 The Act of 15 January 2016 Amending the Police Act and certain other acts (the so-called surveillance act). This amendment led to the creation of a mechanism of oversight of access to telecommunication and internet data based on the ex-post supervision conducted by the regional court (*sąd okręgowy*) on the basis of a biannual statistical report prepared by the law enforcement and intelligence services.

5 The Constitutional Tribunal, judgment of 30 July 2014 (No. K 23/11).

6 See also the Decision of the Constitutional Tribunal of 25 January 2006 (No. S 2/06).

7 Nowadays, the term "the police acts" includes the Act of 6 April 1990 on the Police; the Act of 12 October 1990 on the Border Guard; the Act of 24 August 2001 on the Military Police and military law enforcement bodies; the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency; the Act of 9 June 2006 on the Central Anticorruption Bureau; the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service; the Act of 16 November 2016 on the National Revenue Administration; the Act of 8 December 2017 on the National Security Service.

insufficient because they do not prevent excessive use of powers and unjustified interference with the privacy of individuals. Detailed recommendations of the Venice Commission concerned strengthening of the proportionality principle in the following way: first, limitation of the use of secret surveillance only to the most serious cases. Secondly, limitation of the duration of the metadata monitoring. It is also significant to respect a lawyer-client privilege (and other privileged communications) while ordering secret surveillance. A number of recommendations concerned a mechanism of oversight of secret surveillance and metadata collection: to complement the system of judicial pre-authorization of secret surveillance with additional procedural safeguard, e.g. a privacy advocate; a complaints mechanism; a system of *ex-post automatic oversight of such operations by independent body (*Venice Commission 2016).

Many opinions regarding surveillance for the European Union countries can be found in the European Union Agency for Fundamental Rights' (FRA) reports (European Union Agency for Fundamental Rights 2017a; European Union Agency for Fundamental Rights 2017b). The issue of the impact of surveillance on fundamental right is crucial in democratic countries. One of the FRA reports indicates e.g. following recommendations: clear legal framework; defining in law oversight bodies' competencies over international intelligence cooperation, efficient whistleblower protection, safeguards against surveillance for protected professions (e.g. members of parliament, members of the judiciary, lawyers and media professionals). These reforms should be introduced along with broad consultation and openness during the legislative process. A significant part of recommendations concerned an oversight system of intelligence services. The legal system should provide independent intelligence oversight with sufficient powers and competencies, technical expertise, openness to public scrutiny etc.

In Polish case, introduction of these recommendations would require fundamental systemic changes in surveillance or intelligence law. Such extensive reforms took place in France, Germany, the Netherlands and the United Kingdom in recent years (European Union Agency for Fundamental Rights 2017b: 9). In Poland there are no governmental proposals for such reforms although the program of the ruling party (the Law and Justice, PiS) assumes

strengthening of parliamentary oversight of intelligence services and adopting comprehensive surveillance law (The Party Program of the Law and Justice 2014: 62). Neither the program nor the governmental policy links surveillance issue with protection of individual rights. Poland is definitely going in a different direction strengthening surveillance powers of security services without material and procedural safeguard for fundamental rights.

According to the Polish Ombudsman, the reforms introduced in 2016 (the so-called surveillance act) not only fails to execute the judgment of the Constitutional Tribunal of 2014, but "seriously violates the constitutional rights and freedoms and the standards set out in international law".[8] According to him, in the Polish legal system there is still a shortage of the legal safeguards which would make sure that surveillance measures do not violate fundamental rights.

The most important the Ombudsman's allegations concern the violation of the right to privacy and the protection of personal data of citizens:

- **no time limit or disproportionately long duration of operational surveillance**. Operational surveillance is performed, as a rule, with the prior consent of a regional court. This power can be prolonged to a maximum of 18 months. It is too long time period for the ombudsman and in his opinion, it does not satisfy the condition of proportionality principle.

- **very broad mandate of police and intelligence services to collect metadata.**[9] The grounds for collecting metadata under the police acts are very wide. Services may collect metadata for any useful purpose related to the very broad mandate to maintain peace and order.[10]

- **no real oversight of metadata collection by an independent body.** Regarding the collection of metadata there is

8 The Commissioner for Human Rights application, No K 9/16, p. 6.

9 Metadata is all data connected to and regarding a (tele-) communication. It may include information about phone calls placed or received, numbers dialed, duration of calls, geographical location of mobile devices at a given moment, websites visited, logins, personal settings, addresses of e-mail correspondence etc. (Venice Commission 2016: 7).

10 E.g. under Article 20c para. 1 of the Police Act, the Police can obtain metadata "in order to prevent or detect crimes or in order to save human life and health, or in order to support rescue and find missions".

only a system of ex-post review in Poland. According to the ombudsman, courts do not have all the necessary legal tools to fulfill their controlling function. The reporting obligation is insufficient because reports contain only summarized information, which does not give insight into the particulars of each specific case.

• **lack of right of the monitored person to be informed about surveillance.** As already noted above, such a right has not been provided to citizens yet. According to current provisions, a citizen does not receive such information even when no evidence was detected during the surveillance.

• **flaw in the provisions regulating surveillance of privilege communications.** The ombudsman in his application drew a particular attention to a weaker professional privilege which covers notaries, advocates and legal advisors (who do not act as defence lawyers), tax advisors, doctors, mediators or journalists. Nothing in the Polish law prevents police and intelligence services from listening to such conversations.

The allegations of the Polish Ombudsman are based on the case-law of the European Court of Human Rights, Court of Justice of the European Union and the Polish Constitutional Tribunal. Case-law of these courts is essentially convergent. Therefore, the allegations are very similar to the recommendations from the Venice Commission opinion. *Nota bene: the Venice Commission "in deference to the Constitutional Tribunal" avoided commenting on the compatibility of the 2016 amendments with the Polish Constitution and based its analysis on international standard (*Venice Commission 2016: 5).

SLOVAKIA AFTER 2013

Currently, surveillance reforms are more visible in Slovakia. Systemic changes in the legislation regarding privacy and data protection are related to the final resolution of the Constitutional Court of the Slovak Republic from 29 April 2015.[11] As in Poland, the jurisprudence of the Slovak Constitutional Court is similar to

11 Slovakia, Constitutional Court of the Slovak Republic (*Ústavný súd Slovenskej Republiky*) Resolution No. PL. ÚS 10/2014-78 from 29 April 2015. Available at http://www.concourt.sk.

the jurisprudence of the European Court of Human Rights, Court of Justice of the European Union. According to the judgment, mass and systematic surveillance violates the right to privacy and the principle of proportionality (Kovanič 2019: 43).

The amendments to the three Acts came into force on 1 January 2016.[12] According to J. Kadlečíkovává and I. Rapošová: "the new provisions secure a greater control over data retention process and provide more detailed specification of situations in which data could be retained, stored and requested by state bodies" (Kadlečíkovává, Rapošová 2016: 2). The amendments stated that metadata may be requested only in the case of the most serious crimes, such as terrorism, and could be obtained only based on a court order. Currently, the Slovak intelligence services are entitled to acquire telecommunication data only *ex-ante* and only with the written consent of the competent judge. In this situation, the principle of proportionality must also be fulfilled (Kovanič 2019: 43).

In 2015 also brought a passing of the anti-terrorist legislation. It included the amendment to the Criminal Code[13], which e.g., enabled police access to metadata from telecommunication companies' databases in cases of the search for a wanted or missing person. In the first case, a judicial warrant is required. Moreover, the SIS unsuccessfully tried to gain more unrestricted access to metadata. Such two attempts occurred in 2015 and in 2018. Both tries failed due to political and civil society resistance (Kovanič 2019: 43).

Moreover, the amendments provide for an obligation to establish a new monitoring body - the Special Commission of the National Council to oversee the use of information-technological tools that shall secure the surveillance. It is to be an institution that combines elements of parliamentary and expert oversight. The Special Committee is comprised of 6 MPs of governmental political parties (3 MPs) and opposition political parties (3 MPs). In addition, the committee consists of 2 experts. A committee audit

12 Slovakia, Act No. 397/2015 Coll. which for the purposes of the Criminal Code provides a list of substances with anabolic or other hormonal action and amending and supplementing certain laws (*Predpis č. 397/2015, ktorým sa na účely Trestného zákona ustanovuje zoznamlátok s anabolickým alebo iným hormonálnym účinkom a ktorým sa menia a dopĺňajú niektoré zákony)* from13 November 2015.

13 No. 444/2015.

may be initiated at the request of an authority and the request of a citizen. There is currently no information on the work of the commission. That is why M. Kovanič's opinion: "even the minimal parliamentary control of the use of metadata by the police and intelligence is not functional" seems correct (Kovanič 2019: 44).

In Slovakia, as in the case of Poland, the process of extending surveillance powers is also visible. The most representative example is associated with the launch of the Electronic Toll System (ETS) in Slovakia. The operation of the toll system required the building of a surveillance infrastructure over Slovak motorways, which collected two types of data. The first one was data collected electronically by the operator – such as the vehicle number plate, technical information about a vehicle, the distance driven by a vehicle, and information about toll programs. The second type of data was required for the conclusion of the contract – personal information of the vehicle owner and information about the vehicle. This infrastructure created a potentially extensive surveillance program for the movement of individuals across the country (Kovanič, Coufalova 2020: 123). In past years, the SIS gained unlimited access to all data collected through ETS. The provision of the law is formulated very generally, and the procedure of access is unclear.

Another example of extending surveillance powers is the amendment of the Act on the Protection of Privacy against Unauthorized Use of Information and Technical Means.[14] This amendment specified the definition of information and technical means of surveillance by adding messages transmitted through electronic communication networks. This change meant that the SIS would be able to perform surveillance on communications transmitted by email, social networks or software such as Skype or Google Hangouts, which it had not been able to do officially until then (Kovanič, Coufalova 2020: 124).

Changes in law directly related to terrorist attacks in Europe in recent years are very significant. One of the reactions to the occurrence of terrorist attacks was the expansion of the powers and competencies of intelligence services – including the expansion of surveillance capacities. Most of the anti-terrorist legislation was presented to the National Council as an amendment to the Crimi-

14 No. 404/2015.

nal Code in November 2015 and included changes to 16 laws and the constitution. According to amendment, the SIS received new powers to actively collect information on terrorism, political and religious extremism, cyber threats, and human migration. It also gained new powers to 'shut down' extremist websites, or websites promoting terrorism. The SIS also received the power to request camera or audio recordings from CCTV cameras, or other devices that capture public spaces, if this recording is needed to protect state security. M. Kovanič and A. Coufalova note that in Slovakia, there is "the problem of the indirect amendment of competencies – the increase of powers through the legislative amendment of a different law" (Kovanič, Coufalova 2020: 125).

CONCLUSIONS

The oversight of surveillance powers in Poland and Slovakia is based on the same principles. Both countries have similar problems in this matter. The institutional systems of control and oversight over surveillance powers are not developed in both countries. There is a visible lack of wider public debate on this topic. This can be explained by the low interest in the surveillance issue in these societies. The impulse to legislative changes were, to a greater extent, terrorist attacks in Europe rather than the Snowden revelations. In recent years, legal changes strengthening oversight over surveillance powers are more visible in Slovakia. However, in Slovakia, there are problems at the level of political practice with the implementation of laws. In Poland, governments ignore the legal standard in this field. Finally, in both countries, surveillance powers are primarily to give intelligence services a better tool to perform their tasks.

In both countries, the Constitutional Tribunals play a balancing role between security and human rights. The decisions of these courts take into account the case-law of the European Court of Human Rights and the Court of Justice of the European Union. Ultimately, these rulings may contribute to limiting the powers of intelligence and police services. The Constitutional Tribunals in both countries drew attention to the need to create mechanisms for independent oversight over surveillance powers. In Slovakia, it led to legislative changes introducing regulations regarding the Special Commission. Legislative changes have also been intro-

duced in Poland. However, they have extended the surveillance powers of the services while the proposed oversight mechanisms have provided fictitious solutions. In practice, the judgment of the Polish Constitutional Tribunal has not been implemented yet. In Slovakia, enforcement difficulties occur at the level of political practice. However, both countries face challenges to implement the appropriate provisions for the surveillance policy. Legal guarantees and oversight mechanisms against excessive surveillance are very modest.

REFERENCES

Aldrich, R. J. & D. Richterova. 2018. „Ambient accountability: intelligence services in Europe and the decline of state secrecy". *West European Politics*, 41 (4): 1003-1024.

Caparini, M. 2014. „Comparing the Democratization of Intelligence Governance in East Central Europe and the Balkans". *Intelligence and National Security*, 29(4): 498-522.

European Commission for Democracy through Law (Venice Commission). 2016. *Opinion on the Act of 15 January 2016 amending the Police Act and certain other acts*, Strasbourg, 13 June 2016 (Opinion no. 839/2016).

European Union Agency for Fundamental Rights. 2017a. *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume I: Member States' legal frameworks*, Luxembourg: Publications Office of the European Union.

European Union Agency for Fundamental Rights. 2017b. *Surveillance by intelligence services: fundamental rights safeguards ad remedies in the EU. Volume II: field perspectives and legal update*, Luxembourg: Publications Office of the European Union.

Gruszczak, A. 2009. „The Polish Intelligence Services". In: *Geheimdienste in Europa. Transformation*, *Kooperation und Kontrolle,* eds. T. Jäger, A. Daun, 126-151. Wiesbaden: FRG: VS Verlag für Sozialwissenschaften.

Gruszczak, A. 2017. „The Polish intelligence services and security dilemmas of a frontline state". *Revista Română de Studii de Intelligence*, 17-18: 65-80.

Kadlečíkovává, J. & I. Rapošová. 2016. *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Slovak Republic*, Version of 10 July 2016.

Kolaszyński, M. 2017. „Constitutional status of Polish intelligence services since 1989: intelligence vs. the police". *Politeja: Global and regional security challenges*, 50 (5): 213-225.

Kolaszyński, M. 2018. „Intelligence Control and Oversight in Poland since 1989". *The International Journal of Intelligence, Security and Public Affairs*, 20 (3): 230-251.

Kolaszyński, M. 2019. „Surveillance Powers of Law Enforcement and Intelligence Services in Poland". In: *Security Outlook* 2018, ed. A. Gruszczak, 127-141. Kraków: Księgarnia Akademicka.

Kovanič, M. 2019. „Digital surveillance and privacy: battle for telecommunications metadata in Slovakia". *V4 Human Rights Review*, 1 (1): 42-44.

Kovanič, M. & A. Coufalova. 2020. „The legitimacy of intelligence surveillance: the fight against terrorism in the Czech Republic and Slovakia", *Intelligence and National Security*, 35 (1): 115-130.

Láštic, E. & M. Kovanič. 2017. „Surveillance in Post-communist Slovakia: Constitutional Law". *European Review of Public Laws*, 29(3): 933-948.

Medvecký, M. & J. Sivoš. 2016. „Slovakia: State Security and Intelligence since 1945". In: *Handbook of European Intelligence Cultures*, eds. B. de Graaff, J. M. Nyce, 335-346. Lanham: Rowman & Littlefield.

Persak K. & Ł. Kamiński (eds.). 2005. A *Handbook of the Communist Security Apparatus in East Central Europe: 1944–1989*. Warszawa: Institute of National Remembrance.

Program Prawa i Sprawiedliwości 2014. Zdrowie. Praca. Rodzina. 2014. [The Party Program of the Law and Justice 2014. Health. Work. Family]: http://pis.org.pl/dokumenty

Sarnecki, P. 2010. „Dostęp do akt dokumentujących działania podjęte przez służby specjalne" [Access to the files documenting activities taken by special services]. In: *Regulamin Sejmu w opiniach Biura Analiz Sejmowych: Vol.* 2, ed. W. Odrowąż-Sypniewski, 128-130. Warsaw: Wydawnictwo Sejmowe.

Svenonius, O., F. Björklund & P. Waszkiewicz. 2014. „Surveillance, lustration and the open society: Poland and Eastern Europe". In: *Histories of State Surveillance in Europe and Beyond*, eds. K. Boersma, R. Van Brakel, C. Fonio & P. Wagenaar, 95-117. London and New York: Routledge.

Williams, K. & D. Deletant. 2001. *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia and Romania*. London: Palgrave Macmillan UK.

Završnik, A. 2013. „Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?". *Journal of Contemporary European Research*, 9 (1): 181-202.

Zybertowicz, A. 2007. „Transformation of the Polish Secret Services: From Authoritarian to Informal Power Networks". In: *Democratic Control of Intelligence Services. Containing Rogue Elephants*, eds. H. Born & M. Caparini, 65-82. Hampshire and Burlington: Ashgate.

Матеуш Колашињски*

Јагелонски универзитет, Краков, Пољска

НАДЗОР НАД ОБАВЕШТАЈНИМ ОВЛАШЋЕЊИМА – СЛУЧАЈЕВИ ПОЉСКЕ И СЛОВАЧКЕ

Резиме

Циљ чланка је да представи најважнија питања у вези са надзором над обавештајним овлашћењима у Пољској и Словачкој. Појам „обавештајна овлашћења“ коришћен у студији односи се на посебне обавештајне технике и праксе сакупљања личних података, које се дешавају без знања или дозволе субјекта. Таква овлашћења су типично у рукама полицијских служби и обавештајних агенција и веома су политички осетљива, али и блиско повезана са кључним питањима моћи и безбедности. Надзор ових служби и њихових овлашћења је стандард у демо[16]кратским државама. Пре 1989-1990. године, постојао је сличан модел безбедносних служби у обе анализиране државе. За време комунизма, није постојао цивилни или демократски надзор над полицијским и обавештајним сектором. Под тим системом, контрола над безбедносним службама је вршена од стране унутрашњег круга људи који је представљао највише нивое Комунистичке партије. Најзад, од раних 1990-тих, Пољска и Словачка морале су да граде нови систем контроле и надзора. Данас, обе земље су чланице Европске уније и Савета Европе. Основно питање овог чланка је да испита како изгледају системи контроле и надзора у Пољској и Словачкој у пост-Сноуденовој ери.

Кључне речи: *обавештајне службе, надзор, Пољска, Словачка*

* mateusz.kolaszynski@uj.edu.pl

* Овај рад је примљен 9. априла 2020. године, а прихваћен за штампу на телефонском састанку Редакције, 13. априла 2020. године.