

Secret surveillance in Poland after Snowden

Between secrecy and transparency

Mateusz Kolaszyński

Introduction

Surveillance powers are typical in the work of law-enforcement agencies and intelligence services around the world. In democratic states, they make it possible to fight against such threats as terrorism, cyber-attacks, organized crime, etc. (Gill and Phythian 2018). To this end, state services use secret surveillance—covert techniques and practices of information gathering about people that occur without the monitored subjects' knowledge or approval. These surveillance powers, typically carried out by law-enforcement and intelligence services, are more sensitive politically, as well as closely related to core issues of power and security (Svenonius and Björklund 2018). However, these state activities may also seriously interfere with fundamental rights, in particular privacy and data protection. Nowadays, technological advancements have generated new threats and, at the same time, have provided means of fighting those threats, making such work increasingly complex. Technological progress means that intelligence services have tools for almost unlimited surveillance. It is the obligation of the state to provide adequate safeguards for people and to enact clear laws in this area (FRA 2017a, 2017b).

This problem has often been described as a conflict between security and human rights (Bigo 2012). However, secret surveillance can also be used to protect human rights, e.g., potential victims of crime or terrorist attacks. Thus, this chapter recasts the conflict in surveillance policy as a dilemma between secrecy and transparency (Matei and Bruneau 2011). Secrecy ensures the effectiveness of security services, and thus agencies lobby for solutions that limit transparency. In turn, explicit provisions regarding surveillance, control mechanisms, and independent oversight can be considered aspects of transparency. Such guarantees can also contribute to increased protection of human rights. The goal of this chapter is to discuss the barriers against overcoming the culture of secrecy in the area of surveillance (Kovanic and Coufalova 2019) with particular focus on Poland, where debates about the Snowden revelations have not succeeded in making surveillance practices more transparent (Gruszczak 2017).

The obligation to provide security for citizens is one of the constitutional values in a democracy, and the effectiveness of security provision sometimes requires secrecy. However, the domination of secrecy over other constitutional values is a systemic and institutional problem. Since 1990, there has been no comprehensive move toward transparency. The construction of modern intelligence services has not been completed in Poland. There is a lack of response to contemporary challenges, including the development of information technologies and international cooperation with the services of other countries, as well as regulatory challenges related to Snowden's revelations.

On the contrary, even after Snowden's revelations security services have increasingly extended surveillance powers (Kolaszyński 2019). Since 2016, the role of the Polish Constitutional Tribunal has been limited. Earlier, the rulings of the tribunal had a substantial impact on limiting surveillance. This makes Poland one of the countries that still has a broad surveillance mandate (Svenonius et al. 2014). In general, successive Polish governments have supported reforms that tend to increase surveillance powers. This practice is mostly influenced by the politicization of law enforcement and, first and foremost, intelligence services. Security services can push for beneficial solutions for themselves, such as unlimited access to information. The success of these policies also derives from the weakness of institutional arrangements, including limited possibilities of the opposition, low public awareness, and a lack of real independent oversight. Overall, there is institutional support for broad surveillance powers and a lack of significant safeguards against such policies in Poland.

The article is structured as follows: the first part will present significant legislative changes in the area of surveillance after 2013; the second part will describe institutional and administrative arrangements that should ensure there is a balance between secrecy and transparency, and therefore the successful governance of surveillance; the third part will show the balancing role of the Constitutional Tribunal prior to 2016 and its limited role ever since.

Legal framework after 2013

Since Snowden's warnings about the extent and dangers of secret surveillance, Poland has had no radical rethinking with respect to secret surveillance practices. Since 1983, Polish law has used the term "preliminary investigation" (*czynności operacyjno-rozpoznawcze*) to refer to secret surveillance. This significant change did not mean that before 1983 security services did not keep citizens under surveillance. Indeed, they frequently operated in such a way but did so without any statutory basis. The Act of 1983 thus did not regulate preliminary investigation in a comprehensive way. The practices of the Security Service (*Shżba Bezpieczeństwa—SB*) in the Polish People's Republic (*Polska Rzeczpospolita Ludowa—PRL*) made that draft regulation almost irrelevant,

since under the communist system secrecy was the norm in the state's surveillance policies (Persak and Kamiński 2005).

In 1990, a new intelligence and police law led to changes in regulations concerning secret surveillance (preliminary investigations). The statutory regulation was expanded, and there were attempts to improve the rules in the ensuing years. The process of declassifying secret surveillance during the political transformation came down to the following key issues: changing the statutory basis for secret surveillance; new intelligence and police services structure that would formally separate preliminary investigations from politics; increasing governmental control and external oversight of secret surveillance. But the reforms also raised doubts regarding the role of transparency in surveillance and did not strike a balance between security and human rights.

With regard to state surveillance, the culture of secrecy and the lack of citizen awareness still dominate, despite a few solutions aimed at enhancing transparency. Very often, extensive surveillance powers are granted without adequate procedural guarantees for the protection of human rights and without creating independent oversight mechanisms over security services. Increasingly, the capabilities of state institutions stem from adopting imprecise, laconic regulations (FRA 2017a). This problem of lack of balance has received attention from several institutions, even if it remains unresolved. At the national level, these institutions are primarily the Constitutional Tribunal, the Commissioner for Human Rights (RPO), the Supreme Audit Office (NIK), NGOs, and some experts. At the international level, relevant institutions include the European Court of Human Rights (ECHR), the Court of Justice of the European Union (CJEU), the Venice Commission, and the European Union Agency for Fundamental Rights (FRA).

This part of the chapter will present the most important legal changes regarding secret surveillance after 2013. Most of them were introduced in 2016 after the election of the conservative Law and Justice party (PiS) in order to increase the scope of state secret surveillance. Earlier, the ruling liberal coalition of the Civic Platform (PO) and the Polish People's Party (PSL) ignored changes in the area of secret surveillance, even though reforms became a necessity as a result of the Constitutional Tribunal's ruling and alarming signals from other institutions, such as the RPO. Current solutions in Poland will be presented in the context of international standards set by the ECHR, the Venice Commission, and the FRA.

A key piece of legislation were the amendments referred to as the Surveillance Act of 2016,¹ which implemented some recommendations included in the Constitutional Tribunal judgment of July 30, 2014 (No. K 23/11), which demanded rigorous reform to surveillance. However, the Act only partially implements the judgment, and the most essential principles formulated in the judgment, which reflected the process of the revision of secret surveillance legislation, were not included. This issue will be discussed in the latter part of the chapter. The Surveillance Act additionally introduced

other legal solutions that the Constitutional Tribunal's judgment did not require or refer to at all, in particular with reference to the scope of intelligence services' access to telecommunications and internet data, which have been significantly extended. This led to the creation of a mechanism for the *ex post* oversight of access to telecommunications and internet data conducted by the regional court based on a biannual statistical report prepared by law enforcement and intelligence services. However, the judicial oversight is illusory due to the limited powers of the regional court, which will be further discussed in the second part of the chapter.

In 2016, the Sejm (lower house of the Polish Parliament) passed numerous other laws that extended the reach of surveillance powers. A notable event was the passage of the amendment to the Code of Criminal Proceedings, introduced in March 2016,² enabling the broader use of surveillance in criminal proceedings (Grabowska-Moroz 2016). The amendment introduced a provision (§168a), which states that evidence cannot be considered inadmissible solely because it was obtained in violation of the rules of criminal procedure or by committing an offense. The only exception is when the evidence has been obtained as a result of murder and/or willfully causing bodily injury or imprisonment in connection with the performance of an official public duty. Moreover, the amendment deleted the so-called “*ex post* consent procedure” conducted by the court. According to the previous law, if operational surveillance—recording the contents of telephone conversations and correspondence conducted via telecommunications networks—provided evidence of a different crime or one committed by a person other than the one under investigation, the decision of the court was required. The Act deleted this procedure and provided that only the consent of a prosecutor is required (§168b).

Another regulation that impacts the oversight system of intelligence services and law enforcement is the new *Law on the Prosecutor's Office*.³ According to this new law, the office of the Prosecutor General is held by the Minister of Justice so that this function is fulfilled by a politician, a member of the government. This dual role is especially important because prosecutors are also entitled to permit the use of some secret surveillance. Their control covers access to classified files containing information gathered during surveillance. Moreover, the new law allows the Prosecutor General to order the competent authorities to conduct secret surveillance operations if they are related to the ongoing investigation (Rzepliński 2003).

On June 10, 2016, the Sejm also adopted the Anti-terrorism Law.⁴ This regulation extends the powers of the Internal Security Agency (ABW) and, at the same time, relaxes oversight requirements, particularly toward foreigners. At least three controversial provisions of this Act are related to secret surveillance and concern the following issues: the confidential register maintained by the ABW, wiretapping (in legal terminology: operational surveillance) of foreigners, and criminal proceedings based only on information from secret surveillance. To prevent “terrorist events,” the head of ABW keeps a

register of persons who may be associated with terrorism.⁵ However, how this confidential register is maintained does not meet the standards set by the ECHR (*Leander v. Sweden*, No. 9248/81). The Anti-terrorism Law regulates the exception by way of a fundamental principle in the Polish legal system, according to which any application of operational surveillance by intelligence services and law enforcement requires the consent of an independent authority (a regional court).⁶ The third significant change introduced by the Anti-terrorism Law “liberalizes” criminal trial procedures.⁷ A person can be charged in criminal proceedings based only on information obtained as a result of secret surveillance. Moreover, information from secret surveillance may be the basis for the prosecutor’s request for detention on remand. Thus, pretrial detention and prosecution may occur based on anonymous data, for example, an officer’s note from a meeting with an informant not disclosed in the case file (Bodnar et al. 2019).

Recently, three new institutions emerged which were granted considerable powers in terms of surveillance: the National Revenue Administration (KAS), the National Security Services (SOP), as well as the Internal Oversight Inspector (BNW), which is subject to the mandate of the Ministry of Internal Affairs. The KAS was created from the merging of two services that used surveillance. Due to the large number of institutions authorized to undertake surveillance in Poland, this combination is generally favorable. The SOP, like the Government Protection Bureau (BOR), is responsible for providing VIP security services for the Polish government (security of incumbent and former Presidents of Poland, high-ranking state officials, etc.). However, the new service has garnered significantly more far-reaching powers. Controversy was aroused when surveillance powers were granted to the SOP, because the BOR did not have such powers. The surveillance powers of the SOP are extensive and include operational surveillance and the collection of metadata. It is particularly worth noting that the new law copied the solutions of other police acts without any new proposals for better safeguards for human rights (Kolaszyński 2019).

The BNW is a part of the Ministry of Internal Affairs and is supposed to keep under surveillance other security services upon the request of the Minister of Internal Affairs. The purpose of this service is to improve and unify ministerial control of other institutions, such as the police, the Polish Border Guard, and the SOP. One of the tasks of the new agency is to control the surveillance activities of the services mentioned above. Seconded police officers, border guards, and SOP officers work primarily in the BNW. Formally, this institution is a part of the internal organization of the Ministry of Interior (Kolaszyński 2019).

The extensive surveillance powers of the BNW are controversial. Since 1990—when civilian control over security services was established—only security services (the police, the Polish Border Guard, and intelligence services) have had surveillance powers. The Minister of Internal Affairs had

the right to intervene in the work of services only when entitled to do so by applicable acts. This solution was designed to separate civil and political management in the ministry from professional and apolitical law enforcement and intelligence services (Widacki 1999). After 1990, control over surveillance powers gradually became the domain of prosecutors and courts. The surveillance powers of the new services under the full control of the Ministry of Internal Affairs work against the model mentioned above. On the one hand, the minister gets the opportunity to view the surveillance materials of the supervised services. On the other hand, the minister's Internal Oversight Inspector—the BNW—also has extensive surveillance powers. For example, this institution can use operational surveillance or partake in collecting meta-data (Kolaszyński 2019).

Surveillance methods form the core of the activity of each service. Problems arising from the monitoring of this activity, that is, controlling the controllers, are visible in many countries (FRA 2017a, 2017b). However, the common standard is oversight exercised by an independent, external body. The appointment of the BNW does not meet this standard. The Ministry of Internal Affairs is politically accountable for the activities of the services controlled by it (the police, the Polish Border Guard, the National Security Bureau). That is why a reliable explanation of violations may conflict with the minister's potential accountability (Kolaszyński 2019).

The legislative changes presented above grant the security services extensive opportunities to use secret surveillance. It is also necessary to indicate areas in which systemic reforms have not been undertaken for many years. Three such areas, where regulations are residual and loose, are essential for surveillance. More clarification of the law on these issues and proper development of regulations would ensure an adequate balance between transparency and secrecy (FRA 2017a, 2017b). The first area is the system of control and oversight over intelligence and police services. More on this subject will be discussed in the second part of the chapter. The law also barely regulates the second area—international cooperation in the Polish security services. Additionally, there is no legal basis for intelligence actions taken abroad. Currently, the law does not control any surveillance methods that are used to collect data outside the country. It also does not require the officers to fulfill any particular responsibilities or comply with bans. Both legislative changes and a lack of initiative in other areas mean that the current legal system may be incompatible with the Polish constitution and international standards in many elements (Lefebvre 2016; Kolaszyński 2019).

Since Snowden, international standards have generally been ignored by the Polish authorities, despite the recommendations of the Polish Ombudsman, NGOs, and experts. A report prepared under the auspices of the ombudsman pointed to many deficiencies in the Polish legal system (Bodnar et al. 2019). Polish law does not conform to international standards relating to the use of wiretaps and operational surveillance (as well as the use of metadata) resulting

from the case law of the ECHR. Moreover, Polish law does not correspond to the standard for the use of metadata by the security services and the protection of information related to professional privilege (e.g., lawyers, journalists) set out in the judgment in the case of *Big Brother Watch and Others v. the United Kingdom* (European Court of Human Rights 2018, application Nos. 25198/0258170/13, 62322/14, and 24960/15). Polish authorities do not implement standards related to the jurisprudence of the CJEU, especially in the field of standards related to telecommunications data based on the so-called retention directive (Court of Justice of the European Union 2014, *Digital Rights Ireland*, Nos. C-293/12 and C-594/12; Court of Justice of the European Union 2016, *Tele2*, Nos. C-203/15 and C-698/15) and procedural protection for persons at risk of expulsion (Court of Justice of the European Union 2013, *ZZ v. Secretary of State*, No. C-300/11). The problems identified by international organizations are also not the subject of reflection. A number of recommendations from the Venice Commission have not been introduced into Polish law. According to the *Opinion of 2016* (Venice Commission 2016), procedural safeguards and material conditions established in the police acts on implementing secret surveillance are still insufficient because they do not prevent excessive use of powers and unjustified interference that conflict with the privacy of individuals.

In Poland, there is a visible departure from European standards regarding secret surveillance (Wetzling and Vieth 2018). The lack of balance between secrecy and transparency is a systemic problem that has been known for years. Intelligence services and law enforcement are increasingly able to use secret surveillance. Additionally, more and more institutions are entitled to undertake such activity. The problem is also that politicians have an increasing impact on the use of surveillance. Moreover, rather than the development of adequate control and oversight mechanisms, there has instead been a deterioration in standards (Bodnar et al. 2019). The second part of this chapter will show how this process is supported by institutional solutions or, oftentimes, a lack of them.

Institutional and systemic challenges

According to Richard J. Aldrich and Daniela Richterova, Snowden's disclosures have not changed the state's interference in personal privacy but have rather exposed the crisis of state secrecy. In their view, "the key issue is not government looking at us, but our increasing ability to look at government, and especially new ways of calling the secret state to account" (Aldrich and Richterova 2018, 1003). A similar opinion can be found in the *Guardian* article about the situation in Poland that was published shortly after Snowden's revelations: "The Prism affair questions the very essence of the contract between societies and their governments: accountability" (Bodnar and Szymielewicz 2013). It does seem that after 2013, the challenges

of creating an oversight system of state surveillance became the primary issue. The way these mechanisms function is a practical reflection of how the state confronts the dilemma between transparency and secrecy.

The problem of the lack of balance between secrecy and transparency can be seen from the perspective of the separation of powers. Each branch has a different role in secret surveillance. Together, the executive, legislative, and judicial branches can provide guarantees against the use of secret surveillance. In turn, possible shortcomings of this system have allowed laws to be passed without a balance between transparency and secrecy (Wegge 2017).

In Poland, there is a serious problem with the politicization of the services. Until 1990, security services were part of ministries and were fully politicized (Gruszczak 2009; Caparini 2014). Formal regulation in 1990 was designed to separate civil and political management in the ministry from professional and apolitical services. This solution was to guarantee that secret surveillance would not be used for current policy (Widacki 1999). This was necessary because of the use of surveillance against the opposition in the communist system (Persak and Kamiński 2005). However, separating politics from intelligence services turned out to be very difficult in practice.

In 1990, the principle was introduced according to which politicians would no longer have complete control over the surveillance of citizens, and it was no longer to be used as a tool in dealing with legitimate political opposition (Widacki 1999). However, some chosen members of the government were given control over surveillance powers, in particular, the Prosecutor General as the Minister of Justice (1990–2010, and since 2016) and the Minister of Internal Affairs (1990–1996, and since 2018). After winning the 2015 election, the PiS government not only reverted to the previous influence of politicians on the secret surveillance apparatus but significantly expanded this influence. The new Law on the Prosecutor's Office discussed above and the establishment of the BNW allow for more far-reaching secret surveillance than before.

Politicians can be influenced by those who decide on secret surveillance in Poland, that is, the heads of the special services. These heads have enormous power over their services as they primarily decide on the scope of the surveillance activity. At the same time, they are not clearly separated from the current policy because there are no significant restrictions on who should be appointed head of a service. A candidate for the position does not have to be an officer of any service, nor demonstrate specific experience, knowledge, etc. It is also quite common that many functions are performed by politicians or other people not directly involved with intelligence services and more connected with current politics.

In Poland, there is a lack of governmental control over secret surveillance. According to Hans Born and Gabriel Geisler Mesevage (2012, 6–7) “oversight” should be distinguished from “control” because “the latter term implies the power to direct an organization's policies and activities. Thus, control is typically associated with the executive branch of government and specifically

with the senior management of intelligence services.” There are practically no permanent, institutionalized forms of control over services responsible for secret surveillance. Since there are so few institutional limitations, different governments enjoy considerable independence in exercising control. As a result, since 1990, law enforcement and intelligence services have been supervised by a number of bodies of various structural and political statuses with unsuitable experience and backgrounds. This means no officials have specialized in control over these institutions.⁸ For example, in the government of Jerzy Buzek (1997–2001), the Board for Special Services (KSS) never met at all (Zybertowicz 2007). The creation of effective control mechanisms is hampered by the lack of political responsibility for special services. In Poland, there have been many scandals related to the impact of special services on political and economic life. However, political responsibility for these events is not typical for politicians who control the services. Andrzej Zybertowicz (2007) calls this phenomenon “the institutionalization of non-accountability” and “self-tasking of the services.”

In this situation, with a lack of permanent control over security services and a lack of political responsibility, the special services gain a considerable advantage over politicians. First of all, they are the only ones who have expert knowledge about intelligence activities, including secret surveillance (Łoś 1995). In Poland, there are still not enough civilian experts and supervisory institutions. The small number of private experts has historical reasons, since before the political transformation security research was dominated by the communist party structures (Matei and Bruneau 2011). At the same time, the security services have centralized and hierarchical structures that minimize access from the outside. In the face of any reform attempts, state security experts present a reliable and determined group of influencers with a high degree of knowledge and power. Mixing these two spheres—politics and special services—can give rise to support for broad surveillance powers. In this tandem, intelligence services enjoy expert knowledge and access to secrets. The government lacks permanent structures, and knowledge about special services is almost impossible to verify. These circumstances make politics vulnerable to manipulation. This situation is further exacerbated by the system of informal relations between these spheres (Zybertowicz 2007).

Such relationships within the executive branch have an impact on parliamentary oversight. In 1995, the Sejm Committee for Special Services (SKSS) was appointed, made up of members of the parliament.⁹ The parliamentary majority has a decisive influence on the work of the committee. Recently, several practices meant to increase the power of the opposition to the work of this body have been abandoned. With the original establishment of the committee, the practice of a six-month rotating chairmanship was introduced. During the fourth term of the Sejm (2001–2005), the additional practice developed by which only the opposition deputies became rotating chairmen

(Kolaszyński 2018). In 2015, however, the parliamentary custom of a rotating chairmanship of the committee was abandoned.

The SKSS formally has a broad mandate regarding oversight of the special services. However, the importance of the committee is not demonstrated by the full range of its work since its powers are limited in practice. The committee's members are formally allowed to demand any information about secret surveillance from the government, the heads of special services, and officers subject to them, but the real power to request this information is limited. In order to disclose any information related to secret surveillance, the head of a given institution has to give their consent. The regulations do specify any particular grounds for either approval or rejection of consent, so the committee might be denied access to information without detailed justification (Sarnecki 2010). Polish parliamentary oversight is very often reduced to trying (and failing) to access the "secrets" of special services. At the same time, the committee has not contributed to initiating a policy debate on government control of secret services. Since 1995, the SKSS has not prepared any public report on the situation of special services and their government control that could initiate a debate on this issue.

The lack of real oversight and parliamentary debate is also evident in the legislative process. Laws on secret surveillance have passed without serious discussion about the balance between secrecy and transparency. Opposition MPs and NGOs are often concerned about the encroachment on human rights associated with excessive secret surveillance. However, their impact on the final form of the law is minimal. The majority of the Sejm supports unequivocally government projects that give broad powers to security services. The ultimate argument for supporters of governmental projects is often populist rhetoric, i.e., if someone disagrees with the broad powers of a particular service, then he or she is a supporter of criminals. This approach was evident during the legislative work on the Central Anti-Corruption Bureau (CBA) Act in 2006. Criticism of the extensive powers of this institution was often rejected with arguments such as "honest people have nothing to fear" or "only a supporter of corruption may have doubts about the broad powers of the CBA." Eventually, despite its unprecedented broad powers in Poland, the CBA Act was passed with the support of a significant part of the opposition.

Populist rhetoric is effective due to public opinion. Knowledge about the activities of intelligence services is not common. In general, citizens do not know what functions the security services other than the police perform, nor is there widespread knowledge of the umbrella mechanisms of control and oversight. This problem is characteristic of many Central and Eastern European countries (Matei and Bruneau 2011). One of the main reasons for this is the government and intelligence services' information policy, which leaves a lot to be desired. There is a culture of secrecy in this area because even the necessary information on the activities of special services is not provided. The need for confidentiality often masks incompetence. This also applies to

proactive information policy, which is, to some extent, carried out by only two services, the ABW and the CBA (Matei and Bruneau 2011).

The secret surveillance issue is not popular with the public. This factor reduces the pressure on the government to seek a balance between broad powers and human rights. According to the Public Opinion Research Center (CBOS), the majority of voters support broad surveillance powers. In the opinion of Poles, there is no need to change surveillance capabilities, and security services should have wide surveillance powers. This is particularly apparent with regard to internet surveillance. According to CBOS, when faced with a choice between, on the one hand, increased possibilities for internet surveillance for the police and other services in order to combat crime and, on the other hand, decreased control of online communication to protect users' privacy, Poles usually choose the first option (46% vs. 30%).¹⁰ Moreover, half of the respondents think that the current powers of police services and intelligence agencies to gather information about internet users are acceptable. It is important to note that this CBOS research was carried out in April 2016 after the reform that introduced the so-called Surveillance Act. In general, surveillance is not an issue that is particularly important for Poles. Shortly after the introduction of the Surveillance Act, 54% of Poles didn't know anything about this law (27% of Poles had heard of it but did not know what the changes were; only 19% of Poles had heard of it and had some idea of the changes introduced) (CBOS 2016, 5). A large group of Poles are not interested in the issue of surveillance whatsoever. It seems that lack of awareness is a crucial factor in assessing the attitude of Poles toward this problem (Svenonius and Björklund 2018).

This indifference can be gradually reduced by the activities of NGOs and media pluralism. More and more NGOs are comprehensively monitoring the issue of surveillance. The largest of them include the Panoptykon Foundation, the Helsinki Foundation for Human Rights, and Amnesty International. They use the Act on access to public information.¹¹ As a result, the media has often proved a more effective oversight tool than the overall formal control and oversight mechanisms (Matei and Bruneau 2011). Most of the evidence of irregularities associated with security services originated in media reports (Hillebrand 2012).

The balance between secrecy and transparency is also distorted due to the weakness of independent oversight. In 2001–2002 some responsibilities related to secret surveillance—operational surveillance—were transferred from the Prosecutor General to the courts. The Prosecutor General was no longer supposed to authorize this power but merely provided an opinion on the motions submitted to the court by the various services. This method officially guaranteed external, independent oversight over this area of secret surveillance, which impinges upon human rights to the greatest extent. However, there is a lack of actual judiciary oversight in practice. Judiciary oversight is exercised by the criminal divisions of regional courts, mostly dealing with

criminal cases. There are no other specially designed departments or other structures that would be responsible for giving consent to operational surveillance. For this reason, such duties are treated as peripheral and secondary tasks. Moreover, the courts are not able to review all materials regarding a particular case. They can only examine what the services show them. Ultimately, this oversight is illusory. Publicly available statistics confirm this thesis—the courts accept about 99% of the requests from the heads of secret services for the application of operational surveillance (Rojszczak 2021).

In Poland, no independent body has yet been established to examine citizens' complaints about the surveillance activities of security services. There is still no effective external oversight of access to telecommunications, posts, and internet data, as that guaranteed by law since 2016 is mostly illusory. This monitoring is exercised only *ex post* and randomly; the lack of prior and individual oversight is not the only deficiency with regard to current solutions (Bodnar et al. 2019). Both types of judicial oversight—that established in 2001 over operational surveillance and the one established in 2016 over telecommunications, internet, and postal data—share the same limitations. In both cases, permanent organizational structures that would deal with this type of activity were not guaranteed in the acts. Moreover, no additional financial and human resources were provided for this purpose. Ensuring adequate organizational structures to enable permanent oversight is justified by the scale of the security services' activities: in 2017, special and police services acquired over 1.2 million pieces of data. As for operational surveillance, the police alone filed nearly 10,000 wiretapping applications in 2017 (Bodnar et al. 2019; Kolaszyński 2019).

In Poland, there is no specialized, independent institution that would deal only with the oversight of secret surveillance. In many countries, such external bodies have been created. Currently, one or more such institutions dedicated to security services operate in 16 EU countries. Only some aspects of secret surveillance work also used to be monitored by an independent constitutional body—the NIK and the RPO. Their role is essential, but neither is authorized to carry out any regular oversight of the services (Kolaszyński 2018).

The role of the Constitutional Tribunal

According to some researchers, breaking the secrecy culture exceeds the capabilities of any institution in Poland (Zybertowicz 2007). However, it is worth noting the role of the Constitutional Tribunal in regulating surveillance. This institution has played one of the most significant functions in developing the statutory basis for secret surveillance over the last 30 years. The tribunal has often contributed to the introduction of changes in the regulations and, consequently, the move toward more of a focus on the protection of human rights (judgments No. W 12/94, No. K 45/02, and No. W 54/07). The tribunal's case law has significantly reduced surveillance powers and was of fundamental

importance for statutory changes in the matter of surveillance. However, in 2016 the function of the tribunal in this field was actually suspended. The paralysis of the constitutional court is the most severe change in surveillance policy since Snowden and can explain the expansion of surveillance powers in recent years.

Before 2016, the tribunal decided to limit surveillance powers on several occasions. Two representative cases will be presented below. In both cases, these were sentences issued shortly after the establishment of new special services: the Internal Security Agency (ABW) and the Foreign Intelligence Agency (AW) (2002) and the Central Anti-Corruption Bureau (CBA) (2006). The judgment of the Constitutional Tribunal of April 20, 2004 (No. K 45/02) considered the appointment of political heads to security agencies as nonconstitutional. According to the tribunal, assigning the heads the role of secretaries of state was a sign of circumventing the constitutional ban on joining the parliamentary mandate with employment in a government agency, and the post of head of special services had not been prepared for politicians. This also applies to the use by politicians of intelligence services and their surveillance powers. This ruling was welcomed by constitutionalists (Radziewicz 2004), and since then, the heads of the ABW and AW have not been secretaries of state with political functions.

As with the establishment of the ABW and AW, the Constitutional Tribunal examined the constitutionality of the Act on the CBA. In a judgment on June 23, 2009 (No. K 54/07), the Constitutional Tribunal ruled that the definition of corruption in the CBA Act was unconstitutional because the definition was unclear and ambiguous, resulting in CBA's broad scope of competence. This legal definition played a fundamental role in determining the scope of the CBA's tasks. In this context, the court also ruled on surveillance powers. It considered the use of sensitive data and information obtained as a result of performing surveillance activities without instruments for controlling how these data are stored and verified unconstitutional. This problem also concerned the method of deleting unnecessary data due to the statutory tasks of the CBA. Based on this judgment, the CBA Act was thoroughly amended. This amendment introduced to the CBA somewhat independent, internal control of the rights related to the collection and processing of personal data.

The Constitutional Tribunal judgment of July 30, 2014 (No. K 23/11), which was issued after the Snowden revelations, could have had a similar impact. In this case, the tribunal ruled at the request of the Polish Ombudsman comprehensively concerning surveillance powers. In this judgment, the tribunal specified essential principles that must be jointly met by provisions that regulate acquiring information on individuals in secrecy by public authorities in a democratic state ruled by law. The judgment required the introduction of changes in the law, which concerned the introduction of a mechanism of independent oversight over access to telecommunications data by police and special services officers; clarification in the law of the types of crimes detrimental

to the economic foundations of the state, in respect of which the ABW may conduct surveillance control; introduction of a mechanism guaranteeing the protection of attorney–client privilege; and introduction of a procedure for the destruction of redundant telecommunications data. Furthermore, the tribunal’s judgment contained many recommendations regarding limitations on the use of operational surveillance.

As noted above, the 2016 Surveillance Act implemented some recommendations included in this judgment. The difference from previous rulings of the Constitutional Tribunal lies in the fact that this judgment was only partially implemented—the Polish legislature did not include the essential principles of secret surveillance. Moreover, the Surveillance Act introduces other legal specifications that the Constitutional Tribunal’s judgment did not require or refer to at all (Bodnar et al. 2019). In February 2016, the Polish Ombudsman referred the most important provisions of the Surveillance Act to the Constitutional Tribunal. In his words, the reform not only fails to execute the judgment of the Constitutional Tribunal of 2014, but also “seriously violates the constitutional rights and freedoms and the standards set out in international law.”¹² According to the ombudsman, in the Polish legal system there is still a shortage of legal safeguards that would ensure that surveillance measures do not violate fundamental rights. However, in March 2018, the ombudsman withdrew his application from the Constitutional Tribunal. He stated there was no chance of an independent and substantive judgment of the Constitutional Tribunal. This decision is related to the dispute surrounding the Constitutional Tribunal in Poland. The withdrawal of the application is significant if we take into account the role of the Constitutional Tribunal in limiting the powers of surveillance. Until now, it has been one of the key institutions that make up the oversight system of police and intelligence services. In the same year, the ombudsman withdrew the motions for all legal changes discussed in part one of the work: the Code of Criminal Procedure (April 2018–Article 168a and May 2018–Article 168b); the Anti-terrorism Act (April 2018); and the Act on the Prosecutor’s Office (October 2018). The reason for all these decisions was changes in the composition of the previously appointed Constitutional Tribunal and the fact that unauthorized persons were appointed on political grounds.

Conclusion

A culture of secrecy still dominates Polish surveillance policy. This is connected with the still-dominant logic and interests of the security services, as secret surveillance is primarily used to combat crime and other threats to national security in an effective way. Such an approach is supported by the government, which has limited the influence of alternative expert knowledge. Ultimately, this leads to the adoption of laws that provide extensive surveillance powers without sufficient institutional or administrative mechanisms to govern surveillance practices and prevent abuse.

The pressure toward a more transparent approach to surveillance is still weak due to many factors. The political opposition still has a limited influence on the shape of surveillance law. Public opinion has little interest in this issue, which weakens potential pressure on the government. Also, independent oversight, which only exists formally, does not play any substantial role; it does not allow reliable conclusions based on verifiable facts, and it falls short of professional control mechanisms with appropriate substantive facilities and proper procedures. In addition to all this, the activities of the Constitutional Tribunal—which has in the past played an important role in limiting surveillance and protecting rights—have recently been paralyzed, resulting in a continued imbalance between transparency and secrecy in surveillance.

Notes

- 1 The Act of 15 January 2016 Amending the Police Act and certain other acts (the so-called Surveillance Act).
- 2 Act of 11 March 2016 amending Code of Criminal Procedure and other acts, Journal of Laws, item 437.
- 3 Act of 28 January 2016 Law on Prosecutor Office, Journal of Laws of 2017, item 1767 as amended.
- 4 Act of 10 June 2016 on antiterrorist action, Journal of Laws of 2018, item 452 as amended.
- 5 Act of 6 June 2016 on antiterrorist action, Journal of Laws of 2018, item 452 as amended.
- 6 Article 9 of Act of 10 June 2016 on antiterrorist action, Journal of Laws of 2018, item 452 as amended.
- 7 Article 26 of Act of 10 June 2016 on antiterrorist action, Journal of Laws of 2018, item 452 as amended.
- 8 In 2014, the NIK ran an oversight of control regarding special services (ABW, AW, CBA, and others). Due to classified data protection, the results were never disclosed. They only issued one public statement, which claims that rules in force limit the Prime Minister's power to control special services effectively.
- 9 Article 95, second paragraph of the Constitution of the Republic of Poland of April 2, 1997 (Journal of Laws, no. 78, item 483 as amended) states that the Sejm is responsible for government oversight.
- 10 Fieldwork for national sample: April 2016, N = 1104. The random address sample is representative of the adult population of Poland. For more information see CBOS 2016.
- 11 The Act of September 6, 2001 on Access to Public Information, Journal of Laws of 2019, item 1429.
- 12 The Commissioner for Human Rights application, No K 9/16, p. 6.

References

- Aldrich, Richard J., and Daniela Richterova. 2018. "Ambient Accountability: Intelligence Services in Europe and the Decline of State Secrecy." *West European Politics*, 41(4): 1003–24.

- Bigo, Didier. 2012. "Security, Surveillance and Democracy." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty, and David Lyon, 277–84. New York: Routledge.
- Bodnar, Adam, and Katarzyna Szymielewicz. 2013. "Poland's Citizens Need to Know the Impact of Prism on Their Lives." *The Guardian*, 16 October, www.theguardian.com/commentisfree/2013/oct/16/pires-prism-poland-surveillance-threat.
- Bodnar, Adam, Tomasz Borkowski, Jacek Cichocki, Wojciech Klicki, Piotr Kładoczny, Adam Rapacki, and Zuzanna Rudzińska-Bluszcz. 2019. "Osiodłać Pegaza: Przestrzeganie praw obywatelskich w działalności służb specjalnych—założenia reformy [How to Saddle Pegasus: Observance of Civil Rights in the Activities of Security Services: Objectives of the Reform]." Warsaw: Commissioner for Human Rights, www.rpo.gov.pl/pl/content/powolajmy-niezalezna-instytucje-do-nadzoru-sluzb-specjalnych-propozycja-ekspertow-i-rpo.
- Born, Hans, and Gabriel G. Mesevage. 2012. "Introducing Intelligence Oversight." In *Overseeing Intelligence Services. A Toolkit*, edited by Hans Born, and Aidan Wills, 3–22. Geneva: DCAF.
- Caparini, Marina. 2014. "Comparing the Democratization of Intelligence Governance in East Central Europe and the Balkans." *Intelligence and National Security*, 29(4): 498–522.
- CBOS—Public Opinion Research Center. 2016. "Internet Surveillance." May 2016, www.cbos.pl/EN/publications/reports/2016/072_16.pdf.
- Court of Justice of the European Union. 2013. "Case of ZZ v. Secretary of State for the Home Department." Judgment of 4 June, 2013 (no.C-300/11).
- Court of Justice of the European Union. 2014. "Case of Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others." Judgment of 8 April, 2014 r. (no. C-293/12 and C-594/12).
- Court of Justice of the European Union. 2016. "Case of Tele2 Sverige AB v. Post-och telestyrelsen oraz Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis." Judgment of 21 December, 2016 (no. C-203/15 and C-698/15).
- European Court of Human Rights. 2018. "Case of Big Brother Watch and Others v. The United Kingdom." Judgment of 13 September, 2018 (application nos. 25198/0258170/13, 62322/14 and 24960/15).
- FRA—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.
- FRA—European Union Agency for Fundamental Rights. 2017b. *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Update*. Luxembourg: Publications Office of the European Union.
- Gill, Peter, and Mark Phythian. 2018. *Intelligence in an Insecure World*. Cambridge-Medford: Polity Press.
- Grabowska-Moroz, Barbara. 2016. "National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies, Legal Update Poland." https://fra.europa.eu/sites/default/files/fra_uploads/poland-study-data-surveillance-ii-legal-update-pl.pdf

- Gruszczak, Artur. 2009. "The Polish Intelligence Services." In *Geheimdienste in Europa. Transformation, Kooperation und Kontrolle*, edited by Thomas Jäger and Anna Daun, 126–51. Wiesbaden: FRG: VS Verlag für Sozialwissenschaften.
- Gruszczak, Artur. 2017. "The Polish Intelligence Services and Security Dilemmas of a Frontline State." *Romanian Intelligence Studies Review*, 17–18: 65–80.
- Hillebrand, Claudia. 2012. "The Role of News Media in Intelligence Oversight." *Intelligence and National Security*, 27(5): 689–706.
- Kolaszyński, Mateusz. 2019. "Surveillance Powers of Law Enforcement and Intelligence Services in Poland." In: *Security Outlook 2018*, edited by Artur Gruszczak, 127–41. Kraków: Księgarnia Akademicka.
- Kolaszyński, Mateusz. 2018. "Intelligence Control and Oversight in Poland since 1989." *The International Journal of Intelligence, Security and Public Affairs*, 20(3): 230–51.
- Kovanic, Martin, and Aneta Coufalova. 2019. "The Legitimacy of Intelligence Surveillance: The Fight Against Terrorism in the Czech Republic and Slovakia." *Intelligence and National Security*, 34(6): 115–30.
- Lefebvre, Stéphane. 2016. "Poland's Attempts to Develop a Democratic and Effective Intelligence System, Phase 1: 1989–1999." *International Journal of Intelligence and Counterintelligence*, 29(3): 470–502.
- Łoś, Maria. 1995. "Lustration and Truth Claims: Unfinished Revolutions in Central Europe." *Law and Social Inquiry*, 20(1): 117–61.
- Matei, Florina C., and Thomas Bruneau. 2011. "Intelligence Reform in New Democracies: Factors Supporting or Arresting Progress." *Democratization*, 18(3): 602–30.
- Persak, Krzysztof, and Łukasz Kamiński. 2005. *A Handbook of the Communist Security Apparatus in East Central Europe: 1944–1989*. Warsaw: Institute of National Remembrance.
- Radzewicz, Piotr. 2004. "Głosa do wyroku Trybunału Konstytucyjnego z 20 kwietnia 2004 r. (sygn. akt K 45/02) [Gloss to the Verdict of the Constitutional Tribunal of April 20, 2004 (Act Call No. K 45/02)]." *Przegląd Sejmowy*, 65(6): 163–71.
- Rojszczak, Marcin. 2021. "Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland." *Democracy and Security*, 17(1): 1–29.
- Rzepliński, Andrzej. 2003. "Security Services in Poland and Their Oversight." In *Democracy, Law and Security: Internal Security Services in Contemporary Europe*, edited by Jean P. Brodeur, Peter Gill, and Dennis Töllborg, 110–40. Burlington: Ashgate.
- Sarnecki, Paweł. 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 [The Sejm Regulations According to the Bureau of Research of the Chancellery of the Sejm: Vol. 2]*, edited by Wojciech Odrowąż-Sypniewski, 128–30. Warsaw: Wydawnictwo Sejmowe.
- Svenonius, Ola, and Fredrika Björklund. 2018. "Explaining Attitudes to Secret Surveillance in Post-Communist Societies." *East European Politics*, 34(2): 123–51.
- Svenonius, Ola, Fredrika Björklund, and Paweł Waszkiewicz. 2014. "Surveillance, Lustration and the Open Society: Poland and Eastern Europe." In *Histories of State Surveillance in Europe and Beyond*, edited by Kees Boersma, Rosamunde van Brakel, Chiara Fonio, and Pieter Wagenaar, 95–117. London and New York: Routledge.

- Venice Commission–European Commission for Democracy Through Law. 2016. “Opinion on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts.” Strasbourg, June 13, 2016 (Opinion no. 839/2016).
- Wegge, Njord. 2017. “Intelligence Oversight and the Security of the State.” *International Journal of Intelligence and Counterintelligence*, 30(4): 687–700.
- Wetzling, Thorsten, and Kilian Vieth. 2018. “Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations.” *Heinrich Böll Stiftung*, www.stiftung-nv.de/en/publication/upping-ante-bulk-surveillance-international-compendium-good-legal-safeguards-and.
- Widacki, Jan. 1999. “System bezpieczeństwa wewnętrznego: ewolucja struktur i funkcji [System of Internal Security: An Evolution of Structures and Functions].” In *Druga fala polskich reform [The Second Wave of Polish Reforms]*, edited by Lena Kolarska-Bobińska, 216–40. Warsaw: Institute of Public Affairs.
- Zybertowicz, Andrzej. 2007. “Transformation of the Polish Secret Services: From Authoritarian to Informal Power Networks.” In *Democratic Control of Intelligence Services: Containing Rogue Elephants*, edited by Hans Born and Marina Caparini, 65–82. Hampshire and Burlington: Ashgate.