SAFE AND FREE:
NATIONAL SECURITY SURVEILLANCE AND THE RULE OF LAW ACROSS DEMOCRATIC STATES

The University of Texas at Austin
Strauss CENTER
for International Security and Law

ELECTRONIC SURVEILLANCE IN POLAND

Artur Gruszczak

ABOUT THE AUTHOR

Artur Gruszczak is Professor of Social Sciences, Chair of National Security at the Faculty of International and Political Studies, Jagiellonian University in Krakow. He has provided expertise in security and intelligence matters for the Polish Ministry for Foreign Affairs and Ministry for Internal Affairs, the Office of the Polish Prime Minister, the Polish Ombudsman, the European Parliament and independent analytical institutions, such as Statewatch, Oxford Analytica and GLOBSEC. Currently he is an expert of the Parliamentary Group for the Reform of Special Services in the Polish Parliament.

His principal interests and research areas include: Euro-atlantic security; modern warfare; international intelligence cooperation. He published extensively on these topics. He is the author of *Intelligence Security in the European Union. Building a Strategic Intelligence Community* (Palgrave Macmillan 2016).

ACKNOWLEDGEMENTS

This project was supported by funds from the Robert Strauss Endowment at the University of Texas at Austin and by a charitable gift from Microsoft. Each paper in the Safe and Free series reflects the views of its author. Editorial direction for the series was provided by Adam Klein, Director of the Robert Strauss Center for International Security and Law at the University of Texas at Austin. We are grateful to Strauss Center staff members Ali Prince and Brittany Horton, and to associate editors Zachary Badore, Seth Greenwald, and Taylor Helmcamp, for their help in shepherding the Safe and Free series to publication.

CONTENTS

3	I. Introduction
5	II. Institutions
7	III. Relevant Law
9	IV. Surveillance Process
11	V. Oversight and Transparency
15	VI. Reforms
16	VII. Conclusions

NOVEMBER 2023

I. INTRODUCTION

Electronic surveillance is conducted in Poland on a relatively large scale, mostly as a method practiced by law-enforcement services for preventing and combating crime, as well as for protecting the state and national security against foreign interference. However, electronic surveillance has become a tool of political struggle, especially since the Law and Justice (PiS) party's electoral victory in 2015. Poland has experienced a democratic backsliding marked by the ongoing constitutional crisis, political control over the judiciary, and defiant posture towards European law.[1] This disquieting process has exerted considerable impact on Polish intelligence and security services in terms of their organization, institutional arrangements, human resources, professionalism, and – last but not least – legality of their activities.

Since the transition to democracy in Poland in the early 1990s, the intelligence services have grappled with the problem of their questionable reputation and effectiveness. Initially, the Communist past was a burdensome factor in the organization of intelligence apparatus. The right-wing government's 2006 reorganization of the defense intelligence services provoked new troubles: sensitive information concerning intelligence officers and their activities was disclosed in a government report on the disbanded military intelligence organizations. This shook the reputation of the Polish authorities and weakened the confidence of the allies in the newly established intelligence services as a reliable partner.

After 2015, the new right-wing ruling coalition eroded safeguards against politicization of intelligence services, especially those involved in domestic activities. Due to the significant outflow of personnel (partially subject to the lack of professionalism of newly appointed officers), the special services struggled to operate effectively and reliably. Underfunded and often mismanaged, they were increasingly vulnerable to external threats and prone to internal failures. Several domestic spy scandals and leaks revealed serious flaws in counterintelligence. Reliance on commercial support from foreign contractors showed in-house technological shortcomings.

Legal reforms introduced in 2016 extended to some extent the powers of intelligence and law-enforcement services, especially in the area of electronic surveillance. Concurrently, they weakened privacy safeguards and civil liberties guarantees. What is particularly problematic regarding Polish intelligence

services is the lack of organizational and functional separation between the special services and law enforcement authorities. Hence, what is commonly considered a safeguard against the risk of arbitrary use of information obtained in secrecy is instead to be a serious deficiency in the Polish case.[2] As Mateusz Kolaszyński rightly ascertains, "[s]uccessive Polish governments have supported reforms that tend to increase surveillance powers…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 the political weakness 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."[3]

Electronic surveillance in Poland is mostly exerted domestically. Scant information on overseas surveillance conducted by intelligence agencies (both civil and military) allows for a tentative conclusion about underdevelopment of personal, technical, and financial capacities and reliance on Poland's allies. Hence, electronic surveillance is mostly a method used for purposes of "operational surveillance" by special services and other state security agencies responsible for law enforcement and the protection of public order. Electronic surveillance is heavily used by these services, with limited control and oversight.

II. INSTITUTIONS

The Polish system of intelligence agencies and security services is complex and opaque. It encompasses roughly a dozen institutions empowered with specific competencies regarding intelligence, surveillance, and law enforcement. Few other countries have such a variety of institutions wielding surveillance powers.

The status of "special services" is given to five entities: two of them are foreign intelligence agencies (the civilian Intelligence Agency, AW, and the Military Intelligence Service, SWW), and two others perform counter-intelligence tasks (the Military Counter-Intelligence Service, SKW, and the Internal Security Agency, ABW). The ABW is focused on counterintelligence, law-enforcement activities in the investigative stage, and the protection of classified information.

The last special service is the Central Anti-Corruption Bureau (CBA), another law-enforcement body. CBA specializes in combating corruption, fraud, swindling, and embezzlement of public funds. These five services are authorized to use electronic surveillance for operational purposes. The foreign intelligence agencies

The Polish system of intelligence agencies and security services is complex and opaque. It encompasses roughly a dozen institutions empowered with specific competencies regarding intelligence, surveillance, and law enforcement. Few other countries have such a variety of institutions wielding surveillance powers.

(AW and SWW) are allowed to use electronic and signals intelligence abroad or in Polish territory only if the operational activities abroad so require. Moreover, they need to request ABW or SKW to carry out such activities within Poland.

Apart from the special services, several law-enforcement institutions and security forces are endowed with powers to use surveillance techniques and tools for operational activities.They include: Police, Border Guards, National Revenue Administration, Military Police, Office for Internal Oversight of the Ministry of the Interior and Administration, State Protection Service, and Penitentiary Service (specifically, its Internal Inspectorate). For simplicity, I will continue to use the general term "security services" for the above-mentioned special services, law-enforcement agencies, and security forces.

This institutional mosaic makes it difficult to coordinate the activities of all security services in a timely and efficient manner. Formally, it is the Prime Minister who appoints the heads of the special services and other security agencies, either directly (in the cases of ABW, AW and CBA) or at the request of a competent Minister. The latter exercises supervision of the head of a relevant service, draws up guidelines, formulates and implements operational plans, and authorizes the use of appropriate methods and tools, including electronic surveillance.

Polish law endows the Prime Minister with substantial oversight capabilities, including those related to direct supervision, as well as to the oversight of activities of the special services. However, the Supreme Audit Office, in a classified report produced in 2014, found that oversight exercised by the Prime Minister lacks efficacy, since s/he neither possesses full knowledge of the internal procedures applied by the special services, nor verifies accuracy of operational activities in the completed cases. Essentially, the legal provisions concerning supervision of the special services deprive the Prime Minister of effective oversight and control powers with regard to many activity areas of those services.

Given the entangled structure of the security services, a Minister-Coordinator for Special Services may be established within the government to fulfill tasks assigned by the Prime Minister concerning supervision over the civilian services and control over the military services, as well as their cooperation with other security agencies. Currently this role is assigned to the Minister for Internal Affairs and Administration.

The executive branch also has an advisory and consultative body at its disposal. This is the Council for Special Services, which is connected to the Chancellery of the Prime Minister and chaired by the head of the government. The Council is entitled to give its opinion and advice covering matters of programing,

supervision, and coordination of activities of the special services and other relevant agencies charged with protection of state security.

A significant difference exists between the civilian and military components of the special services. The civilian agencies (ABW, AW and CBA) are directly subordinated to the Prime Minister. By contrast, the two military special services (SWW and SKW), responsible for the protection of the Armed Forces and the proper functioning of the national defense structures, are accountable to the Minister for National Defense. Concomitantly, law-enforcement institutions and security guards are answerable to the Minister for Internal Affairs and Administration.

The civilian foreign intelligence service, AW, is charged by statute with the task of "providing electronic surveillance."[4] However, that term is not further clarified in secondary law, making it susceptible to further interpretations of the contents and meaning of this category.

Likewise, military intelligence (SWW) is authorized to "provide electronic surveillance for the Armed Forces of the Republic of Poland" and military counterintelligence (SKW) is empowered to "carry out counter-signals intelligence."[5] The latter is permitted to observe and record by technical means the image of events in public places and the sound accompanying these events during operational and reconnaissance activities. The remaining two special services, focused on law enforcement, were also granted significant surveillance powers. ABW is authorized to "obtain, analyze, process and transfer to the competent authorities information that may be relevant to internal security of the state and to its constitutional order," which includes the gathering of data and information through the use of electronic devices.

Lastly, CBA, the anti-corruption agency, is empowered to undertake operational surveillance[6] which is conducted in secrecy and consists of monitoring the means of communication and other elements of telecommunications networks, such as computers and IT systems, telephones, databases, e-mails etc., in order to obtain and record the content of conversations, images and voices of people, and electronic communications.

Operational surveillance can also be conducted by other law-enforcement bodies and security forces. They are authorized to collect, process and share metadata regarding telecommunications, such as geographical location of mobile devices, dialed numbers, duration of calls, URLs of visited websites, log-ins, e-mail addresses, etc.

III. RELEVANT LAW

The Polish Constitution of 1997[7] guarantees the right to legal protection of private life of everyone, as well as freedom and privacy of communication. Any limitations may be imposed only for the sake of state security and public order, or public morals.

Poland is also party to international agreements on human rights, including the European Convention for the Protection of Human Rights and Fundamental Freedoms. As a member of the European Union, Poland is obliged to respect EU law and its provisions concerning human rights, enshrined in the preamble and in Article 6 of the Treaty on European Union. Poland is partially exempted from the Charter of Fundamental Rights (by force of an opt-out protocol to the Lisbon treaty), which includes respect for private and family life (Article 7) and the protection of personal data (Article 8). However, the effect of the opt-out on the Charter's applicability in Poland is disputed[8] and has become one of the most salient aspects of the protracted friction between the EU and the Polish government.

Electronic surveillance is regulated by several statutes. The Act of 2002 on the Internal Security Agency and the Intelligence Agency, the Act of 2006 on the Military Intelligence Service and the Military Counter-Intelligence Service, and the Act of 2006 on the Central Anti-Corruption Bureau all contain provisions concerning electronic surveillance and signals intelligence. However, those provisions are general and devoid of legal precision.

The judgement of the Constitutional Tribunal delivered in 2014 in case no. K 23/11 declared the provisions on data retention unconstitutional and required appropriate legislative amendments.[9] However, with the change of government in 2015, the new laws adopted in 2016 did not implement the main conclusions of the judgement; instead, they broadened the powers of the special services and relevant law-enforcement bodies.[10] The so-called Surveillance Law of January 2016, which amended the Police Act of 1990 and the constitutive laws of other security institutions, expanded access of the security services to communications data.[11] They were authorized to collect and process metadata from electronic communications via the Internet, including those unrelated to any crime. Metadata could be downloaded automatically through electronic communication operators and service providers without any individual permission or authorization and without any control of the legality of this process by the operators and providers.[12]

> ***As a member of the European Union, Poland is obliged to respect EU law and its provisions concerning human rights, enshrined in the preamble and in Article 6 of the Treaty on European Union.***

The powers of the special services further increased as a result of the Act on Anti-Terrorist Activities adopted in May 2016. The Internal Security Agency (ABW) was authorized to order wiretapping of foreigners suspected of terrorist activities without court warrants.[13] The Head of ABW was obliged to keep a confidential register of persons who may be associated with terrorism. Yet, in creating and maintaining such register, ABW was exempt from the obligation to respect the principles of necessity and proportionality.

The Act also made it easier to use the fruits of electronic surveillance in criminal prosecutions. For the first time, foreigners as criminal suspects could be charged on the basis of information gathered during a wiretap. Moreover, such information might be sufficient to commence a criminal investigation, including for the prosecutor's request for pre-trial detention.[14]

Yet another noteworthy legislative change came with an amendment to the Code of Criminal Proceedings, which legalized the so-called "fruits of the poisonous tree."[15] This meant that evidence obtained during electronic surveillance in breach of the law could be subsequently used in criminal proceedings, subject to the prosecutor's decision. This should be read in conjunction with another legislative change enacted in 2016, which amended the Act on the Prosecutor's Office. As a result, a prosecutor does not bear a disciplinary responsibility for blatant infringements of the law, insofar as s/he acts in pursuit of the "public interest." The same amendment merged the office of the Public Prosecutor General with that of the Minister for Justice, which meant that the Prosecutor General was a member of the government, representing the executive branch dominated by the ruling coalition. Overall, politicization of the judiciary considerably weakened independent judicial review of the actions of the special services and other relevant security forces, thus exposing citizens to the risk of unlawful acts and abuse of administrative powers.

IV. SURVEILLANCE PROCESS

Electronic surveillance of domestic targets takes two forms: (1) bulk metadata collection, consisting mostly of acquiring and processing communications data; (2) targeted operational wiretapping.

Targeted Wiretapping

Targeted wiretapping follows the procedure established by the Police Act and appropriate Acts concerning the security services. The head of each special service or appropriate security institution submits an application to the district court in Warsaw. In the case of military services (SKW and the Military Police) it is the Military Court in Warsaw. The heads of two security services, the Police and the Border Guard, can lodge an application to other district courts. Before seeking a court order, however, the head of each security service must obtain written consent from the public prosecutor.

The huge majority of the applications (97% on average) are approved by the courts. This is due to the procedure itself. The judges are obliged to issue a positive decision if an application is correct in formal terms and in conformity with the principles of proportionality and subsidiarity (i.e., the least-intrusive means). Typically, the court will reject an application only if there are glaring legal defects. The requesting service may then correct the application and re-submit it.

The maximum period of operational surveillance is 18 months, implemented in several phases. Surveillance by the counterintelligence services (ABW, SKW) may be extended for an additional 12 months. Each extension requires appropriate justification and follows the ordinary procedure, i.e., the court takes the decision, acting at the request of the competent institution, after the service has received consent from the prosecutor. In practice, this means that counterintelligence surveillance may last years.

> ***The number of applications for operational surveillance has increased in recent years. In 2021, there were 7,000.***

The number of applications for operational surveillance has increased in recent years. In 2021, there were 7,000. Most applications of operational surveillance come from the Police (85% in 2021), followed by the Border Guard (4.1%), Anti-Corruption Bureau (CBA, with 3.1%) and Internal Security Agency (ABW, with 2.5%).[17]

Bulk Metadata Collection

Metadata collection includes telecommunications, postal and Internet data. The vast majority (97.7%) of metadata processed in 2016–2020 were telecommunications data. Internet data accounted for 1.6%.[16] Metadata may be processed for the purposes of either judicial proceedings or operational surveillance.

In the case of judicial proceedings, judges or prosecutors are authorized to get access to metadata and process it. No ex-post oversight is required.

The surveillance procedure significantly differs from those regarding judicial proceedings and wiretapping. The requesting security services are authorized to process metadata, to which the subsidiarity clause (least-intrusive means) does not apply. Communications operators and providers are obliged to give access to retained metadata. No prior judicial consent is required. Only ex post judicial review is allowed. Interestingly, both defense intelligence organizations are not mentioned at all in those regulations.

Foreign Targets

When it comes to foreign targets in the territory of Poland, the Anti-terrorist Act of 2016 legalized wiretapping of foreigners (including citizens of the EU) without the consent of the court. The Head of ABW may order, notifying forthwith the Prosecutor General and the Minister-Coordinator of Special Services (if appointed), electronic surveillance for a period not longer than three months of a person who is not a citizen of Poland and is suspected of involvement in terrorist activities. The Prosecutor General may halt surveillance. After the completion of the operational activities, the Head of ABW provides the Prosecutor General with the results and – if requested by the prosecutor – details about the operation.

Polish special services develop their operational and technical capabilities with limited public scrutiny. The law does not stipulate which measures and tools are allowed, leaving open the possibility that the latest and most advanced technical measures are applied. Little is available from open sources; only occasional media leaks and opinions of former top intelligence officials shed some light on this.

Domestic surveillance relies mostly on software purchased from abroad, though some in-house software is also used. In 2017 Poland became one of the customers of the Israeli cybersecurity company NSO Group, which offered its Pegasus spyware for government intelligence and law-enforcement services.

The manner of purchasing the software and the scope of its use have raised serious legal concerns and accusations that the authorities used Pegasus against political opposition. Pegasus was purchased by CBA from the Justice Fund, which was created to compensate victims of crimes. This was in a sharp breach of the provisions of the Act on CBA, which requires that the Agency be financed exclusively from the state budget in order to ensure accountability and parliamentary control.

Moreover, the surveillance software was used not only as a tool to fight organized crime or terrorism but also to wiretap political opponents and civil society activists.[18] According to the opposition, prior to the parliamentary elections in 2019, communications of the electoral committee of the main opposition party, Civic Platform, were obtained by special services from phones bugged with the Pegasus spyware. Allegedly, the messages were then manipulated and used in a massive disinformation campaign.[19]

There are no legal restrictions on domestic collection targeting people located abroad. The law stipulates that the Foreign Intelligence Agency "carries out electronic surveillance" outside Poland's territory, but it can authorize the Internal Security Agency to undertake covert surveillance in Poland (including foreign targets).[20]

Retention

Retention periods are set by the telecommunications law.[21] Communications metadata can be retained for 12 months. Information gathered during a wiretap (targeted operational wiretapping) can be retained for the duration of criminal investigation and prosecution and should be immediately deleted if it does not constitute evidence of the value to investigation and prosecution. Polish law does not make a distinction between a Polish citizen and a foreigner regarding minimization of data.

V. OVERSIGHT AND TRANSPARENCY

Oversight in democratic politics is ideally exercised by supervisory bodies in the legislative and judiciary branches, as well as those representing civil society (advocacy groups, expert bodies). However, in Poland, oversight mechanisms are fragmented, often illusory, and do not allow for effective, impartial, and policy-independent verification of the activities of the special services and other relevant security bodies. This results from politicization of intelligence activities, partisan attitude of the ruling coalition toward the special services, and controversy over the independence of the judiciary,

Oversight Entities

Legislative oversight is exercised by the parliamentary Special Services Committee. It is composed of up to seven members of the Sejm (lower house) representing major parties. Currently the majority (four members) belong to the ruling PiS party, which significantly limits the possibility of independent supervision of the government's decisions. The Committee formulates opinions on draft laws and other normative acts (including government regulations and decisions) concerning special services; on the scope and results of activities of the special services, including alleged irregularities and infringements during their activities; on budgetary matters and financial spendings; and on proposals for appointment and dismissal of the heads of special services and their deputies. It also evaluates the protection of classified information and examines complaints about the activities of the special services. However, the Commission lacks powers needed to exert real control, such as the power to collect testimonies from the heads of special services and their officers.

Members of the Parliament can set up a special committee or an investigative committee in both houses, usually concerning matters of utmost importance for the national interest and rule of law. The Pegasus wiretapping scandal, revealed in late 2021, caused a stir among the opposition, which demanded the creation of an investigative committee. This initiative was blocked in the Sejm (lower house), due to the majority held by the ruling United Right coalition. The opposition managed to establish a special committee in the Senate (upper house).[22] The committee has sought to investigate reported cases of illegal use of Pegasus software for unlawful surveillance of selected opposition politicians and lawyers, which might have had an impact on the 2020 presidential election process. The special committee, however, was devoid of investigative powers and has been systematically boycotted by PiS. Evidence collected during the hearings from the targeted opposition figures, as well as independent experts and representatives of advocacy groups, have exerted pressure on the authorities but did not result in practical outcomes.

> ***In Poland, oversight mechanisms are fragmented, often illusory, and do not allow for effective, impartial, and policy-independent verification of the activities of the special services and relevant security bodies.***

Judicial oversight is sporadic. In the mid-2000s, journalists challenged intrusive collection powers granted by the Telecommunications Act of 2004. Those provisions allowed law enforcement agencies to retain telecommunications data without any external control and in a covert manner.[23] Following a long process involving seven joint motions, the Constitutional Tribunal held in 2014 that the challenged provisions were unconstitutional because they did not include independent supervision over the security services' access to telecommunications data.[24] The Tribunal underlined the necessity of independent supervision over the law enforcement and intelligence services and drew attention to the lack of both *ex ante* and *ex post* judicial oversight.[25] However, it did not require lawmakers to provide for judicial control over data acquisition.[26]

As part of judicial oversight, district courts (specifically, their criminal divisions) and prosecutors exercise control over applications to conduct operational surveillance submitted by the security services. Regard-

ing ex-ante control, the courts and prosecutor's offices verify that an application complies with the criminal procedure and approve it if it is devoid of formal shortcomings. As a result, the percentage of refusals by the courts is extremely low: 0.5 percent in the years 2010-2020.[27] Applications are more often rejected by the prosecutors (up to 3%) than by the courts (up to 1%). Requests for wiretapping filed by the special services usually go unchallenged. In 2021 this applied to four security services: CBA, SKW, KAS and the Border Guard.

Ex-post oversight is quite limited. It was established only in 2016 and concerns only communications data, not wiretapping. It is conducted by the district courts (both common and military). However, the courts are not allowed to review all materials concerning ongoing proceedings and they depend on biannual statistical reports delivered by the security services. Judges, usually coping with enormous workloads, do not have enough time to examine available files. The relevant laws do not specify how this type of oversight should be exercised. Moreover, there are no legal sanctions when the court detects irregularities.

Another form of oversight is provided by independent supervisory bodies in the area of protection of human rights and safeguarding of civil liberties (the Ombudsman) and the audit of the public administration and effectiveness in public service (the Supreme Audit Office).

The Ombudsman (Commissioner for Human Rights) conducts ex post oversight of individual activities of the security services to ensure civil rights compliance. The Ombudsman has been regularly taking steps to improve oversight and supervision in terms of compliance with the Polish Constitution, relevant domestic legal measures, and international agreements. The Commissioner voiced his deep concern after the legislative changes in 2016 (especially because of the adoption of the surveillance laws) expressing regret about the shortfall of appropriate legal safeguards against the risk of violating fundamental rights. The Commissioner has been constantly involved in efforts aiming to improve legal safeguards for citizens exposed to surveillance by security services. He endorsed a report titled "How to saddle Pegasus,"[28] which proposed the establishment of an independent oversight body supervising security services.

The Supreme Audit Office (NIK) is formally subordinate to the Sejm (the chairman of the Office is appointed by the lower chamber of the Parliament with the consent of the upper house) but it retains independence regarding the audit process. NIK oversees the activities of the special services and other law-enforcement and security agencies to ensure the efficacy and integrity of their activities, effective management of public resources, and compliance with professional standards.

Typically, NIK has expressed critical opinions about the operational activities of the special services. In 2012–2013, NIK conducted an audit on the obtaining and processing of telecommunication data. The audit also addressed the issue of electronic surveillance. The findings revealed insufficient protection of human rights and individual freedoms against interference by the state's security and intelligence services. More recently, in 2022, the Supreme Audit Office carried out an ad hoc inspection of the functioning of the services conducting operational and surveillance activities in the territory of Poland. In an official statement concerning preliminary results of the audit, NIK's President lamented that under the existing political regime, any comprehensive and objective assessment of the interference of the special services in the sphere of civil rights and freedoms is significantly hampered.

Transparency

Poland's secret services have long struggled with representatives of civil society over the trade-offs between secrecy and transparency. This reflects both formal

rules providing for secrecy and a natural inclination to maintain closed working environments. Despite the development of legislative instruments and measures aiming to strengthen and consolidate legal and political transparency, pervasive secrecy persists, undermining democratic legitimacy and civil rights.[29]

Poland made significant progress during the post-Communist transition, adopting a legal framework for freedom of information and improving accountability of secret services. However, in the past few years a noticeable decline in transparency and availability of information on the secret services has occurred. This is partly due to the opaque style of politics practiced by the ruling United Right coalition, especially in the areas of public communication and government information policy. More importantly, it results from politicization and instability within the secret services after 2015. This spurs a desire to hide as much as possible about the organization and internal governance, mutual relations, resource management, and operational activities.

Poland made significant progress during the post-Communist transition, adopting a legal framework for freedom of information and improving accountability of secret services. However, in the past few years a noticeable decline in transparency and availability of information on the secret services has occurred.

Relevant laws, decrees, and legal decisions are typically available to the public; information about their operational implementation is generally not. Acts containing regulations and other legal norms concerning surveillance are promulgated in official journals: The Journal of Laws (Dziennik Ustaw) and the Official Journal (Monitor Polski) are publicly available. Likewise, judgments of the Constitutional Tribunal and the Supreme Court are public. Some secondary normative acts (regulations, decrees, decisions etc.) are published in internal bulletins accessible to the personnel of the secret services and law-enforcement bodies. Judgments, judicial opinions, or legal interpretations are most commonly accessible on the official websites of the issuing institutions.

The scale of electronic surveillance is much more difficult to assess. This is mostly due to legal restraints, political decisions, and the culture of opacity in the secret services. In 2011, a mandatory obligation was placed on the Prosecutor General to present to the Parliament a non-classified annual report on operational surveillance. The report includes the number of persons for whom a surveillance decision was issued, the number of refusals, and the number of decisions of the prosecutor rejecting surveillance requests. As an illustration, the data for 2021 indicated that the overall number of operational surveillance decisions amounted to 7,000, which was the highest number since 2011 (the first year of mandatory publication of the report). This was an increase of 8% in comparison to 2020 and almost 20% as compared to 2016. The number of refusals (by judges and the prosecutor) was only 149.[30]

Since 2011, the Minister for the Interior has been required to submit to the Parliament a semi-annual report on operational surveillance executed by the Police, the Office for Internal Oversight of the Ministry of the Interior and Administration, and the State Protection Service. Interestingly, the two latter entities have not done this so far.

Since 2016, as a result of the Surveillance Law, the Minister for Justice twice a year presents a report to the Parliament on the number of processed telecommunications, Internet and postal data, including the general institutional breakdown. In 2021, the law-enforcement agencies and secret services accessed telecommunication data as many as 1.8 million times. Seventy-three percent of these requests were made by the Police.[31]

Transparency is more limited for the special services, whose missions are shrouded in greater secrecy. Only the Anti-Corruption Bureau (CBA) continues to publish an annual report on the results of its activities.[32] The Internal Security Agency (ABW) ceased to publish annual reports in 2016 and abolished the office of its spokesperson. Since then, ABW has only occasionally released general information about its activities, usually highlighting achievements and operational successes concerning terrorist threats, economic crime, and espionage.

Reports of the Supreme Audit Office are published in the Public Information Bulletin and on the Office's website. The president of NIK and auditors take part in conferences, seminars, meetings, and media events at which they present information on audit results. However, the reports on the secret services are confidential

and only official press releases containing general opinions are made available.

The Polish Act on Access to Public Information of 2001 (similar to FOIA rules in the United States) endows the Polish citizen with the right to obtain information on the activities of public authorities and persons performing public functions. It includes processed information (based on first-hand data) to the extent that it is particularly important for the public interest. It also allows for the inspection of official documents. This right has been exercised many times by individuals and legal persons (usually civil liberties advocacy groups and watchdog organizations).

One such organization, the Panoptykon Foundation, has been particularly active in the field of transparency and accountability of the security services. However, their requests for the information on the activities of the special services, including statistical data on electronic surveillance, were persistently turned down, usually based on the need for secrecy. Legal proceedings launched by that Foundation (and some others) were ineffective. In 2018, the Supreme Administrative Court dismissed complaints against ABW, CBA, and SKW concerning the refusal to provide statistical information on electronic surveillance.

Despite these efforts, public opinion is largely uninterested in and unconscious of risks to their privacy and digital rights provoked by massive electronic surveillance. For instance, a public opinion poll on surveillance on the Internet, conducted in April 2016 after the enactment of the Surveillance Law, revealed that only 19% of the respondents had some knowledge about this issue while 27% had heard something but were not sure about the substance of the legal changes. The poll further showed that respondents favored granting the security services access to online information if it helps prevent and solve crime (46% to 30%). Half of the respondents believed that the powers of the Police and other security services to obtain information on the activity of Internet users are sufficient, while 19% claimed they are too small and should be increased.[33]

Another survey on surveillance was conducted in February 2022, this time provoked by the Pegasus spyware scandal. It showed a heightened awareness of the surveillance issue: 75% of the respondents "heard about the surveillance of public figures in Poland using the Pegasus system." However, an equally significant majority (71%) thought it was "a manifestation of political struggle." Consequently, the prevailing opinion was that the Polish secret services should be able to use this type of software in their operational work (45% to 36%, which is very similar to the general attitude to surveillance exhibited in the 2016 survey). Only 44% of the interviewees agreed that "wiretapping or Internet activity control in Poland are not sufficiently controlled."[34]

Redress

Polish law does not provide a redress mechanism. An individual under targeted surveillance may not file a complaint. The target is not informed of the surveillance, even *ex post*. This breach in civil rights protection, and the resulting inconsistency with the Polish Constitution, was raised several times by the Ombudsman in constitutional complaints about the relevant provisions of the Act on Police. Recently, in June 2022, the Constitutional Tribunal rejected the complaint on procedural grounds.[35]

VI. REFORMS

The problem of reform and transformation of intelligence agencies and other security services has been present since the post-Communist transition. Despite political, institutional, and organizational changes, reform has not adequately addressed the question of electronic surveillance. Complaints over opacity and unlawfulness of some forms of electronic surveillance were voiced in the early 2000s by journalists, social activists, and watchdogs. They resulted in motions filed to the Constitutional Tribunal which signaled deficiencies in the existing law. The Tribunal agreed with the principal complaints and by the judgment in Case K 23/11[36] demanded that "an independent oversight body be established, that individuals who had been subject to intrusive surveillance methods be notified, and that procedural safeguards for secret surveillance be tightened."[37]

In response to the Tribunal's opinion, the government drafted in 2013 a bill establishing the Special Services Oversight Committee and modifying the government's supervision over the special services.

In response, the ruling liberal coalition was forced to accelerate work on the legal reform, but its efforts were hindered by criticism from officers representing the special services, as well as experts highlighting risks associated with inadequate consideration of key points and hasty drafting of new bills.

Therefore, the task of implementation of the Constitutional Tribunal's judgment was delegated to the Law and Justice (PiS) party, which won the 2015 parliamentary and presidential elections. The Surveillance Law of 2016, a brainchild of the triumphant national-conservative coalition of the United Right, allowed the security services a practically unlimited processing of the communications data, offering illusory judicial oversight and denying citizens any real influence on electronic surveillance. Second, the Anti-Terrorism Act stripped from foreigners any constitutional safeguards in terms of operational surveillance.[38] Finally, the "fruit of the poisonous tree" limitations implemented in the Code of Criminal Procedure opened the door to various types of abuse by security services and prosecutors.

The consolidation of PiS's hold over the security services, guaranteed by the stable parliamentary majority, and facilitated by political opposition weakness, halted the quest for reforms. An interesting and broadly debated proposal was put forward in September 2019 by a group of experts representing civil liberties organizations, former officials of the Ombudsman office, and representative of the former Civic Platform government. Alluding to the Pegasus spyware scandal, the report titled "How to Saddle Pegasus" advocated for the establishment of an independent oversight body supervising the special services and other entities authorized to conduct surveillance activities. Although the report stirred a debate among experts and some politicians, it did not bring about any modification of the United Right's policy. Correspondingly, the liberal opposition showed little interest in those recommendations.

In October 2021, a Parliamentary Group for the Reform of Special Services was set up by MPs representing opposition to the United Right, although without the participation of the Civic Platform, the main opposition party, which had its own conception of a reform. The Group has discussed oversight and control over special services as part of a comprehensive reform of the Polish intelligence community advocated by the members of the Group and invited experts.

VII. CONCLUSIONS

Electronic surveillance is an important part of the activities of the Polish security services. It is focused on domestic activities of law-enforcement services, chiefly the Police, and in some respects is exercised without conformity to the Polish Constitution and legal standards enshrined in European law. Procedural safeguards and substantive requirements in the Surveillance Law for implementing operational surveillance are insufficient to prevent its excessive use and unjustified interference with the privacy of individuals.[39]

The current geostrategic environment, in particular Russia's invasion of Ukraine and active interference in public affairs in the West, generates new challenges and tasks for Poland. As a frontline state, Poland must improve its intelligence capabilities in order to cope effectively with risks and threats to its national security.[40] Changes introduced under the United Right rule did not contribute to a higher effectiveness and professionalism of the security services. Rather, they consolidated an opaque surveillance apparatus which reflects the characteristic traits of the ruling coalition: politicization, insufficient human resources, double standards in the observance of democratic principles, and weakened cooperation with external partners, especially in the EU. Without legal reforms and accountable leadership, the system will likely become more obsolete and dysfunctional with regard to Poland's national interests.

ENDNOTES

1. See Wojciech Sadurski, *Poland's Constitutional Breakdown*, Oxford: Oxford University Press, 2019; Marcin Matczak, The Clash of Powers in Poland's Rule of Law Crisis: Tools of Attack and Self-Defense, *Hague Journal on the Rule of Law*, 2020, 12(3), https://doi.org/10.1007/s40803-020-00144-0; Wojciech Przybylski, Explaining Eastern Europe: Can Poland's Backsliding Be Stopped?, *Journal of Democracy*, 2018, 29(3); Michael Bernhard, Democratic Backsliding in Poland and Hungary, *Slavic Review*, 2021, 80(3), https://www.cambridge.org/core/journals/slavic-review/article/democratic-backsliding-in-poland-and-hungary/8B1C30919DC33C0BC2A66A26BFEE9553.
2. *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Mapping Member States' legal frameworks,* Fundamental Rights Agency, Luxembourg: Publications Office of the European Union (2015) at 14, https://op.europa.eu/en/publication-detail/-/publication/73b199a7-8f51-11e5-983e-01aa75ed71a1/language-en.
3. Mateusz Kolaszyński, *Secret Surveillance in Poland after Snowden. Between Secrecy and Transparency*, in TRUST AND TRANSPARENCY IN AN AGE OF SURVEILLANCE (2022) at 128.
4. Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency. The original wording in Polish: "prowadzenie wywiadu elektronicznego" may equally be translated as "carrying out signals intelligence." *See https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/99891/119498/F1157569895/POL99891%20Pol.pdf.*
5. Act of 9 June 2006 on the Military Counter-Intelligence Service and the Military Intelligence Service, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20061040709/U/D20060709Lj.pdf (original Polish), and https://www.osce.org/files/f/documents/2/7/243261.pdf (English translation).
6. In the original Polish: *kontrola operacyjna*, which means both operational control and surveillance. This form of covert surveillance was applied to over 60,000 individuals in the years 2010-2020. See Arkadiusz Nyzio, Mity o skrzydlatym koniu. Wokół debaty o Pegasusie i kontroli operacyjnej [Myths About a Winged Horse. Of the Pegasus Debate and Operational Control] Komentarz KBN, no. 4 (93) / 2022, 21 February 2022, at 1.
7. The Constitution of the Republic of Poland of 2nd April, 1997 as published in *Dziennik Ustaw* No. 78, item 483, https://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm.
8. See Agnieszka Kastelik-Smaza, The Application of the Charter of Fundamental Rights of the EU In Poland, *Acta Universitatis Carolinae – Iuridica*, 2018, no. 4, at 103-104, https://karolinum.cz/data/clanek/6410/Iurid_64_4_0101.pdf.
9. Filip Radoniewicz, The Issue of Surveillance Carried Out by Technical Means Within the Jurisprudence of the European Court of Human Rights and the Constitutional Tribunal, *Przegląd Prawa Konstytucyjnego*, 2021, no. 6, at 299-300, https://www.ilo.org/dyn/natlex/natlex4.detail?p_isn=99891.
10. Jan Rydzak, *Now Poland's Government Is Coming After the Interne*t, FOREIGN POLICY (Jun. 10, 2016) https://foreignpolicy.com/2016/06/10/now-polands-government-is-coming-after-the-internet/ (accessed on Jul. 17, 2022).
11. By this I mean telecommunications, Internet, and postal data.
12. Marcin Rojszczak, *Surveillance, Legal Restraints and Dismantling Democracy*, at 5.
13. Barbara Grabowska-Moroz, *The Polish Surveillance Regime Before the ECHR*, ABOUT:INTEL, (Apr. 27, 2020) https://aboutintel.eu/echr-poland-surveillance/; Marcin Rojszczak, *Surveillance, Legal Restraints and Dismantling Democracy*, at 6.
14. Mateusz Kolaszyński, *Secret surveillance in Poland after Snowden* at 130-31.
15. Arkadiusz Nyzio, *The Internal Security of Poland in 2018 – Key Changes and Events*, in SECURITY OUTLOOK 2018, Kraków: Księgarnia Akademicka (2019) at 117, https://www.doi.org/10.12797/9788381380843.05.
16. Arkadiusz Nyzio, *Raport inwigilacyjny (edycja 2021) [Surveillance in Poland A.D. 2021*], KBN ANALYSIS No. 18 (113) / 2022, https://www.academia.edu/90834863/Raport_inwigilacyjny_edycja_2021_(in Polish).
17. Based on: "Jawna roczna informacja Prokuratora Generalnego o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli i utrwalania rozmów lub wniosek o zarządzenie kontroli operacyjnej" (Public annual information of the Prosecutor General on the total number of persons against whom a request to order control and recording of conversations or a request to order operational surveillance have been submitted), https://www.senat.gov.pl/prace/druki/record,12239.html.
18. Marcin Rojszczak, *Electronic Surveillance in a Time of Democratic Crisis: Evidence from Poland*, VERFASSUNG BLOG (April 12, 2022), https://verfassungsblog.de/os6-dem-crisis-pl (accessed March 26, 2022).
19. European Parliament, *Mission Report Following the Delegation to Warsaw, Poland 19-21 September 2022, Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware*, https://www.europarl.europa.eu/doceo/document/PEGA-CR-736647_EN.pdf.
20. Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, Art. 6, https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/99891/119498/F1157569895/POL99891%20Pol.pdf.
21. Act of 16 July 2004 on the Telecomunications Law (https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20041711800/U/

D20041800Lj.pdf) (original Polish) and http://prawo.vagla.pl/files/polish_telecommunication_act.pdf (English translation).
22. *Senate Approves Launching a Special Committee to Examine Use of Pegasus Surveillance Tool,* TVN24 NEWS IN ENGLISH (Jan. 12, 2022, https://tvn24.pl/tvn24-news-in-english/polands-senate-lunches-special-committee-to-examine-use-of-pegasus-software-5557023 (accessed Oct. 18, 2022).
23. See Katarzyna Szymielewicz, *Blanket Data Retention in Poland: The Issue and the Fight,* PANOPTYKON FOUNDATION, https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/PanoptykonFoundation.pdf.
24. Judgment of 30 July 2014, Ref. No. K 23/11, https://trybunal.gov.pl/en/hearings/judgments/art/7004-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/; see also Agnieszka Grzelak, *Data Retention Saga Continues: Decision of the Polish Constitutional Tribunal of 30 July 2014 in Case K 23/11*, EUROPEAN PUBLIC LAW, 2016, 22(3), https://doi. org/10.54648/euro2016030; Jan Podkowik and Marek Zubik, *Data Retention in Poland*, in: Marek Zubik, Jan Podkowik, Robert Rybski (eds.), *European Constitutional Courts towards Data Retention Laws*, Cham: Springer (2021) at 163-169.
25. Marcin Rojszczak, Surveillance, Legal Restraints and Dismantling Democracy, at 4-5.
26. Jan Podkowik, *Privacy in the Digital Era – Polish Electronic Surveillance Law Declared Partially Unconstitutional,* EUROPEAN CONSTITUTIONAL LAW REVIEW (2015) at 11(3), https://doi.org/10.1017/S1574019615000322.
27. *See supra* note 6, Arkadiusz Nyzio, Mity o skrzydlatym koniu, at 6.
28. *How to Saddle Pegasus: Observance of Civil Rights in the Activities of Security Services: Objectives of the Reform* (Sept. 2019), https://bip.brpo.gov.pl/sites/default/files/HOW%20TO%20SADDLE%20PEGASUS%20(OSIOD%C5%81A%C4%86%20PEGAZA).pdf, (accessed Mar. 26, 2023).
29. Dorota Mokrosinska, *Introduction: Transparency and secrecy in European Democracies*, in TRANSPARENCY AND SECRECY IN EUROPEAN DEMOCRACIES: CONTESTED TRADE-OFFS (2021).
30. *See generally*, Arkadiusz Nyzio, Raport inwigilacyjny.
31. Informacja Ministra Sprawiedliwości na temat przetwarzania danych telekomunikacyjnych, pocztowych i internetowych oraz wyników przeprowadzonych kontroli w 2021 roku (Information of the Minister for Justice on the processing of telecommunications, postal and Internet data and the results of controls carried out in 2021), https://www.senat.gov.pl/gfx/senat/userfiles/_public/k10/dokumenty/druki/700/769.pdf.
32. See for instance: *Report on the results of the activities of the Central Anti-Corruption Bureau in 2021* (in Polish), http://cba.gov.pl/ftp/dokumenty_pdf/Informacja_2021.pdf. Earlier reports are available at the CBA's website: https://www.cba.gov.pl/pl/o-nas/informacja-o-wynikach.
33. *Surveillance on the Internet*, CBOS, no. 5/2016, at 2-3, https://www.cbos.pl/PL/publikacje/public_opinion/2016/05_2016.pdf.
34. *Public Opinion on Surveillance*, CBOS, no. 031/2022, https://www.cbos.pl/EN/publications/reports/2022/031_22.pdf.
35. *See,* Case 60/21, https://trybunal.gov.pl/postepowanie-i-orzeczenia/postanowienia/art/11990-brak-mozliwosci-wniesienia-zazalenia-na-postanowienie-sadu-w-przedmiocie-stosowania-kontroli-operacyjnej-przez-osobe-wobec-ktorej-kontrola-ta-byla-stosowana
36. Judgment of 30 July 2014, Ref. No. K 23/11, https://trybunal.gov.pl/en/hearings/judgments/art/8821-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani
37. *Supra note 13*, Barbara Grabowska-Moroz, *The Polish Surveillance Regime*
38. Operational surveillance is ordered by the head of the Internal Security Agency with no requirement of prior judicial authorization. The Prosecutor General (being a member of the government) may put an end to the surveillance. A terrorist suspect is subject to the 14-day detention without charge. No procedural safeguards are provided to ensure access to an effective remedy against unlawful surveillance. See Giulia Berlusconi and Claire Hamilton, Counter-Terrorism in Poland, in Claire Hamilton (ed.), *Contagion, Counter-Terrorism and Criminology*, Cham: Palgrave Macmillan(2019).
39. *Supra note 13,* Barbara Grabowska-Moroz, The Polish Surveillance Regime.
40. See Artur Gruszczak, The Polish Intelligence Services and Security Dilemmas of a Frontline State, *Romanian Intelligence Studies Review*, 2017, no. 17-18.