HOW TO SADDLE PEGASUS:
Observance of civil rights
in the activities of security services: objectives of the reform

Document authors:
Adam Bodnar
Tomasz Borkowski
Jacek Cichocki
Wojciech Klicki
Piotr Kładoczny
Adam Rapacki
Zuzanna Rudzińska-Bluszcz

September 2019

TABLE OF CONTENTS

I. Introduction 3

II. The necessity to respect civil rights in the activities of security and police services 6

III. Independent oversight body for services authorized to use surveillance 13

IV. Necessary changes regarding individuals' right to information and data protection 26

V. Other systemic and legislative changes 31

VI. Other practical changes 37

VII. Biographical notes on the authors 41

I. INTRODUCTION

1. Authors of this document

The present document has been drawn up as a result of **cooperation of a group of experts** who have been observing, from different perspectives, the work of security services in Poland and the related risks that are emerging to the protection of civil rights and freedoms.

The authors of this document **represent various professional groups and communities**. Guided by the sense of responsibility as well as the concern about the quality of functioning of the Polish state and the degree of observance of civil rights and freedoms, we have attempted to take account of different points of view on specific issues. We have also taken the greatest care to balance aspects that may be contradictory to each other, in the spirit of the principle of proportionality that arises from the Constitution.

2. The role of the Commissioner for Human Rights

When preparing this document the expert group met **over for months at the invitation of the Commissioner for Human Rights (CHR)**. For years, the CHR has been taking steps with the aim to ensure better supervision over the country's security services as well as a regulatory environment in which the principles arising from the Constitution and the ratified international agreements would be respected. The CHR also follows the activities of international bodies for which those issues are of particular importance, including, in particular, the Venice Commission[1], the Council of Europe Commissioner for Human Rights[2], the EU Fundamental Rights Agency[3] and the Geneva Centre for Security Sector Governance (DCAF)[4]. The CHR has also taken part in various proceedings held before the Constitutional

[1] *Report on the Democratic Oversight of the Security Services,* 1-2 June 2007, updated on 20-21 March 2015, CDL-AD (2015)006, available at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e

[2] *Democratic and effective oversight of national security services,* Issue Paper by the Commissioner for Human Rights of the CoE, May 2015, available at: https://rm.coe.int/deiTiocratic-and-effective-oversight-of-national-security-services-issue/16806daadb

[3] *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU: Mapping Member States' legalframeworks,* 2015; report available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

[4] Nazli Yildirim Schierkolk, International standards and good practices in the governance and oversight of security services, Tbilisi 2018; report available at: https://www.dcaf.ch/international-standards-and-good-practices-governance-and-oversight-security-services

Tribunal with regard to those issues.

3. Key objectives of this document

This document:
➢ **postulates key political and legislative changes** that could lead to respecting the constitutional principles in the field of activities of security services; ➢ is based on the assumption that **oversight of security services** is an element of an efficient state although it is not aimed at limiting their effectiveness; ➢ **aims to find a balance between protecting civil rights and freedoms and counteracting threats to national security and public order**. Such threats can be related to terrorism, operations of foreign security services, or criminal activities.

Civil rights protection mechanisms aim primarily at **protecting those who may be aggrieved by excessive activities of security and police services or the abuse of their specific powers**. At the same time, such mechanisms **counteract pathologies and malpractices within the services themselves**, including their involvement in political or business machinations or the pursuance of private interests by individual officers.

4. Content of this document

The document contains a postulate of comprehensive changes including, in particular, two key elements:
1) **developing an independent body for oversight of** security services; 2) **granting individuals the right to information on them being of interest to agencies authorized to collect their data**, and on their right of access to such data processed by those agencies.

The document contains numerous postulates of specific changes relating to:
1) certain issues regulated in the so-called *Act on anti-terrorist activities*; 2) the system of "fruit of the poisonous tree"; 3) practical changes that could improve the process of oversight of the operations of security services, exercised by judges and prosecutors.

5. Addressees of this document

This document is addressed to **all political forces in Poland**. We hope that it will become a source of reflection for all major political parties as well as for **academic, journalistic, non-governmental and opinion-forming circles**.

II. THE NECESSITY TO RESPECT CIVIL RIGHTS IN THE ACTIVITIES OF SECURITY AND POLICE SERVICES

1. Constitutional boundaries of the services' activities

According to the Constitution, one of the responsibilities of the state is to **ensure the security of its citizens** (Article 5 of the Constitution). This responsibility is fulfilled by all agencies of the state. However, a particular role in this area is played by **security services** that have special powers to significantly interfere with the right to privacy. Similarly, in certain situations, police services may also conduct surveillance operations. Officers of the services in question may use special powers and operating methods which, as a rule, remain beyond public knowledge.

The Constitution provides for guarantees regarding the protection of the **right to privacy, inviolability of one's premises, confidentiality of correspondence and information autonomy**. In democratic countries it is assumed that task implementation by security services should be carried out with respect for the constitutional values. It should remain within **the limits of legalism**, respect the principle of **the tripartite separation of powers**, and observe the **constitutional rights and freedoms of individuals**.

To this end, various mechanisms are developed to ensure that activities of the services do not exceed the constitutional bounds. They include both regulatory mechanisms that set out specific tasks and competences of the services, as well as their oversight mechanisms.

2. Security services' oversight mechanisms

In Poland, the activities of security services are subject to specific regulations. This is a result of the evolution of the security services' functions, the extension of their powers, as well as the requirements that arise from the Constitution and the jurisprudence of the Constitutional Tribunal.

Pursuant to the current systemic solutions, **oversight of the services is exercised by the following authorities of the state**:

- **The Sejm [lower chamber of the Parliament] and the Sejm Committee on Security Services** – as part of its supervision over the activities of government administration bodies, the Sejm exercises oversight of the security services. Notably, however, the Sejm Committee on Security Services is a body composed of politicians representing individual parliamentary groups. In Poland, the ruling coalition has a significant majority of seats on the Committee, which significantly limits the possibilities of independent oversight;
- **Supreme Audit Office** – exercises oversight of the services within the scope of responsibilities of the Office;
- **Commissioner for Human Rights (CHR)** – exercises control over individual activities of the services, based on lodged complaints regarding the respect of civil rights;
- **State government bodies** (Prime Minister, Minister - Coordinator of Security Services, Governmental Council on Security Services) coordinate and control daily work of security services;
- **courts and prosecutors** - supervise the conduct of secret surveillance and other surveillance operations by security services;
- **The Internal Oversight Bureau of the Ministry of the Interior and Administration** supervises the secret surveillance operations carried out by the Police, the Border Guard and the State Protection Service.

Unlike other democratic states **Poland, in fact, has never completed the process of building modern security services**. The missing element is an independent body responsible for oversight of the services. Currently, the **oversight is fragmentary** and does not enable effective, impartial and non-political verification of the activities of security services.

3. The necessity to establish a body for oversight of security services

The above brief overview explains that **Poland has never established a body** that would:

- **have the sole task of oversight** of security services;
- have the power to examine **complaints** as a body specialized in this area;
- be endowed with the **attributes of independence and impartiality**.

It is noteworthy that such bodies exist in many European countries (e.g. the G-10 Commission

in Germany or the EOS Committee in Norway).

The establishment of an independent body for oversight of security services **has been sought for many years by Polish non-governmental organizations** (in particular, the Helsinki Foundation for Human Rights, the Panoptykon Foundation and Amnesty International), lawyers' associations (in particular the Polish National Bar Council) and **experts**. It was also among the postulates of the **Supreme Audit Office**[5]. Steps towards its establishment were taken by the **Council of Ministers in 2013**. At that time, a bill was drawn up that provided for the establishment of the Special Services Oversight Committee and a reform of the governmental system of oversight of special services. However, due to criticism on the side of various circles (in particular, representatives of certain security services) the bill has never been adopted[6].

4. Recent legislative changes

In the last years, **the situation of citizens as potential victims of abuse of powers by security services has significantly deteriorated**.

The legislative changes adopted in 2016 increased **the deficit in the protection of civil rights**:

- the 2016 amendment to the ***Police Act*** granted security services practically unlimited powers of surveillance over the so-called Internet data;
- the established **mechanism of oversight of metadata use by special services** is rather illusory instead of giving the citizens the actual sense of security (statistical reports subject to verification by courts);
- in 2016, the ***Act on anti-terrorist activities*** was also passed, which granted security services a number of additional powers, and in fact excluded foreign citizens from the scope of the constitutional protection with regard to possible surveillance;
- **the amendment to the Code of Criminal Procedure** introduced the admissibility in criminal proceedings of the so-called "fruit of the poisonous tree" i.e. evidence

[5] Information on the Supreme Audit Office report of 26 August 2014 on oversight of security services is available at: https://www.nik.gov.pl/aktualnosci/nadzor-nad-sluzbami-specjalnymi.html

[6] The 2013 bill on Special Services Oversight Committee, as well as documentation on related public consultations and inter-ministerial arrangements are available at: https://archiwumbip.mswia.gov.pl/bip/projekty-aktow-prawnyc/2013/22523,Projekt-ustawy-z-dnia-2013-r-o-Komisji-Kontroli-Sluzb-Specjalnych.html

obtained in breach of law (Article 168(a) of the Code of Criminal Procedure). This procedural measure opens the door to various types of abuse on the side of police officers, prosecutors and security service officers.

The Commissioner for Human Rights lodged applications with the Constitutional Tribunal with regard to all the three Acts. However, they were later withdrawn by the Commissioner as the judicial panel included persons not authorized to adjudicate, and because of the panel composition's manipulation by the Tribunal[7]. The CHR did not want to lead to a situation in which the Constitutional Tribunal's judgments would legitimize the legal status which raises a number of doubts as to its compliance with the Constitution. **The CHR also counts on direct application of the Constitution by courts**. An example is the judgment of 28 June 2018, issued by the Supreme Court sitting in the composition of seven judges, which restricted the possibilities of using secret surveillance[8]. According to the Supreme Court, the statement used in Article 168(b) of the Code of Criminal Procedure: *"another offense prosecuted ex officio or a tax offense other than the offences covered by the permit to use secret surveillance"* applies solely to offences with regard to which a court may consent to the use of secret surveillance, including those referred to in Article 19(1) of the *Police Act*.

It is also worth adding that new **legislative acts have been adopted that further restrict the protection of the right to privacy. The *Act on population registry*** provides security services with online access to data contained in civil status registry documents. **Poland has also failed to properly implement the so-called Police Directive no. 2016/680** which requires the observance of specific standards in the collection and processing of personal data by the police and other services (see Chapter IV below). Despite numerous postulates, video surveillance regulations are still scattered.

5. Development of new technologies

In the context of the activities of security services it should be emphasized that the above-mentioned legislative deficits are accompanied by **the simultaneous development of new**

[7] CHR's application to the Constitutional Tribunal of 18 February 2016 regarding the amendment to the Police *Act* (withdrawn on 14 March 2018); the CHR's application to the Constitutional Tribunal of 11 July 2016 regarding the *Act on anti-terrorist activities* (withdrawn on 2 May 2018); CHR's application to the Constitutional Tribunal of 6 May 2016 regarding the "fruit of the poisonous tree" (withdrawn on 10 April 2018).

[8] Case ref. no. I KZP 4/18.

technologies. Thus, the lack of control over the operations of special services is likely to have led to their ability to purchase new technologies, thereby creating possibilities of intensive surveillance.

Meanwhile, with regard to oversight and regulatory aspects, **what is experienced in Poland is not an attempt to keep up with technological developments but rather a significant deterioration of the standards**. This creates an additional threat to civil rights and increases the awareness of the need for relevant legislative changes.

For example, it is still unclear whether the Central Anti-Corruption Bureau has purchased the Pegasus wiretapping system. According to the Supreme Audit Office the purchase could have been financed by the Justice Fund[9]. However, regardless of the purchase, several years of technological developments creates significantly greater possibilities for security services not only in Poland, but across the world.

6. International standards

In recent years, international standards regarding the observance of civil rights in the context of the activities of security services have been developing. However, **these standards are generally ignored by the Polish authorities** contrary to the recommendations of the CHR and non-governmental organizations.

In particular:

- the Polish law **fails to meet the standards applicable to the use of wiretapping and secret surveillance** (as well as the use of metadata), that arise from the **case law of the European Court of Human Rights** (*Klass and others v. Germany, Iordache v. Moldova, Liberty and others v. the United Kingdom, Zakharov v. Russia , Szabo and Vissy v. Hungary*[10]);
- the Polish law **fails to meet the standard of metadata collection and processing by**

[9] https://www.tvn24.pl/cba-kupilo-system-inwigilacyjny-za-pieniadze-dla-ofiar-przestepstw,870100,s.html

[10] Klass and others v. Germany, judgment of the European Court of Human Rights of 6 September 1978, complaint No. 5029/71, Iordache v. Moldova, judgment of the European Court of Human Rights of 10 February 2009, complaint No. 25198/02, Liberty and others v. the United Kingdom, judgment of the European Court of Human Rights of 1 July 2007, complaint No. 58243/00, Zakharov v. Russia, judgment of the European Court of Human Rights of 4 December 2015, complaint No. 47143/06, Szabo and Vissy v. Hungary, judgment of the European Court of Human Rights of 12 January 2016, complaint no. 37138/14.

security services for the purpose of obtaining information on "sensitive" individuals (e.g. lawyers, journalists), as set out in the recent well-known judgment on the case *Big Brother Watch and others v. the United Kingdom*[11];

- the Polish authorities do not implement the standards arising from the case law of the Court of Justice of the European Union, in particular as regards the **standards applicable to telecommunications data, based on the so-called Retention Directive** (*Digital Rights Ireland, Tele2*[12]) and the **procedural safeguards applicable to persons at risk of expulsion** (*ZZ v. Secretary of State*[13]).
- standards arising from the opinions of international organizations are not reflected upon. They are left aside which, given the weakness of the public debate as well as numerous other controversies subject to international-level discussion (e.g. the justice system reform) causes, in general, no significant damage to the image or legal situation of the public administration bodies.

The reference point in the current debates on the observance of civil rights in the activities of security services should be, in particular, **the opinion of the Venice Commission of 2016 on the *Police Act* and certain other acts**[14].

The Venice Commission made a comprehensive assessment of Polish legislation and formulated **the following recommendations for the Polish authorities**:

- to strengthen the proportionality principle, by elaborating the test applicable to the secret surveillance ordered under Article 19 and by introducing this test in relation to obtaining of metadata under Article 20c, in order to ensure that secret surveillance/metadata collection are to be ordered only in the most serious cases,

[11] Big Brother Watch and others v. the United Kingdom, judgment of the European Court of Human Rights of 13 September 2018, complaints Nos.: 58170/13, 62322/14 and 24960/15.

[12] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Sfochana, Ireland, The Attorney General and Karntner Landesregierung, Michael Seitlinger, Christof Tschohl and others, judgment of the Court of Justice of the European Union of 8 April 2014, case ref. no. C-293/12 and C-594/12, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis, judgment of the Court of Justice of the European Union of 21 December 2016, case ref. no. C-203/15 and C-698/15.

[13] ZZ v Secretary of State for the Home Department, judgment of the Court of Justice of the European Union of 4 June 2013, case ref. no. C-300/11.

[14] Opinion no 839/2016 on the Act of 15 January 2016 amending the Police Act and certain other Acts, adopted by the Venice Commission at its 107th Plenary Session (Venice, 10-11 June 2016), CDL-AD(2016)012-e, available at: https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD%282016%29012-e

especially under the "urgent procedure" (Article 19(3) of the *Police Act*);

- to prohibit in the Act surveillance of communications which are on the face covered by a lawyer-client privilege; to define precisely when this presumption can be overturned, and to do so also in respect of other privileged communications;
- to limit the duration of the metadata monitoring; to require the police to keep proper records which should enable effective ex-post control of the monitoring operations, especially implemented through "direct access";
- to complement the system of judicial pre-authorisation of the "classical" surveillance under Article 19 with additional procedural safeguards (a "privacy advocate", a complaints mechanism, a system of ex-post automatic oversight of such operations by an independent body, etc.);
- to provide, in respect of metadata collection under Article 20c, an effective mechanism of oversight of specific operations by an independent body; such body should have necessary investigative powers and expertise and be able to use appropriate legal remedies.

The above opinion of the Venice Commission has never been complied with. The state authorities responsible for the changes did not undertake a real discussion on relevant amendments of the legislation. Even the Council of Europe did little to demand that the Polish authorities respond to the above opinion. However, this does not change the fact that it is the most thorough and independent assessment of Poland's regulatory environment in the area in question.

Therefore, when proposing systemic and legislative changes we have taken account of the above recommendations as well as our conclusions regarding to-date experience with security services' activities and the related requirements arising from the Constitution and the international and European law.

III. INDEPENDENT OVERSIGHT BODY FOR SERVICES AUTHORIZED TO USE SURVEILLANCE

1. Main aims of the independent oversight body

Our main postulate is **to establish an independent oversight body to supervise the activities of security services.**

The main goals of work of the oversight body:

- to oversee **all services** authorized to conduct surveillance operations;
- the oversight would cover **surveillance operations as well as other activities** of the services authorized to interfere with civil rights and freedoms of individuals;
- the protection would cover **all persons irrespective of their nationality**;
- all individuals would have the **possibility to lodge a personal complaint**;
- the oversight body's powers would cover **the service's operations carried out in the country and abroad**;
- the oversight body would **analyse the services' activities with regard to their legality understood as the operations' compliance with the Constitution and the safeguards of the protection of civil rights and freedoms arising from the Constitution**, with account taken of the specific nature of work of intelligence services.

2. Independence of the oversight body

The oversight body for services authorized to conduct surveillance operations would be answerable to the **Sejm of the Republic of Poland**, and its members would **be apolitical, impartial in performing their tasks, and independent of the executive branch of power**.
In our proposal we have used experiences of different democratic countries including Belgium, Denmark, the Netherlands, Canada, Norway, Portugal and Sweden. These countries have adopted various models as regards the oversight body's placement within the system of the state authorities. Yet, in all cases, the fundamental characteristic of such a body is its independence.

In the Polish conditions, **the oversight body's answerability to the Sejm, accompanied by transparent rules of its appointment and principles of operation would ensure the**

greatest probability of maintaining its independence.

3. Procedure of appointing the oversight body members

The head and members of the oversight body would be appointed by the Sejm of the Republic of Poland by absolute majority of votes, with the consent of the Senate, from among persons with extensive knowledge and at least ten years of experience in the field of administration of justice, state oversight systems, state security or human rights protection. Prior to the voting in the Sejm, a public hearing of the candidates would be held.

The head of the oversight body would be appointed from among active or retired judges with at least ten years' experience in criminal or administrative cases.

Persons entitled to propose candidatures for the positions of the head of the body as well as its members would be: the **President of the Republic of Poland, the First President of the Supreme Court, the President of the Supreme Administrative Court, the President of the Supreme Audit Office and the Commissioner for Human Rights.**

The requirements to be met by candidates for members of the oversight body, as well as the procedure of their appointment, **should guarantee the body's independence and position of authority.** Therefore, we have assumed that the members of the body will be appointed by the Sejm of the Republic of Poland, with the consent of the Senate, solely from among the candidates proposed by the state authorities indicated in the parliamentary act, as this would limit the impact of current political manoeuvres on the body's composition.

Given the significant role of the head of the body, he/she should be a judge, while the other members should have knowledge and experience in various fields important for the body's operation.

4. The oversight body's composition and term of office

The oversight body would be composed of **its head and 5 members. Their term of office would be 6 years**.

Every 3 years, elections would be held to elect half of the body's composition. The head and

the members of the body would be able to hold the office for no more than two consecutive terms.

In other countries, such bodies have between 3 and 10 members. Therefore, the 6-person composition proposed by us meets the international standard. It should be noted that in most countries, such bodies oversee solely the country's security services but the body in Poland would oversee all services authorized to conduct surveillance operations. A similar solution has been introduced in Belgium which has two 3-person bodies: one that oversees the security services, and the other one that oversees the police.

5. The oversight body membership criteria

The body's membership would not be open to:

- current or former officers,
- current or former soldiers;
- current or former members of a service that is subject to oversight by the body;
- persons holding membership of a political party within the 5 years preceding his/her election to the body.

A member of the body would not be permitted to:

- hold another public function;
- be a member of a political party or participate in its activities;
- be a member of a trade union;
- have any employment-type relationship with another employer, with the exception of the position of an academic teacher or scientist at a university, the Polish Academy of Sciences, a research institute, a scientific institute or a support scientific entity.

The prohibition of membership of a political party or a trade union, and of being employed by another employer arises from the requirement that the body's members should be fully apolitical and independent. This principle is also reflected by the prohibition of political party membership over the last five years (i.e. a time longer than the Parliament's term of office). The body membership closure to former officers of services covered by the body's oversight is connected with the requirement of impartiality. It would be unacceptable for the members of the body to oversee operations once conducted by themselves or their former colleagues

or subordinates. However, the body could use the expertise of the service's former officers by employing them as staff members or experts (see point 16 below).

6. Requirements regarding access to classified information with the highest secrecy levels

Every member of the oversight body would be required to have a security clearance to access information classified as "top secret". With respect to the body's candidates and members, as well as its office personnel, **extended security screening would be conducted by the classified information protection officer of the Prison Service**.

The requirement of access to classified information with the highest secrecy levels is a necessity for members of the body. On the other hand, their security screening by one of the services subject to oversight by the body (e.g. the Internal Security Agency) would create an ambiguous situation of the controlled entity would screen the controlling entity. Hence our decision to assign, to the classified information protection officer of the Prison Service, the task of screening the members of the body and its office personnel. The Prison Service is the only service authorized to conduct extended screening proceedings but at the same time not authorized to conduct surveillance operations, and thus not subject to the oversight exercised by the oversight body.

7. Immunity of members of the body

A **member of the body** would enjoy immunity, similarly as members of Parliament or persons holding functions in certain state authorities (e.g. the Commissioner for Human Rights), and thus:

- **would not, without a prior consent of the Sejm of the Republic of Poland, be held criminally responsible or deprived of liberty**;
- **would not, without a prior consent of the Sejm of the Republic of Poland, be detained or arrested**, except for being detained in the act of crime, when the detention would be necessary to ensure appropriate course of the proceedings;
- his/her detention would have to be immediately reported to the Speaker of the Sejm of the Republic of Poland who could order immediate release of the detainee;
- **a member of the body could not, without a consent of the Sejm of the Republic of Poland, be held liable for actions performed within the scope of his/her function,**

also after the expiry of his/her term of office;

- a member or former member of the body could **be held liable by a court, under civil law provisions, for actions performed within the scope of his/her function, solely upon a consent of the Sejm** of the Republic of Poland and if the rights of third parties have been violated.

The body would control the services authorized to conduct surveillance operations as well as investigative operations. In this situation, possible actions by those services with regard to any of the body's members might cause suspicion that their actual reason is the member's function. Therefore, all actions of the services with regard to the body's members should be subject to control by the Sejm.

8. Responsibilities of the head of the body and its decision-making process

The head of the body would manage its work, represent the body and perform other tasks a specified in the parliamentary act. The head of the body would designate another member as a deputy of the head of the body during his/her absence.

Decisions of the body would be taken in its meetings. Activities conducted within the body's statutory tasks could be carried out by its designated members. **The body's decisions would be considered taken if supported by at least its three members. In case of equal division of vote numbers, the** head's vote would prevail. The specific rules of procedure of the body would be set out in its internal **regulations adopted by the body and approved by the Speaker of the Sejm of the Republic of Poland**.

The head of the body would play a very important role in its work. Therefore, the requirement for the function to be held by a judge would guarantee the body's independence and apolitical nature.

9. Oversight powers of the body

The body would have oversight of:

- Internal Security Agency [Agencja Bezpieczeństwa Wewnętrznego – ABW];
- Foreign Intelligence Agency [Agencja Wywiadu – AW];
- Internal Oversight Bureau of the Ministry of the Interior and Administration [Biuro

Nadzoru Wewnętrznego Ministerstwa Spraw Wewnętrznych i Administracji];

- Central Anti-Corruption Bureau [Centralne Biuro Antykorupcyjne – CBA];
- National Revenue Administration units authorized to conduct surveillance operations;
- Police;
- Military Counterintelligence Service;
- State Protection Service [Służba Ochrony Państwa – SOP];
- Military Intelligence Services [Służba Wywiadu Wojskowego – SWW];
- Border Guard, and
- Military Police.

In Poland, there are 11 services authorized to conduct surveillance operations. Five of them (ABW, AW, CBA, SKW and SWW) have the status of security services, as assigned to them by relevant acts of Parliament; the remaining 6 services are usually referred to as police-type services. It seems justified to extend the oversight to all the services although in other countries the oversight bodies supervise only the security services (as those whose activities interfere more strongly with civil rights and are less covered by judicial review).

10. The scope of oversight

The body's activity would be focused on **oversight of surveillance operations** conducted by the services (and described in relevant acts of the Parliament and internal classified regulations) as well as on oversight **of obtaining and processing sensitive data on citizens. Thus, the focus would be on the services' activity areas of which oversight is currently insufficient**.

The body would monitor the **compliance of the services' activities with the Constitution and other legislative instruments, i.e. the legality, necessity and proportionality of the services' activities in the areas of**:

- using secret surveillance;
- obtaining and processing telecommunications, postal and internet data;
- obtaining and processing data that constitutes banking secret;
- other surveillance operations described in relevant acts of Parliament, in internal rules on surveillance operations, or in other documents of security services.

In this respect, the oversight body would control expenditure of the services' **operational**

funds.

The body would **control the correctness of Polish citizens' personal data processing** by security services and by other services to the extent they process personal data in connection with their tasks aimed at ensuring national security.

In this regard, the body **would assess the services' all internal regulations, instructions, decisions, powers of attorney and authorizations, as well as contracts and arrangements with domestic and foreign institutions**.

The body **would not look into**:

- purposefulness and cost-effectiveness of work of the services, because sufficient powers in this field are held by the Supreme Audit Office and the Sejm Committee on Security Services;
- control of investigative operations conducted by the services, as this area is subject to oversight by prosecutors and courts.

11. Complaint filing with the oversight body

The examination of citizens' complaints regarding the security services' activities connected with their surveillance operations would be a key element of the system that would ensure the observance of civil rights in the operations of the services. **Any person who would feel aggrieved by any of the services would have the right to lodge a complaint with the body, with regard to the operation of the service in question.**

The body would examine complaints, within the scope laid down in point 10 above, lodged by:

- private individuals,
- state authorities,
- non-governmental organizations or other entities,
- officers,
- soldiers,
- the services' personnel,

with regard to the services' functioning, actions or failure to act, including, in particular, violation of the rule of law or the complainants' interests.

12. Complaint examination by the oversight body

When examining the lodged complaints the body would take the following steps:

- inform the person or other entity that has lodged the complaint whether it is grounded or not,
- if the complaint is considered grounded - notify the complainant of steps taken and of their results, with the exception of providing classified information,
- notify the prosecutor's office of any violations of law,
- inform the concerned service's supervisory body of any irregularities found,
- possibly, forward non-classified information on the examined complaint to the general public.

If, as a result of examining a complaint, the oversight body concludes that human or civil rights or freedoms have been violated, its **decision might constitute grounds for the complainant to seek compensation** from the State Treasury, under commonly applicable regulations.
We are of the opinion that it is necessary to balance the interests of the person whose rights have been violated and the interest of the state whose confidential information needs to be protected even if irregularities are found in the operations of the security services. Thus, we propose a solution that consists in providing non-classified information on the results of the body's activities to the complainant and, in the case of particularly severe violations, also to the general public, and in providing classified information to the prosecutor's office and the service's supervising authority. An additional safeguard for citizens would be the possibility to seek compensation on the grounds of the body's decision which considers the complaint grounded.

13. Oversight proceedings conducted by the body

The body would conduct oversight proceedings:

- **based on an annual work plan** submitted to the Speaker of the Sejm of the Republic of Poland and the Sejm Committee on Security Services;
- **based on an instruction from** the Sejm of the Republic of Poland, the Speaker of the Sejm or the Sejm Committee on Security Services;
- **at the request** of the President of the Republic of Poland, the Prime Minister, the

Commissioner for Human Rights, the First President of the Supreme Court, the Prosecutor General, the President of the Office for Personal Data Protection, or ministers responsible for individual services - with regard to those services;

- **on its own initiative**, in particular based on publicly available information on possible irregularities in the activities of the services, or such information obtained when examining a complaint.

The body's oversight proceedings with regard to the services would be conducted according to a pre-developed plan, based on an instruction or at the request or request of the authorities indicated in the parliamentary act. The body would also have the power to carry out ad hoc proceedings on its own initiative, based on publicly available information on possible irregularities in the activities of the services, or such information obtained when examining a complaint. It is important to ensure the flexibility of the body's work so that in the event of a suspected violation of law it can take immediate action to prevent the destruction of evidence of the unlawful acts.

14. No restrictions with regard to the subject and object of oversight

A necessary condition of effective oversight, in particular in case of suspected irregularities in the operation of security services, is the controllers' ability to quickly access all relevant materials without any restrictions. On the other hand, it is necessary to guarantee the security of information on the activities of security services and those who cooperate with them, as unauthorized disclosure of such information may pose a threat not only to the interest of the state but even to the lives of the services' officers and cooperating persons. **For this reason, the oversight of security services should be entrusted to a small specialized body composed of persons whose ability to maintain secrecy has been proven. The oversight body should have unrestricted access to information and premises of the services subject to its oversight.**

The body's right of oversight of security services within the above-mentioned scope would not be subject to any limitations in terms of its subject or object.

In the course of the audits, the body's members would have the right of unlimited access to the buildings and rooms of the audited service, to documents and materials related to the

service's activities, the right to enter and inspect buildings, structures, ICT networks and systems, to summon and interrogate witnesses, and to use the assistance of experts and specialists.

The heads of the audited services would be required to submit, at the body's request, all documents and materials, including those on electronic carriers, necessary to carry out the audit activities, as well as provide access to the audited service's ICT systems, including databases.

The detailed procedure of conducting audits and documenting its results would be analogous to those performed by auditors of the Supreme Audit Office.

15. Information on audit results

Within 14 days of the completion of the audit, the body would:

- present information on the audit results to the authority at whose instruction or request the audit was conducted;
- if the audit reveals a grounded suspicion of an offense, the body **would notify the competent prosecutor's office** as well as the head of the inspected service and its supervising authority;
- if the information on the results of the audit turns out to be of significant importance from the point of view of oversight of the services, **the body would forward that information to the Prime Minister and relevant ministers responsible for those services** and, in the case of special services, also to the Sejm Committee on Special Services.

Every year, the body would submit to the Sejm and the Senate non-classified information on its activities. The information would also be made public. Every year, the body would submit classified detailed information on its services to the Speaker of the Sejm of the Republic of Poland, the Sejm Committee on Special Services, the President of the Republic of Poland and the Prime Minister.

The body would have the right to make the results of its audits public, in particular if they relate to violation of civil rights and freedoms.

The body would forward, to the competent state authorities, classified information on the

results of the conducted audits. Cases of suspected offenses would be reported to a prosecutor. The body's non-classified annual report submitted to the Sejm and the Senate could be made public. In the case of the examination of particularly shocking matters concerning possible violations of civil rights and freedoms, the results of the related audits could also be made public.

16. Cooperation with the oversight body

Government administration bodies, local government bodies, state institutions and entrepreneurs would cooperate with the body to assist it in carrying out its tasks. **The body would cooperate with associations, civic movements, other voluntary groups and foundations that work for the protection of human and civil rights and freedoms**. Such organizations could suggest subjects of future audits and issues that should be of specific interest for the oversight body.

To this purpose, the body would organize meetings with representatives of the above-mentioned organizations, to be held at least once a year. The body **could also cooperate with foreign and international bodies and organizations that work for the protection of human and civil rights and freedoms, as well as with foreign bodies and institutions responsible for oversight of security services in their countries**.

The body’s cooperation with social organizations specialized in human rights protection would strengthen its position as an entity responsible for civilian control over security services, and promote the engagement of civil society and its increased influence on the operation of the state structures. Particularly in the initial period of the body’s work, the cooperation with similar oversight bodies from democratic countries would be of major importance. Cooperation between security services’ oversight bodies from various countries has been conducted for many years and has made it possible to exchange experience and information on legislative solutions and good practices.

17. Office of the oversight body

The oversight body would be supported by an office with **several dozen staff members** who would provide substantive and logistics support. **The office staff would have to meet the same security requirements and be subject to the same restrictions as members of the body**. It should be noted that the future parliamentary act establishing the body would impose on its members and office employees the same requirements with regard to secrecy, foreign travel, etc. as in the case of security service officers.

The office of the oversight body:

- would be managed by the office director reporting directly to the head of the body;
- the office director and employees would be required to have a security clearance to access information classified as "top secret";
- the office director and employees could not be members of a political party, could not engage in political parties' activities, and could not be members of a trade union.

The body would be authorized to seek opinions of experts. Such experts may not include security or police service officers, members or soldiers.

A former officer, soldier or member of such services would not be authorized to become the office director or employee before the expiry of 5 years of completing or leaving the service.

The head of the body would adopt its **internal regulations** that would specify the tasks and organizational structure of the office. The internal regulations would be subject to approval by the Speaker of the Sejm of the Republic of Poland. The costs of functioning of the oversight body and its office would be covered from the state budget.

The cost of establishing the body and its office would amount to several dozen million zlotys due to the necessity to provide secure rooms and ICT systems certified for processing classified information with the highest secrecy levels. However, the costs of subsequent functioning of the body should be no higher than several, at most over ten million zlotys per year.

Given that the annual **costs of the security services sector exceed PLN 1 billion**, the establishment of an oversight body that would monitor the services' compliance with the Constitution and other legislative acts and their observance of civil rights in the performance of surveillance operations does not seem to entail excessive costs.

IV. NECESSARY CHANGES REGARDING INDIVIDUALS' RIGHT TO INFORMATION AND DATA PROTECTION

1. The right to information and data protection in the context of the activities of security services

The second pillar of the reform of privacy protection in the police and special services sector, next to the establishment of an independent oversight body, should consist in **granting individuals the right to information on them being of interest to agencies authorized to collect their data**, and on their right of access to such data processed by those agencies.

The necessity to introduce this right arises from the standards of the constitutional law[15]. For example, the **Constitutional Tribunal in its judgment on the case ref. no. K 23/11** pointed out that the obligation to provide information *"seeks to eliminate the risk of uncontrolled compilation and maintenance of data files not useful for proceedings conducted by the state authorities, but of potential value for the future activities that are not yet known"*[16].

The need for such mechanisms has also been highlighted by **the European Court of Human Rights**[17] and the **Court of Justice of the European Union**[18]. In the case of *Schrems v Data Protection Commissioner*[19] The CJEU pointed out that *"legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter".* In the Case C-203/15, the CJEU, confirming the necessity to inform individuals of the collection of their telecommunications data, pointed out that *"such information is essential for them, in particular for exercising their right to lodge a complaint"*.

Such mechanisms operate in most EU Member States, which has been examined in the report of the EU Agency for Fundamental Rights, entitled *Surveillance by intelligence services:*

[15] See judgments of the Constitutional Tribunal: of 30 July 2014, case ref. no. K 23/11 and of 12 December 2005, case ref. no. K 32/04, and its decision of 25 January 2006, case ref. no. S 2/06.

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

[17] See, inter alia, judgments: of 18 November 1977 in the case of Klass and others v. Germany, of 4 December 2015 in the case of Zakharov v. Russia, and the ruling of 29 June 2006 in the case of Weber and Saravia v. Germany.

[18] See judgments: of 8 April 2014 on the joined cases C-293/12 and C-594/12, and of 21 December 2016 on the case ref. no. C-203/15.

[19] Judgment of the CJEU of 6 October 2015, case ref. no. C-362/14.

fundamental rights safeguards and remedies in the European Union - Mapping Member States' legal frameworks[20].

Granting individuals the right to information on them being of interest to agencies authorized to collect their data:

- will make it possible for concerned individuals to verify the legitimacy of such activities,
- at an earlier stage, will increase officers' awareness that their actions may be subject to verification,
- will reduce the risk of excessive and ungrounded interference with the right to privacy.

Before describing the proposed solution in more detail, we intend to recall the provisions of the Code of Criminal Procedure which provides mechanisms for informing concerned individuals that they have been subject to secret surveillance or their telecommunications data were collected (see Article 239 and 218 of the Code of Criminal Procedure, respectively). The practical application of these provisions is marginal. The **vast majority of secret surveillance and data collection activities take place at the pre-trial stage (based on the so-called competence-related Acts of Parliament) at which no notification mechanism is provided for**. Therefore, the proposed solution relates to the activities conducted at the pre-trial stage.

2. Proposed amendments regarding the right to information on secret surveillance

It is proposed that **an order to conduct secret surveillance should entail the obligation to notify the concerned person of it,** as a rule **12 months after the end of the surveillance.**

The obligation of information provision after 12 months exists e.g. in Germany and seems a reasonable compromise between the services' need to operate efficiently and the observance of the rights of individuals.

Another solution is **to postpone the notification, or to annul this obligation by way of a court decision taken at the request of the service that requested the court's consent to the use of secret surveillance.**

[20] https://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega

The postponement or annulment of the notification obligation should be made by way of a **decision of the court** which examined the application for the consent to the use of secret surveillance. The postponement should be possible **only** based on a **reasoned request** of the entity that requested the surveillance operation, and only if the entity has provided prima facie evidence the existence of:

- a risk to human life or health (e.g. of officers);
- a threat to national security (e.g. in the context of espionage).

3. Information on access to telecommunications, internet or postal data

Collection of telecommunications or internet data may constitute an interference with an individual's privacy, to the same degree as secret surveillance. **Therefore, it is proposed to introduce a mechanism to notify persons whose data has been collected about this fact.**

As a rule, the notification would be made 12 months after the end of the collection operation. As in the case of surveillance, such information should be provided with a 12-month delay.

Given that every instance of data collection by authorized agencies does not require prior authorization, it **will be the sole responsibility of those agencies to decide whether to postpone or annul the notification obligation**. This will be possible in situations similar as in the case of secret surveillance, i.e. if the entity has provided prima facie evidence of the existence of a risk to human life or health (e.g. of officers), or a threat to national security (e.g. in the context of espionage).

In addition, we also suggest the **possibility of annulment of the notification obligation** if the collected telecommunications, internet or postal data were **unnecessary and were thus immediately destroyed** (e.g. a list of telephone numbers recorded by BTS stations), as well as **in the case of so-called subscriber data**, i.e. data referred to in Article 20cb of the Police Act (and, respectively, in the so-called competences-related Acts of Parliament).

The independent oversight body referred to in Chapter III should oversee the implementation of the notification obligations by agencies authorized to collect data, in particular with regard to limitations in its implementation.

4. Correct implementation of the so-called Police Directive

The constitutional principle of information autonomy implies **individuals' right of access to official documents and data files** on them. The right of such access is a pillar of personal data protection and privacy. It also an indispensable supplementation of the above-described notification procedures that only relate to collecting information about citizens in specific manners (surveillance as well as collection of telecommunications, postal or internet data). The police and special services have the right of access to individuals' all personal data that is processed in both public and private databases.

The need to introduce a system of access to information on personal data processing (their content, source, legal grounds for processing, etc.) has been noted by the EU legislators. They thus introduced such a solution in the Police Directive no. 2016/680, with regard to crime prevention authorities. **The directive, within its scope of application, provides for individual's right of access to his/her personal data. However, this right may be subject to limitation if so necessary to:**

- avoid obstructing official or legal inquiries, investigations or procedures;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security;
- protect the rights and freedoms of others.

At the same time, the Directive (in its Article 17) provides for a mechanism whereby, if the rights of data subject to access his/her data are restricted due to the above-mentioned reasons, the rights of the data subject may also be exercised through the "competent supervisory authority". In this case, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The directive does not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, which means data processing to ensure **national security**.

The Police Directive was implemented into the Polish legislation by way of the Act of 14

December 2018 on the protection of personal data processed in connection with the prevention and combating of crime. The Act entrusted the tasks of the competent oversight body to the President of the Office for Personal Data Protection.

The Act **implemented the Directive in a faulty manner**, in particular by significantly **extending the scope of reasons for refusing to notify individuals of the processing of their data** and by **disregarding Article 17 of the Directive** according to which individuals may exercise their powers through the supervisory authority.

It is postulated to change the situation through:

1) ensuring that the list of reasons for refusing to provide information on the processed data is limited solely to the reasons provided for in the directive,

2) introducing a provision according to which the data subject will be able to request the President of the Office for Personal Data Protection to verify whether the access restrictions were grounded.

5. The independent oversight body as an entity complementary to President of the Office for Personal Data Protection

According to Article 3(2) of the Act implementing the so-called Police Directive its provisions do not apply to the protection of personal data processed in connection with ensuring national security, including as part of the implementation of the statutory tasks by the Internal Security Agency, Foreign Intelligence Agency, Military Counterintelligence Service, Military Intelligence Service and the Central Anti-Corruption Bureau.

Leaving aside the doubts as to the exemption's compliance with the directive, it should be noted that from the point of view of the Polish constitutional order, there are no grounds for excluding the protection of personal data of individuals (including their right of access to such data, that arises from information autonomy) processed by security services.

Therefore, it is postulated that also security services should be required to notify data subjects (upon request) of the processing of their personal data (with restrictions similar to those provided for under the so-called Police Directive). Within the scope that remains beyond the powers of the President of the Office for Personal Data Protection (as determined in the implementing act), similar tasks should be entrusted to the independent

body referred to in Chapter III.

V. OTHER SYSTEMIC AND LEGISLATIVE CHANGES

It is also proposed to introduce a number of systemic and legislative changes that relate to the activities of security services in the light of protection of civil rights and freedoms:

1. Decentralized submission to courts of special services' requests for consent to the use of wiretapping and surveillance.

Due to the fact that judges of the District Court in Warsaw are overloaded with tasks relating to issuing consents to use secret surveillance and wiretapping, a **change in the courts' territorial competence** to perform such tasks is proposed**.** The competence could be vested with regional courts e.g. those with jurisdiction over areas in which the individual services' regional units operate. For example, currently ABW has 5 regional units and CBA has 12 units.

The best solution would be to identify one court per court-system region, which would be responsible for conducting the tasks in this field. The lack of a decentralized system of considering the requests for consent to the use of secret surveillance significantly reduces the quality of judicial control over such requests filed by special services.

It does not need to be broadly explained that a court **composed of 1 judge** sitting in a closed session has limited possibilities to control, within **one or two days,** the legality of requests for consent to the use of secret surveillance, that are submitted by the services (mostly with regard to telephone conversations and short text messages) when there are **several dozen such requests pending**.

When introducing the solution under which the requests of special services would be considered by one regional court in each of the 11 court-system regions, consideration should be given to introducing a statutory mechanism to ensure equal workload on the courts. Such mechanism could consist, for example, in forwarding each request for consent to the use of secret surveillance to the special services oversight body for referred to in Chapter III. The body would assign the requests to specific courts in the sequence of receiving them, and

following the principle of exclusion of court competence to consider requests regarding its own jurisdiction (e.g. an application regarding the use of surveillance in the Poznań court-system area would have to be examined by a court from outside this area).

2. Regulating the consequences of entry in the register kept by the Head of the Internal Security Agency; more precise criteria of such entry, and the related appeal procedure (amendment of Article 6(1) and Article 6(3) of the *Act on anti-terrorist activities*)

In order to prevent "terrorist acts" the Head of the Internal Security Agency (ABW) keeps a register of persons who may be suspected of terrorism. **The regulations do not specify the types of data that may be included in the register** (the types of data are determined in a classified instruction of the Head of the Internal Security Agency). The information contained in the register may be transferred to a wide range of entities ("*according to their competences*").

Such system of keeping the register violates a number of constitutional standards:

- certainty of law (Article 2 of the Constitution),
- the right to privacy (Article 47 of the Constitution),
- information autonomy (Article 51 of the Constitution).

Standards of keeping classified registers have also been outlined by the European Court of Human Rights in its judgment in the case *Leander v. Sweden.*

It is postulated to introduce non-classified regulations that would:
➢ determine the catalogue of data that may be included in the register, ➢ precisely determine the purposes for which the data contained therein may be used, ➢ introduce the obligation to periodically verify the necessity for further retaining of the data entered in the register (similarly e.g. as set out in Article 22a(8) of the Act on the Central Anti-Corruption Bureau), ➢ grant individuals, in line with the general principles laid down in Chapter IV, the possibility to be informed of the entry in the register and to challenge the entry.

3. Introduction of controls over surveillance used with regard to foreign citizens and

over the collection of biometric data

It is postulated to withdraw the possibility to use secret surveillance with regard to foreign citizens according to other rules than those applicable to Polish citizens.

According to Article 9 of the *Act on anti-terrorist activities*, in certain situations the Head of the Internal Security Agency may order the use of measures equivalent to secret surveillance with regard to a foreign citizens, **without the consent** of the Prosecutor General and the competent court. This is against the generally applicable rule that every agency authorized to use secret surveillance, before starting to use it (or, in exceptional situations, after starting to use it) is required to obtain consent of two institutions that are independent of each other. In our opinion the current solution creates a significant risk of abuse. Furthermore, such a serious restriction of foreign citizens' right to privacy finds no justification under the Polish constitutional order as Articles 47, 49 and 51 of the Constitution safeguard the rights to privacy, confidentiality of correspondence and information autonomy with regard to all persons irrespective of their citizenship.

4. Repealing of Article 26 of the *Act on anti-terrorist activities*

The provisions of Article 26 of the *Act on anti-terrorist activities* are, in our opinion, contrary to the fundamental principles of a democratic state ruled by law. They use terms that are extremely vague, **thus creating grounds for far-reaching interference with people's rights and freedoms, in particular personal inviolability of individuals. Therefore, we postulate to repeal Article 26 of the *Act on anti-terrorist activities*.**

The provision of Article 26(1) of the *Act on anti-terrorist activities* **provides for the possibility to draw up a statement of charges on the basis of information obtained as a result of secret surveillance activities**. Such information may also constitute the basis for issuing a provisional detention warrant by a prosecutor. Therefore, provisional detention may be used based on an anonymous piece of information such as e.g. an officer's report on a meeting with an informant whose name is not indicated in the case file.

Furthermore, Article 26(2) of the *Act on anti-terrorist activities* **provides for the possibility of using provisional detention on the sole basis of the provision of prima facie evidence of**

committing, planning or preparing a terrorist crime. The provision fails to follow the rule that provisional detention may take place based on reasonable suspicion that the crime has been committed. This means there has to exist evidence that, firstly, the crime has taken place and, secondly, that the person deprived of his/her liberty is the perpetrator of that crime. Reasonable suspicion means there has been an objective assessment of the facts and it concluded that the person in question could commit the given crime.

The statement "provision of prima facie evidence" of committing, planning or preparing a terrorist crime, used in Article 26(2) of the *Act on anti-terrorist activities*, is vague. This regulation does not clearly indicate who and in what situation may be subject to the restrictions provided for therein. This, in turn, means the term is so imprecise that it is not possible to give its commonly binding interpretation and, consequently, its uniform application is not possible. Furthermore, the introduction of the possibility of provisional detention for a period of 14 days on the sole basis of the provision of prima facie evidence of committing, planning or preparing a terrorist crime (in practice e.g. on the sole basis of an anonymous report drawn up by Internal Security Agency) reminds of the past infamous practice of "detention with the purpose to obtain information".

5. Right of defence in proceedings concerning expulsion of individuals who pose a threat to national security

The provisions of Polish law translate into **highly automated actions of the state in cases of expulsion from the territory of the Republic of Poland of citizens of other EU Member States and other foreign citizens suspected of actions that pose a threat to the security of the state, or of conducting terrorist acts**. In such cases, the rights that build the so-called procedural fairness are not safeguarded.

Several cases that became famous in Poland in recent years[21] suggested there may have been violations of human rights standards[22] and EU law standards[23] in those cases.

[21] Cf. e.g. the cases of Ch. Marakchi and Ameer Alkhawlany. See: Tomasz Borkowski, Czy jesteśmy skazani na samowolę służb? [Are we bound to live with the arbitrariness of special services?], Krytyka Polityczna, 28 October 2016, https://krytykapolityczna.pl/kraj/czy-jestesmy- skazani-na-samowole-sluzb-specjalnych/

[22] Al-Nashif v. Bulgaria, judgment of the European Court of Human Rights of 20 September 2002, application no. 50963/99.

[23] ZZ v Secretary of State for the Home Department, judgment of the Court of Justice of the European Union of 4 June 2013, case ref. no. C-300/11.

The current regulations provide that a person suspected of the aforementioned acts:

- **may be expelled from Poland even before the court examines the case**,
- **does not have a guarantee of the full right of defence,** as there is no access to related materials collected by the security services.

In view of the above, taking account of the experience of other countries **it is proposed to introduce the principle that expulsion can only take place based on a court judgment issued after the examination of all collected evidence.**

As regards the right of defence, we are aware that the person concerned should not always have access to all the information gathered by special services. **In some countries, the issue of the right of defence has been solved by appointing special proxies who, on the one hand, represent the person concerned, and on the other hand are bound by specific obligations to keep the obtained information confidential. In Poland, the role of such a proxy could be held by the Office of the Commissioner for Human Rights.** The employees of the CHR Office who would represent the concerned persons before public administration authorities and courts, but would also be required to comply with the obligation to keep confidential all information obtained with regard to the necessity of the person's expulsion. This role of the CHR Office would require to be included in a relevant Act of the Parliament. As a result, the state interest with regard to the protection of state secrets would be protected and, on the other hand, the right to defence would be ensured. As there are only few such cases per year, it would be possible for the CHR Office to undertake this task without the need to significantly increase the Office's budget.

6. Fruit of the poisonous tree: amendment to the Code of Criminal Procedure and annulment of Article 168a of the Code

According to **Article 168a of the Code of Criminal Procedure,** *"Evidence may not be considered inadmissible solely on the grounds of the fact that it has been obtained in violation of the rules of procedure or by means of a prohibited act referred to in Article 1(1) of the Criminal Code, unless the evidence has been obtained in connection with the performance by a public official of his/her personal duties with regard to a murder, willful injury or deprivation of liberty."* The provision was adopted in April 2016.

In practice, Article 168 of the Code of Criminal Procedure **permits the use, in criminal proceedings, of evidence that has been obtained in violation of law** (e.g. as a result of illegal wiretapping, searches, so-called provocations, the use of torture, inhuman and degrading treatment, provided it has not resulted in health injury). **Therefore, the article provides significant grounds for abuse as despite the violation of law the evidence may still be used in the future during the proceedings.**

This provision was challenged by the CHR before the Constitutional Tribunal. However, because of procedural manipulations regarding the composition of the Constitutional Tribunal's adjudicating panel as well as the participation, in the examination of the case, of persons not authorized to adjudicate, the Commissioner withdrew his application from the Tribunal. The article in question is criticized in light of the doctrine and is criticized by courts. In particular, in its judgment of 27 April 2017 the Wrocław Court of Appeal, referring directly to the Constitution, refused to apply Article 168a of the Code of Criminal Procedure (II Aka 213/16).

The final observations of the UN Committee against Torture, of 5 August 2019, included a recommendation to abolish the article. In particular, the Committee expressed its concern over the applicability of this provision and ordered effective action to be taken to enact legislation that would explicitly prohibit the use of evidence obtained through torture or degrading treatment, so as to meet the requirements of Article 15 of the *Convention against torture*. The Committee called for repealing Article 168a of the Code of Criminal Procedure[24].

[24] The concluding observations of the UN Committee against Torture are available at:

VI. OTHER PRACTICAL CHANGES

1. Training programme for judges and prosecutors on how the oversight of security and police services should work

We are of the opinion that at present judges and prosecutors are not sufficiently prepared to exercise adequate oversight of the activities of security and police services within the framework of judges' and prosecutors' statutory competences. A training programme for judges and prosecutors (in the form of an application as well as activities of the National School of Judiciary and Prosecutors) should cover issues related to the activities of the police and special services.

In our opinion, the training should cover **all judges of courts' criminal divisions** (with particular emphasis on regional court and courts of appeal).

The training should cover the following topics:

- constitutional safeguards regarding the protection of the right to privacy and information autonomy;
- secret surveillance operations;
- documentation on wiretapping and secret surveillance activities;
- technologies at the disposal of security services;
- the systems of protection of classified information in Poland and in the world;
- significance of metadata in the activities of security services;
- rules and procedures for approving requests for consent to the use of secret surveillance as well as telecommunications and electronic data;
- technical aspects of the application of operational control and the downloading of telecommunications and electronic data.

2. Real possibility of access to materials based on which surveillance activities are carried out, and of their secondary assessment by oversight authorities (including judges/prosecutors)

https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CAT%2fC%2fPOL%2fCO%2f7&Lang=en

A regional court that examines a special service's request for consent to the use of secret surveillance must **have unlimited access to all information and materials that are available to the service with regard to the case indicated in the request**. The system may not be based only on information provision by the service, within the extent specified by it, without a real possibility of reviewing this information by the court.

At present, the procedures of considering requests for the court's consent to the use of secret surveillance do not ensure a real possibility to verify data on overall situation and context of the case for which the use of surveillance is to be permitted. It happens that judges who issue such consents do not know whether the operation during which surveillance is to be used is indeed justified by sound reasons, whether the importance of the case justifies the use of surveillance, whether the classification of persons to be subject to surveillance as "unidentified individuals" is justified, or whether the proceedings in the case are indeed related to issues of particular social or political significance, also in the context of the subsequent disclosure by the prosecutor's office of sensitive data regarding public figures.

We consider it justified to adopt regulations under which a court that examines a request for consent to use secret surveillance would, in justified cases (when in doubt as to whether all the materials have been submitted to it together with the request) have the possibility to apply to the body referred to in Chapter III for urgent ad hoc control of the fulfilment, by the requesting special service, if its statutory obligation to provide access to all the materials and information relating to the submitted request. Therefore, a system should be introduced under which the special service would not be the sole entity (not subject to any oversight) authorised to manage the information and materials to be forwarded to the court that examines the request for consent to use secret surveillance.

Steps should be taken to strengthen the substantive knowledge of the court that examines, in one-person composition, the requests filed by secret services. Currently, for practical reasons (the place where the requests are examined is the court's classified information office) and for formal reasons (the requests are subject to certain classified information clauses), the judge who examines such a request may not use any assistance of his/her office's employees or assistants.

Another important issue is to ensure appropriate working conditions for courts which examine requests of special services. **The conditions should be adequate to the significant role played by the judges and should be comfortable enough for them to make it possible to take informed and reliable decisions on matters that, by their very essence, are comprehensive in nature, and to comply with the necessary requirements regarding the protection of classified information.**

It is also necessary to introduce **the obligation to forward, to the regional court that has examined the special service's request, the decision taken by the court of appeal**. Today, if a request for consent to use secret surveillance is rejected by a judge and a related complaint is filed by the head of the special service or by a prosecutor, the judge is not informed of the content of the appeal court's ruling issued with regard to the complaint.

3. Harmonization of procedures of requesting consent to the use of secret surveillance and data retention

It would be justified to harmonize the procedures of requesting consent to the use of secret surveillance and data retention by:

- clearly determining, in relevant guidelines and recommendations for judges and prosecutors, what criteria have to be met by a correctly completed request for consent to the use of secret surveillance or to collect telecommunications and electronic data;
- determining uniform rules of cooperation between the system of justice and representatives of IT operators;
- introducing the possibility of electronic verification by judges, by means of remote access to data systems, of the time and methods of using secret surveillance and collecting telecommunications and electronic data;
- making it possible for judges to verify the legality and legitimacy of performing penetration tests by the Internal Security Agency with regard to IT system operators.

VII. BIOGRAPHICAL NOTES ON THE AUTHORS

(in alphabetical order)

Adam Bodnar - Ph.D. and Habilitated Doctor in law; Commissioner for Human Rights (2015-2020 term of office);

Tomasz Borkowski - officer of Special Services (Internal Security Agency [ABW] as well as Office for State Protection [UOP]); in 2011-2015 Secretary of the Governmental Council on Security Services; opposition activist in the Polish People's Republic;

Jacek Cichocki - former Director of the Centre for Eastern Studies (Ośrodek Studiów Wschodnich); in 2008-2011 Secretary of State in the Chancellery of the Prime Minister where he was responsible for Special Services coordination; in 2011-2013 Minister of the Interior, in 2013-2015 Minister-member of the Council of Ministers and Head of the Prime Minister's Chancellery, Chairman of the Standing Committee of the Council of Ministers; Head Secretary of the Governmental Council on Security Services in the cabinets of Donald Tusk and of Ewa Kopacz;

Wojciech Klicki - lawyer and activist; since 2012 connected with the Panoptykon Foundation; specialises in the powers of the police and special services, and in the relations between human rights and state security; member of the Citizens' Legislative Forum [Obywatelskie Forum Legislacji] and of the Professor Zbigniew Hołda Association;

Piotr Kładoczny – Ph.D. in law, lecturer at the Faculty of Law and Administration of the University of Warsaw; Secretary of the Board and head of the legal department of the Helsinki Foundation for Human Rights;

Adam Rapacki - retired Police general, in 2007-2012 Undersecretary of State in the Ministry of the Interior and Administration;

Zuzanna Rudzińska-Bluszcz – attorney at law, Chief Coordinator of Strategic Litigation in the Office of the Commissioner for Human Rights.