HELSINKI FOUNDATION for HUMAN RIGHTS

Warsaw, 28th April 2016

Amendment to the Act on Police and other legal acts regulating surveillance by the law enforcement agencies and security services

Comments of the Helsinki Foundation for Human Rights

The Helsinki Foundation for Human Rights (HFHR) is one of the oldest non-governmental organisations in Poland dealing with the protection of human rights and fundamental freedoms. As part of its activity, HFHR monitors the implementation of human rights standards. The matter of oversight of the security services including provisions concerning surveillance has been in the scope of HFHR's activity for last 20 years. HFHR submitted numerous opinions to the Parliament regarding previous changes in the Act on Police and related acts as well as it submitted *amicus curiae* briefs in the procedure before the Constitutional Tribunal (K 23/11).

The current analysis of the Amendment to the Act on Police and other acts is based on the legal opinion[1] published by the HFHR in December 2015. In January 2016, the representative of HFHR attended a meeting of experts organised by the Council for Digitalization (*Rada ds. Cyfryzacji;* advisory body of the Minister of Digitalization). On 13 January 2015, ten non-governmental organisations signed a letter addressed to the Members of the Parliament, in which they expressed the main demands concerning the discussed draft law. HFHR also took part in the meetings of parliamentary and Senate committees working on the draft Amendment.

The presented analysis is composed of the following parts:

1. Purpose of the adopted legislation.
2. National legislation on surveillance.
3. Supervision of access to telecommunications data.
4. Access to Internet data.
5. Operational surveillance (*kontrola operacyjna*).
6. Destruction of operational surveillance materials containing professional secrets.
7. Matters remaining outside the provisions of the Act of 15 January 2016.
8. Transitional regulations.
9. Broader context and recent amendments.
10. Conclusions.

Each of the parts is composed of three chapters: the legal provisions before the Constitutional Tribunal judgement, the analysis of the specific points of the Constitutional Tribunal judgement and legislation changes adopted in 2016.

[1]Opinion is available at: http://programy.hfhr.pl/monitoringprocesulegislacyjnego/files/2015/12/HFPC_opinia_ustawa_o_policji.pdf [in Polish].

1. Purpose of the adopted legislation

The need to adopt new provisions to the Act on Police and related acts resulted from the obligation to implement the Constitutional Tribunal's judgement of 30 July 2014 (Ref. No. K 23/11). The Tribunal pronounced as illegal a portion of the regulations concerning, among others, the collection by law enforcement agencies of telecommunications data or protection of professional secrets in the course of what is referred to in Poland as "operational surveillance", i.e. wiretapping.[2] The Tribunal ruled that these regulations shall become ineffective 18 months after the publication of the judgement, i.e. on 7 February 2016.[3]

In July 2015, the Senate made the first attempt to comply with the ruling by submitting draft legislation to the Sejm (Poland's Lower House). However, due to the end of the Sejm's term, the draft was not adopted.

On 23 December 2015, a group of MPs submitted a new draft legislation.[4] On 4 January 2016, the Minister of Digitalization held a meeting of the Council for Digitalization, an advisory body with invited experts. This provided a semblance of the draft's social consultation, however no further consultations took place in this regard. The Council evaluated the legislative amendment negatively.[5]

In the course of legislative works in the Sejm, both in August 2015 and in December 2015, the Sejm's Bureau of Research (*Biuro Analiz Sejmowych*) indicated that the proffered amendments contain regulations contravening European Union legislation due to, inter alia, an overly broad catalogue of crimes justifying access to data.[6]

On 15 January 2016, the Sejm passed the Act and on 29 January 2015, the Senate adopted legislation in which it submitted no amendments to said Act.[7] On 3 February 2016, the President of the Republic of Poland signed the Act[8] which became law on 7 February 2016.

2. National legislation on surveillance

The competence to conduct secret collection of data on individuals is regulated in two different kinds of statutes. First of all, so-called "trial wiretapping" (*podsłuch procesowy*) is regulated in the Code of Criminal Procedure (Article 237 of the Code). It requires that the court's decision to wiretap be notified to a person who was under surveillance.

The second kind of acts that regulate secret collection of data are acts regulating the competences of each law enforcement agency and security services, for instance Act on Police (1990), Act on Internal Security Agency and Intelligence Agency (2002) or Act on Anti-Corruption Bureau (2006). These acts regulate e.g. the so-called "operational surveillance" (*kontrola operacyjna*) which does not require notification. They also regulate access to telecommunications data and other competences which allow each service to complete their statutory tasks. These statutory provisions were subject of a judicial review conducted by the Constitutional Tribunal in the judgement of 30 July 2014. The case was initiated by the Ombudsman and Prosecutor General.

---

[2] Judgement is available [in English] at: http://trybunal.gov.pl/en/hearings/judgments/art/7004-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/.
[3] The was published in the Dziennik Ustaw [*Journal of Laws*] on August 6, 2014 (Dz.U. [*Journal of Laws*] pos. 1055).
[4] Sejm publication (*druk sejmowy*) No. 154.
[5] Opinion is available at: https://mc.gov.pl/files/rdc_uchwala_nr_10_ws._projektu_nowelizacji_ust._o_policji.pdf.
[6] Meanwhile, the reasons for the amendment contained only the enigmatic statement that the "the statute's subject matter scope does not contravene European Union law."
[7] Senate publication (*druk senacki*) No. 71.
[8] The Act was published on 4 February 2016 (Dz. U. [*Journal of Laws*] pos. 145).

In July 2014, the Constitutional Tribunal ruled that the provisions of the Act on Police and related Acts did not comply with the constitutional standard of secret collection of data. This standard should include precise and foreseeable provisions, legitimate aim of collection and effective guarantees from abuses of power including independent and effective oversight of secret services' access to data and protection of professional secrets.

The main problem related to the proper implementation of the judgement related to the fact that the government selectively interpreted the recommendations stated in the ruling. The government used the narrowing interpretation of the judgement focusing mainly on its sentence.

Changes introduced by the Act of 15 January 2016 cover several issues: establishment of supervision over the collection of telecommunications data by law enforcement agencies, collection and access to Internet data, limitations on surveillance, i.e. its maximum duration, protection of professional confidentiality, the ways in which surveillance may be conducted and specifying the meaning of "crimes harming economic foundations of the state."

3. Supervision of access to telecommunications data

The competence to access telecommunications data was regulated e.g. by the Act on Police:

Article 20c(1) of the Act on Police (before the Amendment of 15 January 2016)

"For the purpose of preventing or detecting offences, the Police may access data mentioned in Article 180c and Article 180d of the Telecommunications Act of 16 July 2004 (Journal of Laws no. 171, item 1800, as amended), hereinafter referred to as 'telecommunications data', and may process them."[9]

The Constitutional Tribunal found the existing regulations[10] as contravening the Polish Constitution since they lacked independent supervision over the collection of telecommunications data by authorized law enforcement bodies. In this regard, the Tribunal proposed a very general constitutional standard:

> *"The Constitutional Tribunal does not determine at this point what exactly a procedure for access to telecommunications data should look like, and in particular, whether it is necessary – with regard to every type of retained data referred to in Article 180c and Article 180d of the Telecommunications Act – to obtain permission for access thereto. Not always access to the data of the same type results in the same extent of interference in the freedoms and rights of the individual. Thus, in the opinion of the Tribunal, it may not be ruled out that, with regard to accessing telecommunications data in the course of operational and investigative activities, ex post facto supervision will be introduced as a rule. When regulating that mechanism, the legislator should take account, inter alia, of the special character and statutory scope of tasks of particular police forces and state security services, as well as of emergencies in which the quick collecting of telecommunications data may be necessary for the prevention or detection of offences. Pursuant to the constitutional requirement of efficiency in the work of public institutions (the Preamble to the Constitution), a mechanism should be created which would make it possible for police forces and state security services to effectively counteract risks.* ***Nevertheless, the Tribunal***

[9] Article 180c and 180d of the Telecommunications Act – Attachment no. 2

[10] Inter alia, Article 20c paragraph 1 of the Act on Police, Article 28 paragraph 1 point 1 of the act on ABW [*Internal Security Agency*] and AW or Article 18 paragraph 1 point 1 of the Act on the Central Anticorruption Bureau.

recognises arguments for the introduction of ex ante supervision in certain cases. In particular, what is meant here is access to the telecommunications data of persons that hold professions in which the public repose confidence*. However, the said issues must be appropriately weighed up by the legislator".*

The Tribunal found: *"Taking the above into account, Article 20c(1) of the Act on the Police, due to the fact that it does not provide for independent supervision over the process of granting access to telecommunications data referred to in Article 180c and Article 180d of the Telecommunications Act, is inconsistent with Article 47 and Article 49 in conjunction with Article 31(3) of the Constitution."*

The mechanism of supervision adopted in the Act amending the Act on Police of 15 January 2016 is based on the supervision conducted by the regional court (*sąd okręgowy*) on the basis of a statistical report prepared by the police. The analogous provisions were added to other acts regulating law enforcement agencies and security services.

Act on Police – supervision of access to telecommunications data after the Amendment of 15 January 2016

"Article 20ca. 1. Supervision over Police collection of telecommunications, postal or Internet data shall be provided by the **regional court of appropriate jurisdiction for the registered address of the Police body** to which the data was made available.
2. The Police body referenced in paragraph 1 shall convey, pursuant to regulations on the protection of confidential information, to the regional court described in paragraph 1, **semiannual reports** covering:
1) in the course of the reporting period, **the number of instances of collecting** telecommunications, postal or Internet data as well as the **types of said data**;
2) **legal qualifications of the acts** in connection with the occurrence of which applications were made to collect the telecommunications, postal or Internet data, or information about collecting data for the purpose of protecting human life or health or supporting search or rescue activities.

3. As part of the supervision described in paragraph 1, the **regional court may review materials justifying providing access to the** Police of telecommunications, postal or Internet data.
4. The regional court shall **inform** the Police body of the results of the supervision **within 30 days** from the completion thereof.
5. Collecting data pursuant to Article 20cb paragraph 1 shall not be subject to the supervision described in paragraph 1.

The Act of 15 January 2016 provides that the **collection of telecommunications data by law enforcement agencies shall not be subject to any *ex ante* supervision**. Meanwhile, *ex post facto* supervision shall be based on periodic reports presented by law enforcement bodies. The reports shall be submitted semi-annually to the appropriate regional court pursuant to the regulations on the protection of confidential information and shall thereby not constitute public information despite the fact such reports would contain exclusively aggregate information about obtained data (Article 20ca). The court's supervisory activities will be **optional**, **not obligatory**. Moreover, after conducting supervisory activities, the court will only be able to inform the supervised law enforcement service about the results, but will not be able to order destruction of collected data.

The legislator failed to differentiate the duty of supervision according to the type of data obtained (e.g. requiring *ex ante* control in the case of location data or billing data, which constitute a far

greater interference with individual informational autonomy then e.g. subscriber data). Furthermore, subscriber data is exempted from *ex post facto* supervision (Article 20cb paragraph 1 in conjunction with Article 20ca paragraph 5 of the Act on Police).

Article 20cb

Article 20cb. 1. For the purpose of prevention or detection of crimes or for the purpose of protecting human life or health, or supporting search or rescue activities, Police may obtain data:

1) from the register described in Article 179 paragraph 9 Act of 16 July 2004 – Telecommunications Act,
2) described in Article 161 Act of 16 July 2004 – Telecommunications Act,
3) in the case of a user which is not a natural person, the network terminal number and the registered office or place of performing economic activity, the company or name and organizational form of said user,
4) in the case of a stationary public telecommunications network – also the name of the town and street at which the network terminal made available to the user is located,

– and may process such data without the knowledge and consent of the person whom they concern.

Protection of professional secrets

Situations when telecommunications (as well as postal and Internet) data that constitute professional secrets protected pursuant to Article 178 or Article 180 paragraph 2 of the Code of Criminal Procedure [attachment 3] are not covered by the obligatory supervision of the court, which is particularly dangerous in the case of **journalist confidentiality of sources**. The previous regulations did not regulate this issue. The Tribunal did rule directly on this matter, however in the reasoning of the judgement it noted that: *Nevertheless, the Tribunal recognises arguments for the introduction of ex ante supervision in certain cases. In particular, what is meant here is access to the telecommunications data of persons that hold professions in which the public repose confidence.*

Proportionality

In its judgement the Constitutional Tribunal did not analyse whether the scope or purpose of collection of data met the constitutional standards of proportionality. The Tribunal merely noted in the reasoning for its judgment that the "*legislator did not make collecting data contingent upon the factual circumstances of a specific case, the actual threat level or, ultimately, the exhaustion of other means of collecting information less burdensome to the individual."* The Tribunal also noted, that "*not all data of this kind result in the same intensity of interference in human rights and freedoms."*

Article 20c of the Act on Police amended by the Act of 15 January 2016

„ Article 20c. 1. **For the purpose of preventing or discovering crimes or for the purpose of the protection of human life or health, or supporting search and rescue activities**, the Police may collect **data that does not constitute the contents of, respectively, telecommunications messages, posted mail or messages through services provided in electronic format,** as described in:

1) Article 180c and Article 180d of the Act of 16 July 2004 – Telecommunications Act (Dz. U. [*Journal of Laws*] of 2014, pos. 243, as later amended), hereinafter referred to as "telecommunications data,"

2) Article 82 paragraph 1 point 1 Act of 23 November 2012 – Act on Postal Services (Dz. U. [*Journal of Laws*] pos. 1529 and 2015 pos. 1830), hereinafter referred to as "postal data,"
3) **Article 18 paragraphs 1–5 Act of 18 July 2002 on providing services electronically** (Dz. U. [*Journal of Laws*] of 2013 pos. 1422 and of 2015 pos. 1844), hereinafter referred to as "Internet data"
– and may process such without the knowledge and consent of the party, which such concerns.

2. A telecommunications enterprise, postal operator, or service provider providing services electronically shall **make available free of charge the data** described in paragraph 1 to:
1) a police officer indicated in a written application of the Police Chief, Head of the Police Central Investigative Office, the Police Voivodeship Commander, or party authorized by the above;
2) upon the oral request of a police officer in possession of written authorization by the parties described in point 1;
3) via a telecommunications network to a police officer in possession of written authorization from the parties described in point 1.

3. In the case described in paragraph 2 point 3, making available of data described in paragraph 1, shall occur **without the participation of the employees of the telecommunications enterprise**, postal operator or service provider providing electronic services or with the indispensable participation of said employees if such possibility is provided for in an understanding concluded between the Police Chief and such entity.

4. Disclosure to Police of data described in paragraph 1 may occur via a telecommunications network, if:
1) use of the telecommunications network assures:
a) the ability to establish the party collecting the data, the form of data collected and the time at which such data was collected,
b) the technical and organizational security preventing access to the data by an unauthorized party;
2) such is justified by the specifics or scope of tasks performed by Police organizational units or activities conducted thereby.

5. The Police Chief, Commander of the Police Central Investigative Office and Voivodeship Commander shall maintain registers of applications to obtain telecommunications, postal and Internet data, [which registers shall] contain data identifying the organizational entity of the Police and Police officer collecting said data, its type, purpose for collecting such and the time at which such was collected. The register shall be maintained in electronic format pursuant to regulations on the protection of confidential information.

6. The Police Chief, Commander of the Police Central Investigative Office and Voivodeship Commander **shall convey** data described in paragraph 1 **relevant** to a criminal proceeding to a **prosecutor of appropriate subject-matter or geographic jurisdiction**. The prosecutor shall decide on the scope and form of using the conveyed data.

7. The data described in paragraph 1 not relevant to a criminal proceeding shall be subject to forthwith, commissionary and registered destruction.

Article 20da paragraph 1 added by the Act of 15 January 2016

> "1. For the purpose of searching for **missing persons,** the Police may obtain telecommunications, postal and Internet data and may process such without the knowledge and consent of the party whom they concern; provisions of Article 20c paragraphs 2–7 shall apply."

Tribunal does not offer a clear guidance on how to assess the proportionality of proposed Amendment, the point of reference should be sought elsewhere. The relevant standard for personal data protection was established by the Court of Justice of the European Union in the Digital Rights Ireland case. .The court's decision indicated a series of defects in the retention directive, inter alia:

- **the overly broad scope of the directive and data collected pursuant thereto**, and thereby lack of exclusions, inter alia, with respect to parties whose communication is covered by professional privilege (secrecy);
- lack of criteria describing **the most serious crimes**, which would substantiate access to such data;
- lack of requirements referencing ***ex ante*** **oversight** and, as such, lack of protection against abuse.

The Court of Justice of the European Union's decision in *Digital Rights Ireland* updates the need to verify which crimes, or rather the investigation and prevention of which crimes, may be associated with the need to collect telecommunications data. The necessity of such supervision results from the requirement of **proportionality** of limitations on personal data protection. The process of adopting the Act of 15 January 2016 lacked such verification.

The scope of competences regulated in Article 20(c) of the Act on Police is extremely broad. It covers "preventing or discovering crimes" as well as "protection of human life or health, or supporting search and rescue activities." Access to telecommunications, postal and Internet data is justified by any actions taken by the Police in order to prevent or discover any crimes, and not the most serious ones. Moreover, during the legislative process of the Amendment, no review was conducted of the extent to which collecting telecommunications data is necessary to investigate particular categories of crimes.[11] In the opinion of HFHR, the need to verify these regulations with respect to their usefulness and necessity results precisely from EU law as well as ECHR case-law. The adopted act *de facto* provides for **no substantive limitation** on law enforcement bodies' access to such data, meaning the act contravenes the guidelines of the Court of Justice.

What is more, under current legislation, collecting telecommunications, postal or Internet data would not be subject to the **principle of subsidiarity**, i.e. the access to the telecommunication data is not possible only if and when less burdensome means turnout (or may turn out) not useful (ineffective). Further, legislation adopted in January 2016 provides no obligatory automatic procedure (e.g. every three years) that would verify the usefulness and legality of collected data.[12]

Bearing in mind a very broad scope of cases when access to telecommunications data is allowed under Article 20c (1), lack of mechanisms to protect professional secrets and resignation from the subsidiarity requirement, it is highly unlikely that the court conducting the *ex post* oversight will find that access to data in any case was illegal.

4. Access to Internet data

[11] In a 2013 report, the Supreme Audit Office recommended such an analysis be conducted. [*cf*.: Information about the results of the audit "Collecting and processing by authorized entities data from billing, localization information as well as other data described in Article 180 c and d of the Telecommunications Act" (Ref. No. 107/2013/P/12/191/KPB)].

[12] The July 2015 draft legislation provided for the principle of subsidiarity as well as such obligatory verification.

Access to Internet data was not covered by the judgement of the Constitutional Tribunal of July 2014. The Act of 15 January 2016 adjusted the principles of collecting Internet data to statutes on each law enforcement agency or security services, and placed this data under the same legal regime as the collection of telecommunications data.

Previously, this regulation was contained in the Act on providing services via electronic means:

Previous regulation on the access to Internet data

Article 18. 1. A service provider **may process the following personal data** of a service recipient necessary to connect, formulate content, amend or dissolve the legal relationship between the two:

1) the service recipient's surname and given names;
2) the PESEL [*Universal Electronic System for Registration of the Population, i.e. the Polish national identification number*] or – such number has not been conferred – the number from a passport, personal identification document, or other identification document;
3) registered permanent residential address;
4) correspondence address, if different than the address described in point 3;
5) data used to verify the service recipient's electronic signature;
6) the service recipient's electronic addresses.

2. For the purpose of executing agreements or another legal act with service recipient, service provider may process **other data** necessary due to the specificity of the provided service or of its billing.

3. Service provider shall distinguish and demarcate data described in paragraph 2, as data which must necessarily be provided for the provision of services via electronic means pursuant to Article 22 paragraph 1.

4. A service provider may process, with service recipient's consent and for the purposes described in Article 19 paragraph 2 point 2, **other data** concerning service recipient, which is not necessary for the provision of services via electronic means.

5. A service provider **may process the following data**, which characterize the way in which a service recipient utilized services provided via electronic means (*operating data*):

1) designations identifying service recipient conferred pursuant to data described in paragraph 1;
2) designations identifying a telecommunications network terminal or a tele-information system used by the service recipient;
3) information about the initiation, termination and scope of each use of services provided via electronic means;
4) information about use by service recipient of services provided via electronic means.

6. A service provider shall provide information about data described in paragraphs 1-5 to state bodies for the needs of proceedings conducted by said bodies.

Amendments introduced into the act on providing services via electronic means pursuant to the Act of 15 January 2016:

Article 8. In the Act of 18 July 2002 on providing services via electronic means (Dz. U. [*Journal of Laws*] of 2013 pos. 1422 and of 2015 pos. 1844) **Article 18 paragraph 6 shall say as follows**:

"6. A service provider shall make available data described in paragraphs 1–5 free of charge to **state bodies authorized pursuant to separate regulations** for the needs of proceedings conducted by said bodies."

Above all, the definition of Internet data covers **a very broad catalogue of information** (Article 18 paragraph 1-5 of the Act on providing services via electronic means).

The previous wording of Article 18 paragraph 6 did not limit the scope of its application solely to criminal proceedings, but also included civil and administrative proceedings.[13] Such a general formula used in the statute resulted in doubts as to the scope of data which may be conveyed to state bodies.[14] Pursuant to the amended Article 18 paragraph 6, the only entities able to obtain Internet data will be those upon whom such authority was conferred by the acts on law enforcement agencies and security services or pursuant to procedural provisions.

HFHR considers the increased precision of the statute a positive development. However, this amendment should be construed in the light of other changes introduced at the same time, *inter alia*, in the Act on Police.

Act on Police amended by the Act of 15 January 2016

„Article 20c. 1. **For the purpose of preventing or discovering crimes or for the purpose of the protection of human life or health, or supporting search and rescue activities**, the Police may collect **data that does not constitute the contents of, respectively, telecommunications messages, posted mail or messages through services provided in electronic format,** as described in:

1) **Article 180c and Article 180d** of the Act of 16 July 2004 – Telecommunications Act (Dz. U. [*Journal of Laws*] of 2014, pos. 243, as later amended), hereinafter referred to as "telecommunications data,"
2) Article 82 paragraph 1 point 1 Act of 23 November 2012 – Act on Postal Services (Dz. U. [*Journal of Laws*] pos. 1529 and 2015 pos. 1830), hereinafter referred to as "postal data,"
3) **Article 18 paragraphs 1–5 Act of 18 July 2002 on providing services electronically** (Dz. U. [*Journal of Laws*] of 2013 pos. 1422 and of 2015 pos. 1844), hereinafter referred to as "Internet data"
– and may process such without the knowledge and consent of the party, which such concerns.

First**,** it will be possible to access Internet data after meeting the broad and therefore extensive requirement of "identifying, preventing, investigating or collecting and recording evidence of crimes or for the purpose of protecting human life or health or supporting search or rescue activities."

Second, the new regulation expands the ways of access to Internet data and at the same time the scope of the data. Pursuant to Article 20c paragraph 2 of the Act on Police, the service provider

[13] K. Klafkowska-Waśniowska, *Komentarz do Article18 ustawy o świadczeniu usług drogą elektroniczną* [in:] D. Lubasz (ed.), M. Namysłowska (ed.), W. Chomiczewski, K. Klafkowska-Waśniowska, *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, LexisNexis, 2011, pt. 10.
[14] *Dostęp państwa do danych użytkowników usług internetowych. Siedem problemów i kilka hipotez*, Raport Fundacji „Panoptykon", Warszawa 2013, pp. 21-22.

providing services via electronic means shall make available free of charge data, *inter alia*, via a telecommunications network to a Police officer possessing written authorization. At that point, disclosure of Internet data occurs without the involvement of the service provider's employees "if such possibility is provided for in an agreement concluded between the Chief of Police" and the service provider.[15]

Article 20c paragraph 2-4 of the Act on Police

2. A telecommunications enterprise, postal operator, or service provider providing services electronically shall **make available free of charge the data** described in paragraph 1 to:
1) a police officer indicated in a written application of the Police Chief, Head of the Police Central Investigative Office, the Police Voivodeship Commander, or party authorized by the above;
2) upon the oral request of a police officer in possession of written authorization by the parties described in point 1;
3) via a telecommunications network to a police officer in possession of written authorization from the parties described in point 1.

3. In the case described in paragraph 2 point 3, making available of data described in paragraph 1, shall occur **without the participation of the employees of the telecommunications enterprise**, postal operator or service provider providing electronic services or with the indispensable participation of said employees if such possibility is provided for in an understanding concluded between the Police Chief and such entity.

4. Disclosure to Police of data described in paragraph 1 may occur via a telecommunications network, if:
1) use of the telecommunications network assures:
a) the ability to establish the party collecting the data, the form of data collected and the time at which such data was collected,
b) the technical and organizational security preventing access to the data by an unauthorized party;
2) such is justified by the specifics or scope of tasks performed by Police organizational units or activities conducted thereby.

Third, Internet data, especially so-called operating data (Article 18 para. 5 of the Act on providing services via electronic means), still constitute an extremely broad scope of information. Further, it is not clear whether and to what extent this may include the contents of messages conveyed. This depends on, *inter alia*, the extent to which provisions of the Telecommunications Act concerning telecommunications confidentiality apply to services provided via electronic means (*inter alia*, in light of Article 159 paragraph 2 point 4 of the Telecommunications Act[16]).

In the face of the last of these reservations, Article 20c paragraph 1 of the Act on Police reserves that as part of this procedure, law enforcement agencies shall be able to obtain **data that does not constitute contents respectively of telecommunications messages, posted mail or messages sent via electronic services**. Here, it is obvious that the contents of such a message may be accessed only as part of operational surveillance, e.g. wiretapping, which requires *ex ante* court consent.

[15] This form of making data available may occur after meeting the conditions of Article 20c paragraph 4 of the Act on Police.
[16] Pursuant to this provision, it is prohibited to review, record, store, convey or otherwise use contents or data covered by telecommunications confidentiality by persons other than the sender and recipient of the message, unless such is: (…) 4) necessary for reasons other than those provided for by statute or separate regulations.

In HFHR's opinion, effectiveness of *ex post facto* court supervision conducted pursuant to, *inter alia*, Article 20ca of the Act on Police, is fundamental to evaluating how Internet data will be accessed. However, the regulation allows to collect a broad scope of data allowing fairly precise recreation of various aspects of private life as reflected by, *inter alia*, the kinds of visited webpages.

5. Operational surveillance (*kontrola operacyjna*)

Technical means used during operational surveillance

Operational surveillance is a method for secretly obtaining the content of communication. It is ordered by the regional court, the procedure is initiated by the competent authority (e.g. Police of Internal Security Agency) with the consent of the competent prosecutor.

The Constitutional Tribunal ruled that, *inter alia*, Article 19 paragraph 6 point 3 of the Act on Police and Article 27 paragraph 6 point 3 of the Act on the Internal Security Agency – construed to mean that the appropriate official body ordering a form of eavesdropping [operational surveillance] is required to indicate legally defined technical means for collecting the information and evidence and recording such in the manner used in the individual case – comply with Article 2 and Article 47 in connection with Article 31 paragraph 3 of the Constitution.

The previous wording of provisions of particular law enforcement agency statutes granting authority for surveillance is based on the wording of the Act on Police of 1990, which in Article 19 paragraph 6 provided that surveillance is conducted in secret and includes:

> *1) reviewing the contents of correspondence;*
> *2) reviewing the contents of posted mail;*
> *3) use of **technical means** enabling clandestine access to information and evidence and the recording thereof, in particular the contents of telephone conversations and other information conveyed via telecommunications networks.*

The Tribunal's interpretation of the reviewed statute indicates that the technical means described in Article 19 paragraph 6 point 3 of the Act on Police "must allow for the collecting of information about the individual and, cumulatively, recording thereof in a manner allowing its subsequent use." Furthermore, "the systemic interpretation of the statutes under review indicates they constitute supplementation and expansion of the capability to obtain information and evidence in excess of what is allowed by, *inter alia*, Article 19 paragraph 6 points 1 and 2 of the Act on Police." The Tribunal further found that the "expression <<reviewing the contents of correspondence>> is not limited solely to traditional forms of exchange of information, but includes every form of conveying information between parties, irrespective of form (traditional mail, e-mail, SMS, MMS, etc.)".

The Tribunal indicated a standard with respect to regulating collecting information about parties via secret surveillance by stating *"with respect to the principle of specificity of legal regulations and legislative forms of limitations on constitutional freedoms and rights **it is not categorically necessary to establish a finite list of technical means for surveillance**."* However, the standard expressed in the sentence of the judgement sets an obligation for the body ordering surveillance, i.e. the court, of a legally defined technical means to collect information and evidence and recording such as was used in the individual case.

Article 19 paragraph 6 of the Act on Police amended by Act of 15 January 2016:

Surveillance shall be conducted in secret and is based on:

1) collecting and recording the contents of conversations conducted using technical

means including via telecommunications networks;
2) collecting and recording images or sounds of persons from indoors, means of transport or locations other than public places;
3) collecting and recording the contents of correspondence including correspondence conducted via electronic means of communication;
4) collecting and recording data contained in data carriers, telecommunications terminal devices, information technology and tele-information systems;
5) collecting access to and review of the contents of posted mail.

Paragraphs 6a and 6b were also added:

6a. Surveillance does not include activities described in paragraph 6 point 2 based on collecting and recording of images indoors described in Article 15 paragraph 1 point 4a.[17]

6b. Performing acts described in paragraph 6a shall not require judicial consent.

The legislature decided to amend Article 19 paragraph 6 of the Act on Police (and other acts regulating operational surveillance). According to the new wording of this provision, operational surveillance consists of five methods. Article 19 paragraph 6 point 4 of the Act on Police engenders serious doubts, for it provides that surveillance is based on collecting and recording **data contained in data carriers, telecommunications terminal devices, information technology and tele-information systems**. Such wording of the statute constitutes **expansion** of the allowable surveillance scope as compared to the previous wording of Article 19 paragraph 6 point of the Act on Police. Due to the secret nature of court decisions ordering surveillance, which additionally do not contain justification in the event when requests for surveillance are approved, it is unusually difficult to verify whether the previous practice of conducting surveillance also included the authority to review data contained in data carriers or information technology systems.

This type of authority constitutes a kind of "secret search," which had hitherto occurred pursuant to Article 236a Code of Criminal Procedure, i.e. it required assurance of appropriate procedural guarantees to a party subjected to such activity.

Code of Criminal Procedure

Article 236. Upon a judicial or prosecutorial request concerning search, impounding of property and with respect to material evidence and other activities the right to suit inures to parties whose rights have been transgressed; suit against rulings issued or acts performed in connection with preparatory proceedings shall be reviewed by the district court in the jurisdiction of which the proceeding is being conducted.

Article 236a. Provisions of this section shall apply respectively to an administrator and user of a device containing information technology data or information technology system, with respect to data contained in said device or system or upon a medium subject to its administration or use, including correspondence conveyed via electronic mail.

The new wording of Article 19 paragraph 6 of the Act on Police means that a party whose computer was searched in such a manner may never learn of that fact (due to the lack of a duty of notification). In the opinion of the HFHR, such a far-reaching expansion of the scope of

[17] Article 15 paragraph 1: In performing activities described in Article 14, police officers shall be entitled to: (…) 4a) observe and record using technical means images from facilities designated for detained individuals are those held for the purpose of regaining sobriety, police children's shelters, processing facilities and temporary processing facilities (...).

surveillance along with the deterioration (as compared to the current legal condition in the Code of Criminal Procedure) of individual procedural rights, constitutes a disproportionate encroachment upon the private sphere of life and violates the confidentiality of correspondence and individual informational autonomy.

Legal basis for operational surveillance conducted by the Agency for Internal Security

The Constitutional Tribunal found unconstitutional Article 27 paragraph 1 in connection with Article 5 paragraph 1 point 2 let. b of the Act on the Internal Security Agency and Foreign Intelligence Agency.

Act on the Internal Security Agency (2002):

Article 27 paragraph 1

> "In performing investigative-reconnaissance activities performed by the Internal Security Agency for the purpose of performing tasks described in Article 5 paragraph 1 point 2, when other means have been ineffective or not useful, the court, upon the written request of the Head of the Internal Security Agency submitted after receiving the written consent of the Prosecutor General, may, by way of a directive, order operational surveillance."

Article 5 paragraph 1 point 2 let. b

Internal Security Agency tasks include (…):

> 2) investigating, preventing and detecting crimes (…)
>
> b) harming the economic foundations of the state (…).

This provision was deemed to contain an insufficiently precise limitation of the right and freedoms due to the lack of a defined list of crimes described in Article 5 paragraph 1 point 2 let. b.

However, the legislator failed to supplement the Internal Security Agency's tasks by correcting Article 5 of the Act on the Internal Security Agency and Foreign Intelligence Agency. The only changes reference the wording of Article 27 paragraph 1 of the Act on the Internal Security Agency, pursuant to which operational surveillance may be conducted for the purpose of investigating, preventing and detecting crimes described in "sections 35-37 Act of 6 June 1997 – Criminal Code (Dz. U. [*Journal of Laws*] No. 88, pos. 553, as later amended) and sections 6 and 7 Act of 10 September 1999 – Treasury Criminal Code (Dz. U. [*Journal of Laws*] of 2013 pos. 186, as later amended) — if such harm the economic foundations of the state."

This is an unusually broad list of crimes, including larceny with breaking and entering, destruction of property or motor vehicle theft while the foundation that remains in the statute requiring the crime to "harm the economic foundations of the state" is imprecise and difficult to verify.

Legal basis for conducting operational surveillance should be reflected in tasks performed by the Internal Security Agency described in e.g. Article 5 of the Act on Internal Security Agency. This has an influence on the legal basis for collecting telecommunications data. The amended Article 28 paragraph 1 regulating access to telecommunications and Internet data refers to Article 5 paragraph 1 of the Act on the Internal Security Agency and Foreign Intelligent Service, which still does not define crimes that "harm the economic foundations of the state." Therefore, the list of bases for the Internal Security Agency's collecting of telecommunications data remains open.

Collecting telecommunications and Internet data by the Internal Security Agency after passing of the Act of 15 January 2016

Article 28 paragraph 1 of the Act on the Internal Security Agency

"1. The Internal Security Agency may obtain data necessary to execute **tasks described in Article 5 paragraph 1**, which data do not constitute content of, respectively, a telecommunications message, posted mail or message conveyed pursuant to services provided via electronic means, as described in:

1) Article 180c and Article 180d Act of 16 July 2004 – Telecommunications Act (Dz. U. [*Journal of Laws*] of 2014 pos. 243, as later amended)), hereinafter referred to as "telecommunications data,"
2) Article 82 paragraph 1 point 1 Act of 23 November 2012 – Postal Act (Dz. U. [*Journal of Laws*] pos. 1529 and of 2015 pos. 1830), hereinafter referred to as "postal data,"
3) Article 18 paragraph 1–5 Act of 18 July 2002 on providing services via electronic means (Dz. U. [*Journal of Laws*] of 2013 pos. 1422 and of 2015 pos. 1844), hereinafter referred to as "Internet data"

– and may process such data without the knowledge and consent of the party whom the data concerns"

6. Destruction of operational surveillance materials containing professional secrets

The Constitutional Tribunal ruled that, *inter alia*, Article 19 of the Act on Police is unconstitutional **to the extent that it does not provide a guarantee for the forthwith, commissionary and registered destruction of materials containing information covered by evidentiary proscriptions (such as those established in Article 178 and 180 (2) of the Code of Criminal Procedure), as to which the court has not revoked professional privilege or such revocation was unlawful.**[18] The reasoning of the Constitutional Tribunal led to a conclusion that the previous wording of Article 19 of the Act on Police (and other acts regulating operational surveillance) does not provide adequate procedural guarantees for professional secrets. The Constitutional Tribunal stated:

> *The constitutional defect of Article 19 of the Act on the Police is the lack of a statutory guarantee – in the case of a justified suspicion that obtained material contains privileged information and hence requires special protection – that additional verification of the material will be carried out by a competent court and possibly the professional confidentiality requirement will be waived, before the material is provided to the functionaries of a given police force or state security service or to a public prosecutor. The Tribunal is aware of risks ensuing from the possibility of accessing privileged information by the said functionaries, especially that there is no clear statutory prohibition against the use of "the fruit of the poisonous tree". The said risk is serious, but not serious enough to exempt a certain group of individuals – including defence counsels and journalists – from the scope of operational surveillance. In this state of affairs, it is the legislator's obligation to introduce legal solutions which would prevent the risk of unauthorised use of information that requires protection, or which would at*

18 *„Taking this into consideration, the Constitutional Tribunal states that Article 19 of the Act on the Police – insofar as it does not provide for the guarantee of immediate, witnessed and recorded destruction of material that contains information prohibited from being used as evidence, with regard to which the court has not waived the professional confidentiality requirement or in the case of which the waiving of the requirement is inadmissible – is inconsistent with Article 42(2), Article 47, Article 49, Article 51(2) and Article 54(1) in conjunction with Article 31(3) of the Constitution".*

least minimise that risk.

(...)

Thus, binding guarantees provided for in the Code of Criminal Procedure with regard to information protected by professional confidentiality become illusory, since despite a general prohibition on using such privileged information as evidence in a given case, the legislator permits – although indirectly, by an ambiguous statutory regulation – that such information may be collected and stored by police forces and state security services authorised to carry out operational surveillance. This is particularly striking in the context of privileged information in possession of defence counsels and journalists (within the above-indicated scope), which – under the Code of Criminal Procedure – is covered by absolute legal protection in the form of a prohibition on the use of such information as evidence".

The amendments under review introduce in particular statutes (e.g. the Act on Police) a special procedure, which, contrary to the letter of the judgement, does not directly order destruction of the outlined materials.

Article 19 of the Act on Police amended by the Act of 15 January 2016

"15f. In the event the materials described in paragraph 15:

1) contain information described in **Article 178** Code of Criminal Procedure, the Chief of Police, Head of the Police Central Investigative Office or Voivodeship Commander of Police **shall order their forthwith, commissionary and registered destruction**;

2) may contain information described in Article 178a and Article 180 § 3 Code of Criminal Procedure, excluding information concerning crimes described in Article 240 § 1 Criminal Code or information constituting secrets related to performing a profession or function described in Article 180 § 2 Code of Criminal Procedure, the Chief of Police, Head of the Police Central Investigative Office or Voivodeship Commander of Police **shall convey said materials to a prosecutor**.

15g. In the event described in paragraph 15f point 2, the prosecutor, forthwith after receiving the materials, **shall submit them to the court** which ordered the operational surveillance or consented to such pursuant to the procedure described in paragraph 3 along with a **request** for:

1) a finding of which of the conveyed materials **contain information** described in paragraph 15f point 2;

2) admissibility in a criminal proceeding of materials containing information constituting professional secrets related to performance of a profession or function described in Article 180 § 2 Code of Criminal Procedure and not covered by proscriptions described in Article 178a and Article 180 § 3 Code of Criminal Procedure, with the exclusion of materials concerning crimes described in Article 240 § 1 Criminal Code.

15h. Forthwith after submission of a request by the prosecutor, the court shall issue a finding of admissibility of materials described in paragraph 15g point 2, when such is **necessary in the interest of justice and circumstances cannot be established pursuant to other evidence**, and shall also order the forthwith destruction of materials inadmissible in a criminal proceeding.

15i. The prosecutor shall be entitled to **appeal** the court's ruling concerning admissibility in a criminal proceeding of materials described in paragraph 15g point 2. Provisions of the Code of Criminal Procedure shall appropriately apply to the appeal.

15j. A Police body shall be obligated to execute a court order to destroy materials described in paragraph 15h, and the forthwith, commissionary and recorded destruction of materials inadmissible in a criminal proceeding. The Police body shall forthwith inform the prosecutor described in paragraph 15g regarding the destruction of such materials."

The Act of 15 January 2016 provides that the confidential materials described in Article 178 of the Code of Criminal Procedure (defence and confessions) shall be destroyed (and such shall be recorded) by the service which collected such information. Meanwhile, in the case of other secrets described in Article 180 (2) of the Code of Criminal Procedure, the collected information shall be obligatorily conveyed to the prosecutor[19] who, however, shall not be able to verify such and order their destruction, but will have to automatically convey them to the court (Article 19 paragraph 15f of the Act on Police). In turn, the court shall rule on their admissibility in a criminal proceeding "if such is necessary for the interests of justice and the circumstances may not be established pursuant to other evidence." The court shall also rule on the destruction of inadmissible materials.

The Constitutional Tribunal emphasized the duty to guarantee "forthwith, commissionary and recorded destruction of materials containing information covered by evidentiary proscriptions." Meanwhile, the Act of 15 January 2016 gives primacy to a procedure that would allow the use of the previously collected information in the future criminal procedure.

Secondly, the planned procedure provides for an **extremely broad "accessibility"** to collected information containing professionally privileged communication. An example of this is the duty to convey the collected materials to the prosecutor, who then has a duty to convey them further to the court. Further, it is unclear what the purpose of conveying such information to the prosecutor is. The prosecutor has no jurisdiction to independently order the Police to destroy such materials, but may only submit an appropriate request to the court. What is more, in light of the wording of Article 19 paragraph 15g, the prosecutor may not request destruction of the materials. The provision does not call for the prosecutor's supervisory role in conducting the operational surveillance. It merely leads to expanding the group of individuals able to review the materials containing professionally privileged communications collected in the course of operational surveillance.

Furthermore, the Act does not provide for the duty to inform individuals subject to the duty of professional confidentiality that such protected information has been collected in the course of operational surveillance.

7. Matters remaining outside the provisions of the Act of 15 January 2016

The amendment still does not implement the notification requirement set by the Constitutional Tribunal on 25 January 2006 (Ref. No. S 2/06). The Tribunal indicated the need to establish a **duty to inform individuals covered by operational surveillance that such has been conducted**. The Tribunal argued that "*existence of such a police duty is certainly recommended and would respond to the need for effective procedural implementation of the constitutional right described in Article 51 paragraph 4 of the Constitution. A similar problem in other European states led to raising the procedural guarantee standard (German legislation, in light of the Klass and others case – an affirmative duty to inform of in-progress and completed operational surveillance)*".

The Constitutional Tribunal also referenced this in its decision of 30 July 2014, indicating that among the constitutional standards referencing surveillance-investigative activities there exists a

[19] In case of operational surveillance conducted by the Internal Security Agency – materials are conveyed to the Prosecutor General (Minister of Justice).

requirement to "*establish norms for the procedure of informing parties about the secret collection of information about them within a reasonable time after the completion of operational activities and assuring, upon the interested party's request, judicial review of the legality of the use of such activities; departure from such is permitted by way of exception.*"

In the justification for the draft act of 16 January 2016, the authors do not share the conclusions flowing from the 2006 ruling on the duty to inform and the 2014 decision, and indicate three types of obstacles to implementing the duty to inform:

> - It would violate the fundamental principles pursuant to which law enforcement services function, and could materially hinder the effective operation of said services, but could also threaten the security of Armed Forces of the Polish Republic as well as individuals providing covert assistance to law enforcement.
> - It would result in difficulties with establishing the personal data of individuals due to the material scale of use of so-called prepaid telephones.
> - It would contravene the legal requirement to protect the forms and methods of investigative-surveillance activities and the fact that such are being conducted.

The legislator attempted to argue why the duty to inform should not be introduced into law. In the opinion of the HFHR it is possible to implement the Constitutional Tribunal's duty to inform into the Polish legal order while securing the public interest of order and public safety. First, the concern that the duty to inform could *"hinder the effective operation of said services*" may be mitigated by delaying such duty in time until e.g. the completion of the procedure in progress in cases where collected materials have not led to the initiation of preparatory proceedings. Second, if an individual under surveillance uses prepaid phones, it is possible for the statute to contain an appropriate exclusion pursuant to which the inability to establish subscriber data would render impossible the duty to inform in such case. Third, it is significant that the referenced duty to protect the forms and methods of law enforcement operations flows from statute, while the duty to inform individuals that he or she was subject to operational surveillance flows from the referenced interpretation of Article 51 paragraph 4 of the Constitution. An argument suggesting that it renders impossible the execution of obligations that arise under constitutional norms may engender doubt as to its constitutionality. Meanwhile, the converse argument that the constitutional requirement does not comply with legislative norms, violates the constitutional hierarchy of generally applicable laws.

In the opinion of the Helsinki Foundation for Human Rights, execution of the Constitutional Tribunal's ruling of 30 July 2014 requires implementation of the Tribunal's order of 25 January 2006 to include the appropriate duty of notification. The duty to inform should, at a minimum, cover professions of public trust to the extent to which law enforcement collected and subsequently destroyed professionally privileged information.

The second issue that was not covered by the Amendment is creating an independent body with jurisdiction to control all aspects of law enforcement and security services' activities (e.g. signals intelligence). As such, the proffered law creates no mechanism for a complaint by a party subject to surveillance. Proposal to establish such a body appeared in 2013. However, after submission of a draft law on the Control of Special Services, work on amendments ceased. Currently, independent judicial oversight of law enforcement is selective (e.g. with respect to ordering operational surveillance). The remainder of law enforcement activity remains outside such on-going independent expert control.

8. Transitional regulations

Transitional regulations of the Act of 15 January 2016 also engender serious reservations. The

regulations provide for the possibility of continued use of hitherto applicable regulations despite the fact that these have been deemed unconstitutional by the Tribunal.

> Article 13. **Hitherto regulations** shall apply to operational surveillance conducted prior to and not completed subsequent to applicability of the new act.
>
> (…)
>
> Article 15. **Hitherto regulations** shall apply to proceedings regarding access to data described in Article 180c and Article 180d Act of 16 July 2004 – Telecommunications Law and data identifying a party using mail services and concerning the fact or circumstances of providing mail services or using such services, which have been initiated and not completed prior to the act's entry into force, and to collected data.
>
> Article 16. **Hitherto regulations** shall apply to operational surveillance conducted pursuant to Article 27 paragraph 1 of the Act of 24 May 2002 on the Internal Security Agency and Foreign Intelligence Agency for the purpose of performing tasks described in Article 5 paragraph 1 point 2 let. b of said act, which have not been completed prior to the act's entry into force.

9. Broader context and recent amendments.

1. After the Act of 15 January 2016 was adopted, the Parliament amended the Law on the Prosecution.[20] According to Article 1(2) of the Law, the position of the Prosecutor General is held by the Minister of Justice, who is entitled to influence each investigation conducted by other prosecutors. The Prosecutor General is entitled to give instructions on procedural issues (Article 7) and decides on every aspect of human resources policy in the prosecutors' offices.[21] What is particularly important, the Prosecutor General may request to carry out operational activities (*czynności operacyjno-rozpoznawcze*)[22] undertaken by the relevant competent authorities, if they remain in direct connection with the ongoing investigation. The Prosecutor General is entitle to get access to the materials collected in the course of such activities.

2. The Code of Criminal Procedure was amended in March 2016.[23] The draft of law (introduced to the Parliament in January 2016) proposed to delete Article 168a of the Code.[24] However, during the work of the parliamentary committee, a new wording of the provision was introduced:

> Evidence cannot be considered inadmissible solely on the grounds that it was obtained in violation of the rules of procedure or by means of an offense referred to in Article 1 § 1 of the Penal Code, unless the evidence has been obtained in connection with the performance by a public official duties as a result of: murder, willful causing of bodily injury or imprisonment.

3. Introduction of Article 168b of the Code of Criminal Procedure and deletion of "*ex post*" consent of the court

---

20 Law of 28 January 2015 on Prosecutor Office (Prawo o prokuraturze, Journal of Laws, pos. 177).

21 A number of prosecutors have been ordered to change their place of work and are delegated to different prosecutorial units.

22 Operational activities covers all secret methods of obtaining the evidence. It contains of i.e. operational surveillance and access to telecommunication data.

23 Act of 11 March 2016 amending the Code of Criminal Procedure and other acts (Journal of Laws, pos. 437).

24 The provision stated that: „It is unacceptable to conduct and use evidence obtained for purposes of criminal proceedings by means of an offense referred to in Article. 1 § 1 of the Criminal Code". It entered into force on 1 July 2015.

Moreover, the amendments to the Code of Criminal Procedure introduced Article 168b:

If, as a result of operational surveillance, ordered at the request of an authorized body on the basis of special provisions, evidence was obtained that the person towards whom the operational surveillance was used committed a publicly prosecuted crime or a fiscal offense different than that covered by the operational surveillance order or that a person different that that covered by the operational surveillance order committed a publicly prosecuted crime or a fiscal offense, the prosecutor decides on the use of such evidence in criminal proceedings.

The previous procedure regulating the so-called "ex-post consent procedure" (*kontrola następcza*) conducted by the court was deleted. It was regulated e.g. in Article 17 of the Act on Anti-Corruption Bureau and in Article 19 of the Act on Police.

Article 17 para. 15a-15e of the Act on Anti-Corruption Bureau (deleted by Article 18 of the Act of 11 March amending the Code of Criminal Procedure and other acts):

15a. The use of evidence obtained in the course of operational control shall be permitted solely in a criminal procedure for a criminal or fiscal offence in relation to which such control by any competent entity is permitted.

15b. The Public Prosecutor General shall take a decision on the scope and manner of application of the submitted materials. Article 238 § 3-5 and Article 239 of the Act of 6 June 1997 – the Code of Criminal Procedure shall be applied respectively.

15c. In the event of obtaining, in the course of operational control, evidence that a criminal or fiscal offence, in relation to which operational control may be ordered, has been perpetrated by a person in relation to whom operational control has been performed, **other than referred to in the regulation on operational control, or perpetrated by another person**, the decision to use such evidence in a criminal procedure is issued by the **court**, referred to in section 2, at the request of the Public Prosecutor General.

15d. The request referred to in section 15c shall be submitted to the court by the Public Prosecutor General within one month of the date the Prosecutor receives the materials gathered in the course of operational control, submitted to him by the Head of the CBA without delay, not later than 2 months of the date of the control's completion.

15e.The court shall issue a decision referred to in section 15c within 14 days of the date of the request submission by the Public Prosecutor General.

4. Draft of the Law on Anti-terrorism Actions

On 21 April 2016, the Minister of Internal Affairs and Administration published a draft of the Law on Anti-terrorism Actions. Article 7 of the draft provides a competence to conduct operational surveillance (analogous to one conducted under Article 19 paragraph 6 of the Act on Police) against foreigners without the prior consent of the court.

Article 7 of the draft Law on Anti-terrorism Actions

In order to identify, prevent or combat terrorist crimes, the Head of the Internal Security Agency

may order towards a person who is not a Polish citizen, for a period not longer than three months, clandestine performance of activities consisting in:

1) collecting and recording the contents of conversations conducted using technical means including via telecommunications networks;
2) collecting and recording images or sounds of persons from indoors, means of transport or locations other than public places;
3) collecting and recording the contents of correspondence including correspondence conducted via electronic means of communication;
4) collecting and recording data contained in data carrier, telecommunications terminal devices, information technology and tele-information systems;
5) collecting access to and review of the contents of posted mail.

2. The Head of the Internal Security Agency shall immediately inform the Prime Minister and the Prosecutor General about the order referred to in paragraph 1.

3. The actions referred to in paragraph 1 may be extended under the terms of Article 27 of the Act of 24 May 2002 on the Agency of Internal Security and Intelligence Agency.

4. The Head of the Internal Security Agency informs the Prosecutor General of the results of the actions referred to in paragraph 1 immediately after their completion and, at his request, about the course of these activities, presenting materials collected in the course of these activities. The Prosecutor General may order termination of the activities referred to in paragraph 1.

5. The Head of ABW forwards all materials collected during the use of the actions referred to in paragraph 1 to the Prosecutor General. The Prosecutor General shall decide on the scope and use of the materials. Article 238 § 3-5 and Article 239 of the Code of Criminal Procedure shall apply accordingly.

6. Prosecutor General orders the destruction of those materials obtained as a result of the actions referred to in paragraph 1 which do not contain evidence of a criminal offense or are not relevant to national security.

7. The Head of the Internal Security Agency orders immediate, commissionary and recorded destruction of materials referred to in paragraph. 6.

10. Conclusions

1. Access by law enforcement agencies and security services to telecommunications and Internet data remains beyond independent and effective control.

2. The extremely broad scope of Article 20(c) of the Act on Police means that the adopted act *de facto* provides for **no substantive limitation** on the law enforcement angencies' access to telecommunications, Internet and postal data.

3. Access to telecommunications, postal and Internet data by law enforcement agencies and security services is not subject to the principle of subsidiarity.

4. New regulations on the access to Internet data allow to collect a broad scope of data enabling a fairly precise recreation of various aspects of private life.

5. New wording of Article 19 paragraph 6 (regulation of "operational surveillance") constitutes

expansion of the allowable surveillance, as compared to the previous wording of the provision.

6. The term "harming the economic foundations of the state," contained in the description of one of the task of the Internal Security Agency, is still not defined in the statute.

7. The Amendment does not provide an effective guarantee against the abuses with respect to the protection of professional secrets.

8. The Amendment still does not implement the notification requirement set by the Constitutional Tribunal on 25 January 2006 (Ref. No. S 2/06). The Tribunal indicated the need to establish a duty to inform individuals covered by operational surveillance that such surveillance has been conducted.

9. Under Polish law, there is no independent oversight body with a jurisdiction to control all aspects of law enforcement agencies' and security services' actions.

10. Transitional provisions of the Amendment provide for the possibility of continued use of the hitherto applicable regulations, despite the fact that these have been deemed unconstitutional by the Tribunal.

11. New amendments – adopted after January 2016 – concerning different aspects of surveillance also pose a threat to the right to privacy and secrecy of communication. However, the ongoing constitutional crisis and the refusal of the Government to publish and implement the judgements of the Constitutional Tribunal, reduce a factual possibility that the new law on surveillance will be subject to constitutional review.

Attachments:

Attachment 1: Article 237 and 239 code of criminal procedure

Article 237. § 1. After the proceedings have started, the court, upon a motion from the state prosecutor may order surveillance and recording of the content of telephone conversations, in order to detect and obtain evidence for the pending proceedings or to prevent a new offence from being committed.
(…)
§ 3. The surveillance and recording of the content of telephone conversations is allowed only when proceedings are pending or a justified concern exists, about the possibility of a new offence being committed regarding: […].

Article 239.
§ 1. The announcement of the order to conduct surveillance and recording of telephone conversations to the person concerned, may be adjourned for a period necessary to promote the proper conduct of the case.
§ 2. The announcement of the order, referred to in para. 1, during the preparatory investigation may be adjourned not beyond the valid conclusion of preparatory investigation.

Attachment 2: Article 180c and 180d of the Telecommunications Act (2004)

Article 180c. 1. The obligation referred to in Article 180a (1) shall cover the data necessary to:
1) trace the network termination point, telecommunications terminal equipment, an end user:
a) originating the call,
b) called;
2) identify:
a) the date and time of a call and its duration,
b) the type of a call,
c) location of telecommunications terminal equipment.

2. The minister competent for communications in agreement with the minister competent for internal affairs, having regard to the type of telecommunications activities performed by operators of a public telecommunications network or providers of publicly available telecommunications services, data specified in paragraph 1, costs of data collection and retention as well as the need to avoid multiple retention and storage of the same data, shall specify, by means of an ordinance:
1) a detailed list of data referred to in paragraph 1;
2) types of public telecommunications network operators or providers of publicly available telecommunications services obliged to retain and store the data.

Article 180d. Telecommunications undertakings shall be obliged to provide conditions for access and retention as well as to make available at their own cost the data referred to in Article 159 (1) (1) and (3) to (5), in Article 161 and in Article 179 (9) related to the provided telecommunications service and processed by them to authorized entities, the Customs Service, the court and to the prosecutor, under the terms and observing the procedures specified in separate provisions.

Article 159. 1. The communications confidentiality within telecommunications networks, hereinafter called the "telecommunications confidentiality", shall encompass:
1) data concerning the user;
2) individual message content;
3) transmission data understood as data processed for the purpose of transferring messages within

telecommunications networks or charging payments for telecommunications services, including location data, which should be understood as any data processed in a telecommunications network or within the framework of telecommunications services indicating geographic location of terminal equipment of a user of publicly available telecommunications services;
4) location data, understood as location data beyond the data necessary for message transmission or billing;
5) data relating to call attempts between specific telecommunications networks termination points, including data relating to unsuccessful call attempts meaning calls between telecommunications terminal equipment or network termination points which have been set up and not answered by an end user or aborted.
2. Knowledge, record, storage, transfer or another use of contents or data subject to telecommunications confidentiality by individuals other than the message sender and receiver shall be forbidden, unless:
1) this constitutes the subject of a service or is required to perform it;
2) this is agreed by a sender or a receiver whom such data concerns;
3) performing this action is essential to record messages and associated transmission data applied within legal business practice for the purpose of ensuring evidence for commercial transactions or for the purpose of communications in commercial activities;
4) this is necessary for other reasons provided for in the Act or separate regulations.
3. With the exception of cases specified in the Act, the disclosure or processing of content or data subject to telecommunications confidentiality shall violate the obligation to keep the telecommunications confidentiality.
4. The provisions of paragraphs 2 and 3 shall not apply to messages and data public by their nature, data for a public purpose or disclosed by a ruling of a court in criminal procedure, a prosecutor's ruling or under separate regulations.

Attachment 3: Article 178 and 180 of Code of Criminal Procedure

Article 178. The following persons may not be examined in the capacity of witnesses:

1) defence counsel on facts communicated to him while he was giving legal advice or conducting the case, or
2) a priest on facts communicated to him in confession.

Article 180
§ 1. Persons obligated to preserve an official secret, or secrets connected with their profession or office may refuse to testify as to the facts to which this obligation extends, unless they have been released by the court or the state prosecutor from the obligation to preserve such a secret.

§ 2. Persons obligated to preserve secrets such as lawyers, physicians or journalists, may be examined as to the facts covered by these secrets, only when it is necessary for the benefit of the administration of justice, and the facts cannot be established on the basis of other evidence. The court shall decide on examination or permission for examination. This order of the court shall be subject to interlocutory appeal.

§ 3. Releasing a journalist from the obligation to preserve a secret may not permit data to be released, enabling identification of the author of press enunciation, letter to the editor or other material of the same nature, as well as identification of persons imparting information published or passed to be published, if these persons reserved the right to keep the data secret.

§ 4. The provision of § 3 shall not apply, if the information regards the offence referred to in Article 240 § 1 of the Penal Code.

§ 5. The refusal of a journalist to disclose the data referred to in § 3, shall not exempt him from liability for an offence he committed by publishing information.

Attachment 4

Article 19 Act on Police:
1. In case of preliminary investigation carried out by the Police to prevent, detect, establish perpetrators and to obtain and record evidence of the perpetrators prosecuted on indictment, of intentional crime: *[...]* when other means appeared ineffective or there is significant probability of the means being ineffective or useless, the district court, upon a written request of the Police Commander in Chief, submitted after a prior written consent of the general Public Prosecutor or a written request of the Voivodship Police Commander, submitted after prior written consent of the district prosecutor with territorial competence, may, by way of resolution, order operational control.