

## Research Article

# THE LEGAL REGULATION OF SPECIAL MEANS BY THE INTELLIGENCE AGENCY OF THE SLOVAK REPUBLIC WITHIN THE CASE LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS

*Adrián Vaško*<sup>1</sup>

Submitted on 07 Feb 2022 / Revised 11 Apr 2022 / Approved 14 Jun 2022

Published online: 20 Jun 2022

**Summary:** – 1. Introduction. – 2. Intelligence Activity. – 3. Subjects of Intelligence Activity. – 4. Resources in Intelligence Activities. – 5. Selections from the Case Law of the European Court of Human Rights in Relation to Intelligence Services. – 6. Concluding Remarks.

**Keywords:** intelligence agency, intelligence activity, intelligence, special means, privacy protection

## ABSTRACT

**Background:** *The article is focused on the use of special rights or means by the intelligence agency of the Slovak Republic. The use of these statutory means in a democratic society is in the public interest, especially in the context of current security challenges (e.g., international organised crime, terrorism, etc.). At the same time, however, the use of special means by the intelligence agency represents a significant interference with guaranteed fundamental human rights and freedoms, in particular, the right to privacy. In this article, the author examines the*

---

1 Senior Lecturer at the Department of Penal Law, Criminology, Criminalistics and Forensic Sciences, Matej Bel University, Slovakia [adrian.vasko@umb.sk](mailto:adrian.vasko@umb.sk) <https://orcid.org/0000-0002-2113-7909>

**Corresponding author**, solely responsible for writing, conceptualization, data curation, and methodology. Competing interests: No competing interests were disclosed. **Disclaimer:** The author declares that his opinion and views expressed in this article are free of any impact of any organizations.

**Managing editor** – Dr. Olena Terekh. **English Editor** – Dr. Sarah White.

**Copyright:** © 2022 A Vaško. This is an open access article distributed under the terms of the Creative Commons Attribution License, (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

**How to cite:** A Vaško ‘The Legal Regulation of Special Means by the Intelligence Agency of the Slovak Republic within the Case Law of the European Court of Human Rights’ 2022 3(15) Access to Justice in Eastern Europe 1-17. DOI: <https://doi.org/10.33327/AJEE-18-5.3-a000309>

**Published online:** 20 Jun 2022 (<https://doi.org/10.33327/AJEE-18-5.3-a000309>)

admissibility of the use of special intelligence tools in the context of the case law of the European Court of Human Rights and presents de lege ferenda recommendations for the regulation of the relevant legislation governing the activities of the intelligence agency of the Slovak Republic.

**Methods:** The scientific methods: legal comparison, content analysis of websites, functional analysis of legal acts, and analysis of the ECtHR decisions were used to process the research data.

**Results and Conclusions:** In the article, the author provides an overview of the current legal regulation on the use of special means by the intelligence services of the Slovak Republic, which he assesses from the point of view of compliance with the case law of the European Court of Human Rights. After a critical evaluation, the author states that the legal regulation is likely to require an amendment in the short term to ensure compliance with Art. 8 of the Convention: the right to respect for private and family life. Then, in the case of a complaint by a Slovak citizen regarding interference with the right to privacy using special means by the intelligence agencies of the Slovak Republic, it can be said that there was a violation of this right.

## 1 INTRODUCTION

In the 21<sup>st</sup> century, as in the past, intelligence agencies are an important part of the apparatus of individual states. The validity of the existence and operation of intelligence agencies is not generally doubted. Current security challenges at the global level, such as international and transnational crimes, require the use of intelligence in preventing, restraining, and detecting those crimes. Intelligence agencies are generally entitled to use means, methods, and forms of intelligence activities. In the conditions of the Slovak Republic, these are called special means.<sup>2</sup>

The use of special means is necessary from the point of view of the protection of fundamental human rights and freedoms, protection of the constitutional order, internal order, state security, and protection of the state's foreign policy and economic interests in a democratic society. At the same time, intelligence agencies are also focusing on organised crime, terrorism, extremism, cybersecurity, and illegal international passenger transport and migration. In this context, the results of intelligence activities – intelligence information in compliance with the established legal limits – can also be used in criminal proceedings. If the criteria are met, the selected intelligence information can be accepted in criminal proceedings as evidence.<sup>3</sup> The use of special means also constitutes an interference with the right to respect for private and family life, guaranteed, *inter alia*, by the Convention for the Protection of Human Rights and Fundamental Freedoms.<sup>4</sup>

The European Court of Human Rights (hereafter, the ECtHR), based in Strasbourg, has already affected the field of intelligence agencies in its case law. We believe that it is useful to consider the legal regulation of special means of the intelligence agencies of the Slovak Republic from this point of view as well. In many ways, such an assessment can be inspiring for the future.

2 Act no. 46/1993 Coll. on the Slovak Information Service, as amended <<https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/46/20160101>> accessed 22 January 2022; Act no. 198/1994 Coll. on Military Intelligence, as amended <<https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1994/198/20180401>> accessed 22 January 2022.

3 A Vaško, 'Možnosti využitia spravodajských informácií v trestnom konaní' in *Bratislavské právnické fórum 2019: zákonnosť a prípustnosť dôkazov v trestnom konaní: zborník príspevkov z medzinárodnej vedeckej konferencie, Bratislava, 14. - 15. februára 2019* (Bratislava, Univerzita Komenského v Bratislave 2019) 88-99.

4 Convention on the Protection of Human Rights and Fundamental Freedoms <[https://www.echr.coe.int/documents/convention\\_eng.pdf](https://www.echr.coe.int/documents/convention_eng.pdf)> accessed 22 January 2022.

## 2 INTELLIGENCE ACTIVITY

In the Slovak legal order (as well as the Czech one), the characteristics of intelligence activity are not explicitly or declaratively defined. The characteristics of intelligence activity can be determined by an analogous interpretation of the provisions of legal norms, in accordance with which it can be purposefully implemented. Thus, it can be stated that for the purposes of examining and evaluating intelligence activity, it is appropriate to assess it pragmatically. From our point of view, although we respect the need for the theoretical knowledge we present, we refer to the system of intelligence activities as a system of secret, targeted processes implemented by competent state administration bodies when collecting, sorting, keeping, analytically processing, sharing, and interpreting relevant information in relation to the identified needs of the designated entities.<sup>5</sup>

Intelligence activity is primarily support (especially information) provided by its implementers (members and employees of intelligence agencies) to competent addressees.<sup>6</sup> These addressees need it for the active implementation of processes and operations and for setting priorities in ensuring the functionality of certain social positions, especially in securing tasks in the field of protection and defence of state sovereignty, democracy, freedom, and justice. This is mainly because the decisive precondition for the existence of every state, its political stability, economic prosperity, and peaceful social and cultural development is a rationally built and permanently functioning system of effective defence of its constitutional establishment, sovereignty, territorial integrity, security, internal order, economic and other legitimate interests, rights, and freedoms of all its citizens.

## 3 SUBJECTS OF INTELLIGENCE ACTIVITY

Reliable intelligence agencies are a specific attribute of state sovereignty. Therefore, their close interconnection with the structures of other states can be seen as a limitation of this sovereignty. The conspiratorial nature of the functioning of intelligence agencies and the exclusivity of the professional status of intelligence elites also create limits to the exercise of a transnational interest in the activities of intelligence agencies.<sup>7</sup>

The intelligence protection of the state is provided by special state bodies: intelligence agencies of various purposes, such as foreign intelligence (also referred to as the intelligence service), internal intelligence (incorrectly designated as counter-secret service, correctly designated defensive intelligence or counterintelligence), military intelligence, financial intelligence, criminal intelligence, radio and radio-electronic intelligence, and others according to the specific needs and interests of each state.

An intelligence agency is a government organisation whose main task is to obtain important, up-to-date, and publicly inaccessible information on acute and latent risks and other relevant facts through the use of special means and methods of work capable of endangering or influencing vital or other interests in any way.<sup>8</sup> Thus, it performs the function of a secret

5 M Lisoň, A Vaško, 'Teorie spravodajské činnosti' in V Porada et al (eds) *Bezpečnostní vědy* (Plzeň, Aleš Čeněk s.r.o. 2019) 375 et seq.

6 Ibid.

7 R Laml, 'Národné a nadnárodné z hľadiska spravodajskej činnosti malej krajiny' in *Zborník z medzinárodného sympózia, ktorú zorganizovali Asociácia bývalých spravodajských dôstojníkov spolu s Fakultou práva Paneurópskej vysokej školy dňa 8. 12. 2010 na tému 'Národné versus nadnárodné záujmy v činnosti spravodajských služieb'*. (Bratislava: Eurokódex 2010) 3-9.

8 Lisoň, Vaško (n 5).

information service for the state's decisive sphere. It gathers the information obtained, systematically evaluates this information, and creates an autonomous, often very detailed, knowledge fund and conditions for sharing information. In a democratic state governed by the rule of law, strong control of the intelligence agencies is a necessity and a condition *sine qua non* for political stability and further peaceful democratic development of society.<sup>9</sup>

The intelligence community in the Slovak Republic currently consists of two main components: the Slovak Information Service and Military Intelligence. To a certain extent, a specialised unit of the Police Corps – the Office of Special Activities and Operations of the Presidium of the Police Corps, dealing with, among other things, criminal intelligence – can also be considered a part of the intelligence community. The Slovak Information Service (hereafter referred to as the SIS) was established by Act no. 46/1993 Coll. on the SIS of 21/01/1993. After the division of the Czech and Slovak Federal Republics, it was necessary to build a full-fledged system of security forces in the Slovak Republic.

At its inception, the SIS was defined by law as a state body of the Slovak Republic, performing tasks in matters of protection of the constitutional establishment, internal order, and security of the state to the extent defined by this Act. Its activities are governed by the Constitution, constitutional laws, and other generally binding legal regulations. Act no. 444/2015 Coll., amending the Act no. 300/2005 Coll. on the Criminal Code, as subsequently amended, defined the SIS in more detail with effect from 1 January 2016 as the General Security and Intelligence Service of the Slovak Republic.<sup>10</sup>

The Information Service provides information on criminal activity to the Police and Prosecutor's Office, in particular, on organised crime. It also provides the necessary information to other state authorities if they need it to prevent unconstitutional or otherwise illegal activity.

The information obtained is provided only for the purpose stated in the relevant paragraphs and provided that its provision does not jeopardize the fulfilment of the specific task of the information agency under this Act or the disclosure of the sources and means of the information agency or the disclosure of the identity of its members or persons acting in favour of the information agency. This does not apply if the consequence of not providing the information is demonstrably more serious than the consequence of providing it.

The SIS is entitled to use special means in accordance with the provisions of Section 10 of the SIS Act. In carrying out the tasks stipulated by this Act, the SIS is entitled to use the special means, which are:

- a) Information and operational means
- b) Information and technology means<sup>11</sup>

The SIS is obliged to ensure the protection of special means against disclosure and misuse. In the case of the SIS, according to the Act, the information and operational means are:

- a) Tracking people and things
- b) Legalising documents and legend
- c) Using persons acting in the interest of the information service
- d) Exchange of things
- e) Fake transfer of things

9 M Grach, 'Spravodajské služby by ochrana štátu' in *Literárny týždenník* (Bratislava 1998) 5.

10 Act no. 46/1993 (n 2).

11 Act no. 166/2003 Coll. on the Privacy Protection against Unauthorized Use of Information and Technical Means and on the amendments and supplementation of some laws, as amended < <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2003/166/20160101> > accessed 22 January 2022.

The SIS is to keep records of the use of information and operational resources. Details on the use and registration of information and operational resources shall be adjusted by the Director.<sup>12</sup> The SIS is entitled to use information technology in accordance with the provisions of the Act No. 166/2003 Coll. on the Privacy Protection against Unauthorized Use of Information Technology and on changes and amendments of certain laws (the Act on Protection against Eavesdropping), as subsequently amended.

Military Intelligence (hereafter referred to as MI) was established by Act no. 198/1994 Coll. on MI of 30/06/1994. At its inception, MI was defined by the law as a special service performing tasks of providing intelligence protection of the defence of the Slovak Republic within the competence of the Ministry of Defense of the Slovak Republic to the extent provided by law. MI consisted of two components: Military Defense Intelligence, which acted as a military 'counterintelligence', and Military Intelligence, which acted as a military 'intelligence'. As of 1 January 2013, the organisation of MI was changed by an amendment to the Act, and the services were merged into one within the competence of the Ministry of Defense.

In accordance with the current version of the Act, Military Intelligence is an intelligence service performing the tasks of providing intelligence, defence, and security of the Slovak Republic within the competence of the Ministry of Defense of the Slovak Republic.<sup>13</sup> The Minister of Defense of the Slovak Republic provides the National Council of the Slovak Republic, the President of the Slovak Republic, and the Government of the Slovak Republic with information obtained by Military Intelligence that is important for their decision-making and activities. The Minister will also provide necessary information to other state authorities if needed to prevent any illegal activity. The information obtained is provided only to fulfil the purpose stated in the law. MI is entitled in accordance with the provisions of S. 10 of the MI Act to use special means.

In carrying out the tasks stipulated by this Act, MI is entitled to use the special means, which are:

- a) Information and operational means
- b) Information and technical means<sup>14</sup>

MI is obliged to ensure the protection of special means against disclosure and misuse. In the case of MI, the information and operational means are according to the Act:

- a) Tracking people and things
- b) Legalizing documents
- c) Persons acting on behalf of the MI,
- d) Exchange of things
- e) Fake transfer of things

The procedure for requesting, using, and registering information and operational resources is to be determined by the Director. MI is entitled to use information technology in accordance with the provisions of the Act No.166/2003 Coll. on the Privacy Protection against Unauthorized Use of Information Technology and on changes and amendments of certain laws (the Act on Protection against Eavesdropping), as subsequently amended.

12 Act no. 46/1993 (n 2).

13 Act no. 198/1994 (n 2).

14 Act no. 166/2003 (n 11).

## 4 RESOURCES IN INTELLIGENCE ACTIVITIES

Neither the law nor any other legal norm provides an exhaustive list of all the means and tactical procedures that can be used within intelligence activities when fulfilling tasks of intelligence agencies. The means used in the activities of intelligence agencies represent entities, tools, aids, equipment, or their sets, which can be used to achieve greater efficiency and effectiveness in the performance of specified tasks.

The theory of the activities of intelligence agencies classifies these resources into three groups (respecting the needs of their explanation and design). These are the so-called means of activities of intelligence agencies. The first group includes those of general applicability. These are also used when implementing other types of cognitive activities outside intelligence agencies. Using these means, it is possible, for example, to significantly influence the level of observation (monitoring), the detection of some quantitative properties of identified objects (means used in observing the object of intelligence interest at a greater distance, at night, or when examining micro-properties of objects, consumption, distance), etc.

The second group includes special means that are used in the implementation of intelligence activities. The starting point for their explanation is the common tasks the citizens delegate to the state authorities in the field of protection and defence. In accordance with the fulfilment of the tasks set, these are mainly the following means:

- Special technical (various means of computer technology, connecting and transport means, material-technical equipment, etc.)
- Firearms
- Information systems and records
- Various technical means, equipment and their assemblies, materials, procedures, methods and rules of their use, etc.

The third group consists of means that have been and are being created in accordance with the specific implementation requirements and needs of intelligence activities. In relation to its implementation, these means have a specific character. When using them, intelligence officers are required to respect several limiting factors resulting from:

- Their legal characteristics, in particular, the legal conditions for their use (*regulations, controls*)
- Objectives that can be achieved through their use (*performance*)
- Personnel and economic demands, etc.

In terms of theory, the means of intelligence activity can be classified as:

- Information and technical means (means of intelligence technology)
- Information and tactical means (means of intelligence tactics)
- Information and logistics means (means of intelligence support).

In accordance with and within the scope of the law, members of the intelligence agencies are entitled to use the information and technical means (hereafter referred to as ITM).<sup>15</sup> The basic condition to be successful when using them is that the presumed recognisable phenomenon (action) or condition causing their use still persists. Otherwise, it is possible to obtain information about the consequences of the known phenomenon using these means, thus making any further specific action more difficult.

Intelligence officers use the information and technical means within their intelligence activities for the purpose of obtaining and fixing information about ongoing proceedings

<sup>15</sup> Act no. 166/2003 (n 11).

or the conditions that these proceedings caused. Their efficiency and effectiveness depend on the performance parameters of the technology (technological sources of information).

## 5 SELECTIONS FROM THE CASE LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS IN RELATION TO INTELLIGENCE SERVICES

Intensive invasions of the right to privacy are caused by special means of intelligence. This right is guaranteed in our conditions by the constitutional law (Art. 6(1) of the Constitution of the Slovak Republic).

At present, in the decision-making activity of the ECtHR, it is possible to follow the shift from the principle of maintaining such absolute protection of human rights and freedoms to the need to maintain the protection of the public interest.

The criteria on the basis of which these guarantees can be assessed vary from case to case and are relative. The following evaluation criteria can be taken into account:

- The nature, extent, and duration of the means of secret surveillance
- The legal basis for the authorisation to use the means of secret surveillance
- The type of public authority that is authorised to approve the use of such a device and the control of the use of such a device
- The form of the remedies available to review the decision granting the given remedy.<sup>16</sup>

In the past, the ECtHR has dealt mainly with issues related to the course of justice and the right to privacy in this context.

The decision of the ECtHR in the case of *Szabó and Vissy v. Hungary*, App. No. 37138/14, Judgment of 12 January 2016, can be considered one of the ground-breaking decisions in relation to the activities of intelligence services.<sup>17</sup>

In the context of Art. 8 of the European Convention on Human Rights (hereafter referred to as the Convention), the ECtHR dealt with the safeguards against arbitrariness and abuse contained in the Hungarian legislation allowing covert surveillance. The Court took the opportunity to extend the general principles previously formulated in the context of criminal proceedings to the legal framework for the use of surveillance means for intelligence purposes. The ruling is particularly interesting as it provides a critical mirror for the domestic legal regulation of using intelligence technology to track individuals.<sup>18</sup>

The complaint was filed by two employees of an NGO criticizing government policy. Under Hungarian law, the fight against international terrorism has been entrusted to the police. In order to carry out these tasks properly, a special counter-terrorism unit was set up in 2011. The law granted extensive powers to this unit, including the conduct of secret house searches, wiretapping, detention, and opening of transported consignments, as well as monitoring the content of electronic correspondence. The use of these means was subject to prior authorisation. The law distinguished between two permitting regimes. The stricter regime,

16 M Tittlová, 'Teoretické a praktické problémy odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní' in J Záhora (ed), *Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní* (Praha, Leges 2017) 288.

17 *Szabó and Vissy v Hungary*, App no 37138/14 <<http://hudoc.echr.coe.int/eng?i=001-160020>> accessed 22 January 2022.

18 V Pysk, 'Z aktuální judikatury Evropského soudu pro lidská práva – ochrana utajovaných informací' in *Správní právo*, Legislativní příloha č. II, ročník X (Praha, Ministerstvo vnitra České republiky 2018) XLII- XLIX.

where only a court could issue a permit, concerned the use of these means to investigate criminal offence categories defined by law. Conversely, their use for the proper performance of intelligence tasks in the interest of the protection of national security was subject only to a permit authorised by the Minister of Justice.

The applicants thought that they might have been subject to surveillance under the auspices of intelligence operations when they criticised the actions of government officials in fulfilling their work duties. As they had no other remedy, they sought protection through a constitutional complaint. In their submission, they argued that the legal regulation of the applicability of covert surveillance means did not provide sufficient guarantees capable of excluding arbitrariness in the activities of the relevant police department. The Constitutional Court rejected the applicants' allegations, stating that secret surveillance carried out for intelligence purposes was subject to external parliamentary scrutiny, in which the relevant Committee of members of the legislature ensured that the rights of the persons concerned were not violated. The government argued that the complaint was incompatible *ratione personae* with the provisions of the Convention and its Protocols, considering that the applicants could not be considered victims of the alleged violation within the meaning of Art. 34 of the Convention. The Court held the opposite view. In the beginning, the Court recalled that an individual may, in certain circumstances, be the victim of a violation of the Convention because of the simple existence of a law allowing covert surveillance without having to prove that the measure was actually applied to them.<sup>19</sup>

In a relatively recent judgment,<sup>20</sup> the Grand Chamber of the ECtHR further specified the criteria by which it is necessary to assess in the future whether a person can be considered a potential victim of covert surveillance. The Grand Chamber first clarified that the status of victim cannot be invoked by everyone, but only by those who have an increased likelihood of being subject to surveillance. Reasonable suspicion depends on the scope of applicability of the relevant legal provisions, i.e., whether the surveillance tools can only be used in relation to a certain group of persons or whether anyone can be subject to them. In the first case, only an individual belonging to the target group of persons can be considered a victim. However, this is not the case when the legislation allows almost anyone to be subject to covert surveillance. The second criterion to be taken into account is the existence and effectiveness of the remedies available at a national level.

The Hungarian legislation stated that almost anyone could fall victim to covert surveillance. In addition, it did not provide any procedural institute through which the alleged victims could turn to an independent body endowed with the power to deal with their objection of unlawful surveillance. In the light of these features of the legislation, the Court concluded that the applicants could legitimately feel that the measures in question might have been directed against them and must therefore be regarded as potential victims of the alleged violation of the Convention. The court of First Instance thus rejected the government's objection and declared the complaint admissible.

As to the merits of the complaint, the Court acknowledged that the means of covert surveillance to which the applicants could have been subject under the relevant legislation were undoubtedly capable of interfering with their right to respect for privacy, home, and correspondence. Any interference with those rights is permissible within Art. 8 of the Convention only if it has been established by law, pursued one of the legitimate objectives set out in the second paragraph of that provision, and provided that it was necessary to

19 *Klass and others v Germany*, App no 5029/71, Judgment of 6 September 1978 <[https://www.stradalex.com/en/sl\\_src\\_publ\\_jur\\_int/document/echr\\_5029-71](https://www.stradalex.com/en/sl_src_publ_jur_int/document/echr_5029-71)> accessed 22 January 2022.

20 *R Zakharov v Russia*, App no 47143/06, Judgment of the Grand Chamber of 4 December 2015 <<https://policehumanrightsresources.org/roman-zakharov-v-russia-47143-06>> accessed 22 January 2022.





thus expressed concern that the legislation could have been deliberately set up to allow for widespread and strategic monitoring of the population.

The Court also saw insufficient safeguards against arbitrariness in the regime of authorising the use of intelligence technology by the Minister of Justice. In order for the consent to be granted, it was sufficient that the request was based on grounds in favour of the need to use those means. The Court, however, deemed that covert surveillance must be subject to the so-called 'strict necessity' of the intervention. Therefore, it must not be possible to achieve the objective pursued by other, less invasive means, given the fundamental rights of the persons concerned. In any event, it is not sufficient to simply state the reasons without providing the Minister with the evidence to give a specific suspicion that the individual in question may have been involved in terrorist activities. Otherwise, the Minister would not be able to carry out an appropriate adequacy test and assess whether the need to interfere with the rights of the person in question, given the circumstances of the case, is strictly necessary.

The fact that the consent to the covert surveillance was issued by the Minister of Justice did not escape the Court's objections. According to the Court, although it is possible for a permit to be issued by a body other than a judicial authority, in any event, it has to be a body sufficiently independent of the executive power, and a member of the government is definitely not independent.<sup>24</sup>

In an area that is as prone to political abuse as covert surveillance, effective decision-making should, in principle, be exercised – at least in the final instance – by an independent judiciary. This does not necessarily mean that there must be an *ex ante* judicial review, as the same purpose can be achieved by a subsequent judicial review, which can provide additional redress for illegal surveillance.<sup>25</sup> In many situations, typically in the face of current terrorist threats, the issuance of the prior authorisation will often not be appropriate, as this could lead to undesirable delays leading to loss of life.<sup>26</sup> However, subsequent judicial review is an absolute necessity if there is no loss of public confidence.

The Court further described the legislation on the maximum permissible duration of these measures as vague and arbitrary. Although it explicitly set a limit of 90 days with the possibility of extension, it left open whether the duration of the monitoring could be extended only once or repeatedly.

Finally, the Court also considered the remedies available to the persons concerned. The Court emphasised that the question of the effectiveness of any remedy was inextricably linked to the need for the individuals concerned to learn in addition that they had been under surveillance. The requirement of such *ex post* notification means that as soon as the reasons the surveillance was ordered for have ceased to exist and the person concerned can be notified, without jeopardising the purpose of the monitoring, they should be notified so that they are free to decide whether to request a review of the legality of a measure which infringed its fundamental rights and freedoms.

In the absence of a notification mechanism, the Court did not consider the other remedies referred to by the Hungarian government to be effective (e.g., a complaint to the Minister of the Interior). In addition, the Court explicitly denied that the Security Committee of the Parliament could provide sufficient redress. The Minister of Justice was obliged to submit a

<sup>24</sup> *R Zakharov v Russia* (n 20).

<sup>25</sup> *Kennedy v The United Kingdom*, App no 26839/05, Judgment of 15 May 2010 <[https://www.stradalex.com/en/sl\\_src\\_publ\\_jur\\_int/document/echr\\_26839-05](https://www.stradalex.com/en/sl_src_publ_jur_int/document/echr_26839-05)> accessed 22 January 2022.

<sup>26</sup> *Telegraaf Media Nederland Landelijke Media BV and others v The Netherlands*, App no 39315/06, Judgment of 22 November 2012 <[https://www.stradalex.com/nl/sl\\_src\\_publ\\_jur\\_int/document/echr\\_39315-06\\_001-99089](https://www.stradalex.com/nl/sl_src_publ_jur_int/document/echr_39315-06_001-99089)> accessed 22 January 2022.

report on the activities of the intelligence services to this Committee twice a year. However, the report was inaccessible to the public and thus did not provide the necessary degree of transparency and public scrutiny. However, beyond the content of this report, the Committee was not entitled to request any additional information. The Committee was also not able to deal in detail and provide redress in specific cases because they did not have access to individual files. In the light of these findings, the Court did not hesitate to conclude that the national legal framework allowing for the comprehensive surveillance of persons did not provide sufficient guarantees capable of precluding arbitrary interference with the rights of the persons concerned, not excluding the applicant. T a violation of Art. 8 of the Convention.

The present judgment is another of the Court's many contributions to the issue of covert surveillance. The Court does not, in principle, distinguish between the various methods of such monitoring. These general principles therefore apply, whether by telephone or<sup>27</sup> spatial interception,<sup>28</sup> interference with letter freedoms or electronic correspondence,<sup>29</sup> or even GPS tracking.<sup>30</sup> Until recently, the Court dealt with covert surveillance of persons, usually in the context of criminal investigations by law enforcement authorities. However, the present judgment is significant since the Court extends the scope of that case law to intelligence surveillance for intelligence purposes.<sup>31</sup> Its standards can therefore critically compare the relevant provisions of Slovak law governing the activities of intelligence services,<sup>32</sup> especially the legislation concerning the use of intelligence technology.<sup>33</sup>

Another important judgment of the ECtHR in relation to intelligence activities is the Judgment of 4 December 2015 in App. No. 47143/06 – *Roman Zakharov v. Russia*.<sup>34</sup> In that decision, the ECtHR states, *inter alia*, that supervision and control of means of covert surveillance of persons come into consideration in three stages:

- a) At the time of their authorisation
- b) In their implementation
- c) After their deployment has been completed

In the first two cases, the examination of the nature of the case will take place without the knowledge of the persons concerned and must therefore be set up in such a way as to exclude any risk of abuse and arbitrariness. It is therefore desirable, in principle, that the judiciary is trusted, providing the best guarantee of independence, impartiality, and due process. As regards the follow-up, its effectiveness is necessarily conditional on the persons concerned subsequently becoming aware that they were the subjects of covert surveillance. Only then can they consider having the legality of the regulation or the implementation of these measures assessed by an independent court.

*Scope of Covert Surveillance.* The Court reiterated that national law must set clear limits on the applicability of these measures in order to make clear to the persons concerned the circumstances in which public authorities may have recourse to them. To that end, the nature of the offences for which covert surveillance may be authorised must be clearly

27 *Lambert v France*, App no 23618/94, Judgment of 24 August 1998 <[https://www.stradalex.com/en/sl\\_src\\_publ\\_jur\\_int/document/cedh\\_23618-94\\_001-47619](https://www.stradalex.com/en/sl_src_publ_jur_int/document/cedh_23618-94_001-47619)> accessed 22 January 2022.

28 *Savovi v Bulgaria*, App no 7222/05, Judgment of 27 November 2012 <[https://www.stradalex.com/fr/sl\\_src\\_publ\\_jur\\_int/document/echr\\_7222-05](https://www.stradalex.com/fr/sl_src_publ_jur_int/document/echr_7222-05)> accessed 22 January 2022.

29 *Copland v The United Kingdom*, App no 62617/00, Judgment of 3 April 2007 <<https://www.5rb.com/wp-content/uploads/2013/10/Copland-v-UK-ECHR-3-Apr-2007.pdf>> accessed 22 January 2022.

30 *Uzun v Germany*, App no 35623/05, Judgment of 2 September 2010 <[https://www.legislationline.org/download/id/7570/file/ECHR\\_case\\_Uzun\\_v\\_Germany\\_2010\\_en.pdf](https://www.legislationline.org/download/id/7570/file/ECHR_case_Uzun_v_Germany_2010_en.pdf)> accessed 22 January 2022.

31 *R Zakharov v Russia* (n 20).

32 Act no. 46/1993 (n 2).

33 V Pysk V (n 18).

34 *R Zakharov v Russia* (n 20).

defined, as must the range of persons whose telephone calls may be intercepted. However, the requirement of predictability does not necessarily require that the law contain an exhaustive list of the offences that may be grounds for ordering interception in the interests of national security. It is sufficient for their scope to be defined by the characteristics of socially harmful conduct.

The legislation under consideration allowed the use of covert surveillance means in the case of moderate, serious, and particularly serious criminal offences, i.e., those for which the maximum penalty was set at a minimum of three years. The Court considered such an arrangement to be sufficiently clear and definite. However, the Court was concerned that there was a significant number of other factors, including less serious forms of crime, such as pickpocketing. In addition, the legislation allowed the interception of not only suspects or accused persons but also other persons who may have information about the crime or other relevant information without further clarifying these concepts. Similarly, these measures were applicable following the receipt of the information on events or activities that threaten Russia's national, military, economic, or environmental security. However, even these concepts did not elaborate on the legal regulations, which left the executive body with an essentially unlimited power to expose the person concerned to the risk of arbitrariness. On the contrary, the Court recognised that this wide discretion in the interpretation of central concepts may be limited if prior judicial authorisation is required for the application of those measures. Independent *ex ante* judicial review is a key safeguard against arbitrary interference with the rights of data subjects.

*Enabling Eavesdropping.* The Court gradually examined the nature of the body that could authorise the monitoring, the scope of its review of powers, and the content of the authorisation issued by the body. According to the Court, the authorising body may also be an entity other than the court if it is sufficiently independent of the executive power.<sup>35</sup> The Russian legislation contains an important safeguard against arbitrariness in conducting wiretaps, as it requires that the interception of any communication be first authorized by the court.

The case law implies a requirement for the scope of the review powers of the Court. The licensing authority must be able to verify the existence of a reasonable suspicion of the person concerned and, thus, whether there are any circumstances justifying the suspicion that the person is committing any act based on which the eavesdropping may be ordered. In addition, it must be able to assess whether permission for eavesdropping is necessary in a democratic society, i.e., proportionate, to achieve the objective pursued, including whether the objective pursued cannot be achieved by other means which are less invasive in terms of the rights concerned.<sup>36</sup> The scope of judicial review was considered by the Court to be quite limited in this case, as judges are not in practice provided with all relevant information to assess whether there is sufficient factual evidence in a particular case to justify the suspicion that the person concerned is involved in activities for which the intervention in their communication may be allowed. In particular, the courts do not have access to information on secret agents, police informants, or the organisation and tactics of how the investigative procedures are used. The legislation does not require judges to examine the existence of a 'reasonable suspicion' against the person concerned, but the judges do not even apply a proportionality test. In practice, requests for a wiretapping permit are not usually accompanied by any background material, and the judges do not require such material.

35 *Dumitru Popescu v Romania* (No 2), App no 71525/01, Judgment of 26 April 2007 <<https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-80352%22%5D%7D>> accessed 22 January 2022.

36 *Association for European Integration and Human Rights and Ekimdzchiev v Bulgaria*, App no 62540/00, Judgment of 28 June 2007 <<https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-81323%22%5D%7D>> accessed 22 January 2022.

*Interception Notices and Remedies Available.* The Court recalled that the requirement that the individuals concerned subsequently find out that they were subject to surveillance is closely linked to the question of the effectiveness of the remedies. The Court is aware that practically, it is not always possible to inform an individual that their communication was eavesdropped upon, as this could jeopardise the long-term purpose of the surveillance. Therefore, even failure to notify such individuals of this fact cannot itself lead to the conclusion that such intervention was not necessary in a democratic society. However, as soon as the purpose of the surveillance cannot be interfered with, the persons concerned must be informed that they were subjected to such interception.<sup>37</sup>

The Court had previously declared the absence of such a mechanism incompatible with Art. 8 of the Convention, finding that it deprived the persons concerned of any effective possibility of seeking compensation for unlawful interference with their rights.<sup>38</sup> The Court took the opposite view, as, under the legislation, anyone who thought they might have been monitored could request an independent authority to review such circumstances.

Russian legislation does not require that the persons concerned be subsequently informed of the monitoring that was carried out. Thus, they have almost no opportunity to find out that their communication was intercepted unless it is used against them as evidence of guilt in subsequent criminal proceedings. Although persons who have learned in some way that they were watched may, by law, request information on the data thus obtained, such a request is subject to the condition that the person must be able to prove that means of covert surveillance have been deployed against them. Even if they bear the burden of proof, the legislation does not allow the persons concerned to become acquainted with classified information, including information on the means and procedures used in the surveillance, the identity of the persons who carried out the surveillance, and the findings. The Court thus concluded that the possibility for the persons concerned to obtain information on the monitoring carried out was ineffective in practice.<sup>39</sup>

In seeking a fair balance between the interests of the state in the protection of national security and the interests of the individuals concerned whose rights were affected, the state enjoys a degree of discretion. However, it is subject to European supervision by the Court, which must verify that the national legislation provided sufficient and effective safeguards against abuse. Although the covert surveillance system is designed to protect national security, it carries the risk of undermining or even destroying the democracy it is supposed to defend. The court must therefore verify whether the national mechanism for supervising the decision and carrying out covert surveillance is capable of maintaining interference with the rights of individuals only to the extent necessary in a democratic society.<sup>40</sup>

Finally, the Court recalled that the requirement of predictability of legislation has different content in the context of covert surveillance as in other areas. Naturally, the law cannot be defined in such a way that the individual realises under what circumstances they are likely to be intercepted and can thus adjust their actions. However, since the executive power is exercised in a secret manner in these cases, the risk of abuse is obvious. It is therefore essential that the law contains clear and detailed rules for covert surveillance. The law must be clear enough to provide individuals with adequate guidance as to the circumstances and conditions under which the competent authorities are entitled to take such a measure.<sup>41</sup>

37 *Weber and Saravia v Germany*, App no 54934/00 <<https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-76586%22%5D%7D>> accessed 22 January 2022.

38 *Dumitru Popescu v Romania* (n 35).

39 *R Zakharov v Russia* (n 20).

40 *Ibid.*

41 *Ibid.*

In the light of these facts, the Court concluded that the Russian legislation did not provide sufficient and effective safeguards against the arbitrariness and risk of abuse inherent in any covert surveillance system, especially when the police and intelligence services have direct access to all mobile communications using various technical equipment. Finally, the applicant provided the Court with examples showing that arbitrary interference with rights often occurred in practice. The legislation under assessment thus did not meet the requirements of the quality of the legal framework and was not able to limit interference to what is necessary in a democratic society. The Court thus concluded that there had been a violation of Art. 8 of the Convention.

## 6 CONCLUDING REMARKS

Taking into account what we have mentioned above, we believe that the current legislation on the use of special means by the intelligence agencies of the Slovak Republic can be assessed critically. The use of information and technical means by intelligence agencies in the Slovak Republic is governed by a separate legal regulation,<sup>42</sup> and therefore we will not deal in this paper with the compliance of its provisions with the case law of the ECtHR. We will focus our attention on information and operational means, with the exception of legalisation documents and legends. These are supportive in nature, and their use does not itself constitute an interference with fundamental human rights and freedoms.

From the point of view of the case law of the ECtHR, it seems the most problematic regulation on the monitoring of persons and things consists of issues related to the process of authorising the use of such means (in the case of the SIS, the Director), as well as issues of *ex post* notification of the use of such means against a person unless there are national security grounds for not doing so. However, even in these cases, there should be a mechanism to examine the justification of the interference with human rights and freedoms by the state authority.

The current legal regulation of using a mock transfer of things or controlled supply by intelligence agencies was introduced into intelligence laws by Act no. 444/2015 Coll., as subsequently amended, changing and amending the Act no. 300/2005 Coll. on the Criminal Code, amending certain laws (the so-called anti-terrorist package). Specifically, this is S. 11(1d) Exchange of things and letter e) fictitious transfer of property in Act no. 46/1993 Coll. on the Slovak Information Service (similarly in the Military Intelligence Act).

A condition is set for the lawful use of these information and operational resources based on the prior written consent of the judge of the court competent according to a special regulation (*ex ante*). This special regulation means the provision of S. 4a of the Act no. 166/2003 Coll. on the Protection of Privacy against Unauthorized Use of Information Technology and on changes and amendments of certain laws (the Eavesdropping Protection Act), as subsequently amended. The process of authorising the use of these means is, in our view, in line with the requirements set out in the case law of the ECtHR. The absence of a notification mechanism, or any other means, similar to tracking people and things, may be a problem.

Information-operational means – persons acting in favour of the intelligence service – in our opinion, do not represent a fundamental problem from the point of view of the case law of the ECtHR. In certain cases, the use of information obtained in criminal proceedings would involve a procedure under the applicable law. The process of obtaining intelligence

<sup>42</sup> Act no. 166/2003 (n 11).

is classified, and, as a rule, its result – intelligence – is usually classified. Pursuant to the provisions of S. 10(2) of the Act no. 46/1993 Coll., the Slovak Information Service is obliged to ensure the protection of special means against disclosure and misuse (a similar provision is contained in the Military Intelligence Act).

In order to ensure the right to an effective defence, it is possible to find a solution in the Act no. 215/2004 Coll. on the Classified Information Protection and on changes and amendments to certain acts, the Institute of Another Authorized Person (S. 35(2)). For persons acting in favour of the information agency, we again refer to S. 23(2) of the Act no. 46/1993 Coll. on the Slovak Information Service, according to which the Director of the Slovak Information Service (and, by analogy, the Director of the Military Intelligence) may decide on the waiver of confidentiality. The Criminal Procedure Code also contains provisions on a witness whose identity is confidential, which, in our opinion, are also applicable to members and persons acting in favour of the intelligence agency after meeting the legal conditions.

Of course, the activities of persons acting in favour of intelligence services must comply with the requirements of the case law of the ECtHR in the context of the regulation of the use of a 'provocateur' agent. The agent's conduct must meet certain standards so that it does not deviate from the limits of legality. Clear limitations and guarantees distinguish the permissible procedure from guiding or provoking the commission of a criminal offence, which is in conflict with Art. 6 of the Convention. The public interest cannot justify the use of evidence obtained by provocation, so criminal proceedings would not be fair from the outset.<sup>43</sup> The ECtHR stated in its decision-making process that the use of special investigative methods does not itself lead to a violation of the right to a fair trial.<sup>44</sup>

In conclusion, we quote the provision of the Art. 8 of the Convention on the right to respect for private and family life:

- 1) Everyone has the right to respect for his private and family life, his home and his correspondence.
- 2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

## REFERENCES

1. Act no. 46/1993 Coll. on the Slovak Information Service, as amended <<https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/46/20160101>> accessed 22 January 2022; Act no. 198/1994 Coll. on Military Intelligence, as amended <<https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1994/198/20180401>> accessed 22 January 2022.
2. Vaško A, 'Možnosti využitia spravodajských informácií v trestnom konaní' in *Bratislavské právnické fórum 2019: zákonnosť a prípustnosť dôkazov v trestnom konaní: zborník príspevkov z medzinárodnej vedeckej konferencie, Bratislava, 14. - 15. februára 2019* (Bratislava, Univerzita Komenského v Bratislave 2019) 88-99.

43 *Teixeira de Castro v Portugal*, App no 25829/94, 9 June 1998 <<https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-58193%22%5D%7D>> accessed 22 January 2022.

44 *Ramanauskas v Lithuania*, App no 74420/01, 5 February 2008 <<https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-84866%22%5D%7D>> accessed 22 January 2022.

3. Convention on the Protection of Human Rights and Fundamental Freedoms <[https://www.echr.coe.int/documents/convention\\_eng.pdf](https://www.echr.coe.int/documents/convention_eng.pdf)> accessed 22 January 2022.
4. Lisoň M, Vaško A, 'Teorie zpravodajské činnosti' in V Porada et al (eds) *Bezpečnostní vědy* (Plzeň, Aleš Čeněk s.r.o. 2019) 375 et seq.
5. Laml R, 'Národné a nadnárodné z hľadiska spravodajskej činnosti malej krajiny' in *Zborník z medzinárodného sympózia, ktorú zorganizovali Asociácia bývalých spravodajských dôstojníkov spolu s Fakultou práva Paneurópskej vysokej školy dňa 8. 12. 2010 na tému 'Národné versus nadnárodné záujmy v činnosti spravodajských služieb'*. (Bratislava: Eurokódex 2010) 3-9.
6. Grach M, 'Spravodajské služby a ochrana štátu' in *Literárny týždenník* (Bratislava 1998) 5.
7. Act no. 166/2003 Coll. on the Privacy Protection against Unauthorized Use of Information and Technical Means and on the amendments and supplementation of some laws, as amended < <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2003/166/20160101>> accessed 22 January 2022.
8. Tittlová M, 'Teoretické a praktické problémy odpočúvania a záznamu telekomunikačnej prevádzky v trestnom konaní' in J Záhora (ed), *Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní* (Praha, Leges 2017) 288.
9. *Szabó and Vissy v Hungary*, App no 37138/14 <<http://hudoc.echr.coe.int/eng?i=001-160020>> accessed 22 January 2022.
10. Pysk V, 'Z aktuální judikatury Evropského soudu pro lidská práva – ochrana utajovaných informací' in *Správní právo*, Legislativní příloha č. II, ročník X (Praha, Ministerstvo vnitra České republiky 2018) XLII- XLIX.
11. *Klass and others v Germany*, App no 5029/71, Judgment of 6 September 1978 <[https://www.stradalex.com/en/sl\\_src\\_publ\\_jur\\_int/document/echr\\_5029-71](https://www.stradalex.com/en/sl_src_publ_jur_int/document/echr_5029-71)> accessed 22 January 2022.
12. *R Zakharov v Russia*, App no 47143/06, Judgment of the Grand Chamber of 4 December 2015 <<https://policehumanrightsresources.org/roman-zakharov-v-russia-47143-06>> accessed 22 January 2022.
13. *Amann v Switzerland*, App no 27798/95, Judgment of the Grand Chamber of 16 February 2000 <[https://hudoc.echr.coe.int/fre#{%22fulltext%22:\[%22Amann%20v.%20Switzerland%22\],%22documentcollectionid%22:\[%22GRANDCHAMBER%22,%22CHAMBER%22\],%22itemid%22:\[%22001-58497%22\]}](https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22Amann%20v.%20Switzerland%22],%22documentcollectionid%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58497%22]})> accessed 22 January 2022.
14. *Kennedy v The United Kingdom*, App no 26839/05, Judgment of 15 May 2010 <[https://www.stradalex.com/en/sl\\_src\\_publ\\_jur\\_int/document/echr\\_26839-05](https://www.stradalex.com/en/sl_src_publ_jur_int/document/echr_26839-05)> accessed 22 January 2022.
15. *Telegraaf Media Nederland Landelijke Media BV and others v The Netherlands*, App no 39315/06, Judgment of 22 November 2012 <[https://www.stradalex.com/nl/sl\\_src\\_publ\\_jur\\_int/document/echr\\_39315-06\\_001-99089](https://www.stradalex.com/nl/sl_src_publ_jur_int/document/echr_39315-06_001-99089)> accessed 22 January 2022.
16. *Lambert v France*, App no 23618/94, Judgment of 24 August 1998 <[https://www.stradalex.com/en/sl\\_src\\_publ\\_jur\\_int/document/cedh\\_23618-94\\_001-47619](https://www.stradalex.com/en/sl_src_publ_jur_int/document/cedh_23618-94_001-47619)> accessed 22 January 2022.
17. *Savovi v Bulgaria*, App no 7222/05, Judgment of 27 November 2012 <[https://www.stradalex.com/fr/sl\\_src\\_publ\\_jur\\_int/document/echr\\_7222-05](https://www.stradalex.com/fr/sl_src_publ_jur_int/document/echr_7222-05)> accessed 22 January 2022.
18. *Copland v The United Kingdom*, App no 62617/00, Judgment of 3 April 2007 <<https://www.5rb.com/wp-content/uploads/2013/10/Copland-v-UK-ECHR-3-Apr-2007.pdf>> accessed 22 January 2022.



19. *Uzun v Germany*, App no 35623/05, Judgment of 2 September 2010 <[https://www.legislationline.org/download/id/7570/file/ECHR\\_case\\_Uzun\\_v\\_Germany\\_2010\\_en.pdf](https://www.legislationline.org/download/id/7570/file/ECHR_case_Uzun_v_Germany_2010_en.pdf)> accessed 22 January 2022.
20. *Dumitru Popescu v Romania* (No 2), App no 71525/01, Judgment of 26 April 2007 <<https://hudoc.echr.coe.int/fre#%22itemid%22:%22001-80352%22>> accessed 22 January 2022.
21. *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, App no 62540/00, Judgment of 28 June 2007 <<https://hudoc.echr.coe.int/eng#%22itemid%22:%22001-81323%22>> accessed 22 January 2022.
22. *Weber and Saravia v Germany*, App no 54934/00 <<https://hudoc.echr.coe.int/eng#%22itemid%22:%22001-76586%22>> accessed 22 January 2022.
23. *Teixeira de Castro v Portugal*, App no 25829/94, 9 June 1998 <<https://hudoc.echr.coe.int/eng#%22itemid%22:%22001-58193%22>> accessed 22 January 2022.
24. *Ramanauskas v Lithuania*, App no 74420/01, 5 February 2008 <<https://hudoc.echr.coe.int/fr#%22itemid%22:%22001-84866%22>> accessed 22 January 2022.