IUS ET ADMINISTRATIO ISSN 2300-4797

NR 2/2024 (55) DOI: 10.15584/iuseta.2024.2.5

JUDr. Jakub Matis

The use of intelligence in criminal proceedings in the conditions of the Slovak Republic

Wykorzystanie danych wywiadowczych w postępowaniu karnym w warunkach Republiki Słowackiej

Abstract

The presented article deals with the activities of intelligence services, the concept of their functioning in the present in comparison with the past functioning. The object of the examination will be the legality of the use of intelligence information as evidence in criminal proceedings in the Slovak Republic. The core part of the article focuses on the applicability of intelligence information in the context of evidence in criminal proceedings. As these are institutes that go beyond the limits of the Slovak Criminal Procedure Code, special legal regulations will also be analysed in connection with intelligence activities, in particular Act No. 46/1993 Coll. on the Slovak Information Service and Act No. 198/1994 Coll. on Military Intelligence. Last but not least, the aim of the article will be to analyse the use use of information-technical means within the legal limits. In order to achieve the set objectives, we use the method of analysis of the current legislation. In the conclusion of the paper, we evaluate the findings and take our positions and on the application of the analyzed institute.

Keywords: evidence, intelligence, SIS, information-technical means.

Streszczenie

Prezentowany artykuł dotyczy działalności służb wywiadowczych, koncepcji ich funkcjonowania w teraźniejszości w porównaniu z funkcjonowaniem w przeszłości. Przedmiotem badania będzie legalność wykorzystania informacji wywiadowczych jako dowodów w postępowaniu karnym w Republice Słowackiej. Zasadnicza część artykułu koncentruje się na możliwości zastosowania informacji wywiadowczych w kontekście dowodów w postępowaniu karnym. Ponieważ są to instytucje, które wykraczają poza granice słowackiego kodeksu postępowania karnego, przeanalizowane zostaną również specjalne regulacje prawne związane z działalnością wywiadowczą, w szczególności ustawa nr 46/1993 Dz.U. o Słowackiej Służbie Informacyjnej i ustawa nr 198/1994 Dz.U. o wywiadzie wojskowym. Wreszcie, celem artykułu jest analiza wykorzystania środków informacyjno-technicznych w granicach prawa. Aby osiągnąć wyznaczone cele, wykorzystujemy metodę analizy obowiązującego ustawodawstwa. W podsumowaniu opracowania oceniamy wyniki i zajmujemy stanowisko w sprawie zastosowania analizowanego instytutu.

Słowa kluczowe: dowody, wywiad, SIS, środki informacyjno-techniczne.

1. The linking between law enforcement and intelligence agencies

The relationship linking law enforcement and intelligence agencies is driven by the growing crime in terms of its structure and dynamics. In this context, achieving the purpose of criminal proceedings requires cooperation between law enforcement, the courts and the intelligence services.

Intelligence services have specific means and entitlements, the use of which the legislature entrusts to their explicit competence. Law enforcement authorities, courts cooperate with intelligence services in the form of obtaining information relevant to criminal proceedings which law enforcement authorities are incapable of obtaining. In addition, intelligence gathering serves as a tool of protection for the role of criminal law[1].

The so-called Intelligence Legislation does not contain detailed regulation of the intelligence gathering process. The primary law regulating the implementation of intelligence activities is Act No. 46/1993 Coll. on the Slovak Information Service. This legislation explicitly stipulated their tasks and authorisations for the use of specific means. In this way, they obtain information in a lawful manner, which they provide to the necessary extent to the intended addressees.

The earliest use of intelligence was given by its technological nature. By historical interpretation, we may conclude that it was the acquisition of information by classified knowledge. The growing number of objects subject to the control in question was associated with military espionage and the consolidation of the power of certain entities within the state.

First and above all, intelligence information has the character of a supportive means of information, serving the authorised body. This role arises from the need of any rationally built democratic state to ensure political stability, economic prosperity, peaceful social and cultural development, a 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[2].

According to Pili, intelligence agencies are social epistemic institutions, "organisations with the goal of providing knowledge and foreknowledge of an enemy's intentions and behaviour to the decision maker"[3].

---

[1] A. Vaško, S*pravodajská informácia – významný zdroj poznania pre trestné konanie*, Bratislava 2020, https://www.judikaty.info/cz/document/article/6901/ [access: 30.11.2024].

[2] A. Vaško, *Spravodajské informácie v trestnom konaní v slovenskej republike de lege lata* [in:] *Zborník pôvodných vedeckých prác, štúdií a odborných článkov Kriminálne spravodajstvo*, Bratislava 2022, p. 89.

[3] G. Pili, *Intelligence and Social Epistemology – toward a Social Epistemological Theory of Intelligence*, "A Journal of Knowledge, Culture and Policy" 2019, No. 33(6), pp. 574–592.

The legal order of the Slovak Republic does not have a legal definition of the concept of intelligence activities, unlike operational-search activities, which are defined in a number of legal regulations such as the Laws on the Police Force, the Prison and Judicial Guard Corps and the Financial Administration, but not in the Criminal Procedure Code itself. Unlike the Police Force, the intelligence services are not law enforcement authorities and their information is not primarily intended for those bodies or for the courts[4].

Intelligence information is the final product of intelligence activities, which is produced as an output of targeted collection and analysis processes. In the context of crime detection, it serves as a basis for further investigation. Similarly, intelligence information is the result of operational and investigative activities and provides specific knowledge necessary for the effective conduct of criminal proceedings. Both of these pieces of information, unlike raw data, contain evaluated knowledge about the subjects under surveillance (e.g., criminal groups, perpetrators), which allows for the estimation of their capabilities, risks, and intentions. They are purposefully generated for law enforcement authorities, who use them to optimise their investigative activities[5].

Intelligence information, a specific sub-information product of criminal-police cognition, is produced by the use of inductive-deductive logic. It involves a degree of interpretation resulting inevitably in a permissible degree of speculation and risk[6].

2. Evidence and intelligence services

Evidence is an indispensable part of criminal proceedings. Its aim is to objectively and fully establish the state of facts of the case, which is a prerequisite for the issuing of a legally correct and justified decision. Evidence has a fundamental impact on all stages of criminal proceedings and its results directly determine the final decision in a particular case. Evidence can thus be described as a central element of criminal proceedings as a whole[7].

Evidence is taken at every stage of the criminal proceedings. It is indispensable, as it is the only way to enable the law enforcement authorities and the court to obtain the basis for the further course of the proceedings and the decision.

---

[4] A. Vaško, *Možnosti využitia spravodajských informácií v trestnom konaní*, "Zborník z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2019" 2019, p. 90.

[5] B. Pikna, *Nástroje evropského práva v oblasti získávaní důkazů při aplikaci operativně pátracích prostředků* [in:] *Sborník příspěvků z mezinárodního semináře uskutečněného na Policejní akademii ČR dne 2. listopadu 2004*, Praha 2004, p. 99.

[6] A.Vaško, *Možnosti využitia*…, pp. 90–91.

[7] J. Ivor *et al.*, *Trestné právo procesné*, Bratislava 2010, p. 419.

Legal theory divides evidence into specific phases stages:
- search for evidence,
- conducting and documenting the evidence,
- verification
- evaluation.

Evidence in criminal proceedings is regulated in the sixth title of the Code of Criminal Procedure (§§ 119–161). Ivor *et al.*, characterize evidence as the procedure of the law enforcement authorities and the court regulated by law, or other persons, leading to the search, securing, execution and evaluation of knowledge important for the knowledge of the factual circumstances relevant for the decision on guilt and punishment, as well as for the further procedure in the proceedings[8].

The main purpose of the criminal procedure is to regulate the procedure of the law enforcement authorities, i.e. the prosecutor and the police and, on the other hand, the courts, so that criminal offences are identified duly and their perpetrators are justly punished according to the law[9].

The Criminal Procedure Code, in Section 119(2), provides a statutory definition of "evidence" as follows: "Evidence may be anything that can contribute to the proper clarification of the case and which was obtained from the evidence sources according to this Act or a special act". This definition of evidence is based on the principle that only what has been obtained in accordance with the law can be used to prove guilt and impose a penalty. The procedural act by which a law enforcement agency and the court obtain important information to clarify the matter is referred to as a "means of proof". According to Section 119(2) of the Criminal Procedure Code, "Means of proof are in particular the interrogation of the accused, witnesses, and experts, expert opinions, on-site verification of testimony, recognition, reconstruction, investigative experiment, inspection, objects and documents important for the criminal proceedings, notification, information obtained using information technology or means of operational-search activities"[10].

In the process of crime detection, various information products are produced, which are characterised by the specific competence of the entity that obtained them (e.g. intelligence information, operational-search information). Information in this context represents a report that contains new knowledge and reduces the level of uncertainty in the investigation. It is a kind of extension of knowledge about a particular situation which is essential for the successful performance of law enforcement tasks.

[8] J. Ivor *et al*., *Trestné právo procesné 1*, Bratislava 2017, p. 404.

[9] Section 1 of the Code of Criminal Procedure.

[10] Section 119(2) Code of Criminal Procedure.

In this section, we focus on the complex issue of the usability of information obtained under other laws as evidence in criminal proceedings. Specifically, we are interested in whether it is necessary for such legislation to explicitly allow for the use of information so obtained in criminal proceedings.

An analysis of the legal regulation of the activities of the intelligence services in Slovakia, in particular the Act No. 46/1993 Coll. on the Slovak Information Service and Act No. 198/1994 Coll. on Military Intelligence, reveals that the original concept of these services was primarily focused on the collection and analysis of information without direct executive powers. The question arises whether information obtained in the framework of this activity can be directly used as evidence in criminal proceedings.

As an argument supporting the admissibility of intelligence information as evidence in criminal proceedings, the amendment to Act No. 444/2015 Coll., which expanded the scope of intelligence services, can be mentioned. In particular, the provisions of Section 11(1)(d) and (e) of Act No. 46/1993 Coll. on the Slovak Information Service (by analogy also in the Act on Military Intelligence) allow intelligence services to carry out case substitution and disguised case transfer. The introduction of these new powers clearly indicates that the legislator expects the intelligence services to be more actively involved in the detection and proof of criminal activity. It is therefore reasonable to assume that information obtained under these new powers may be used as evidence in subsequent criminal proceedings.

Another argument in favour of the use of intelligence information is the grant of prior judicial consent. In order to be able to lawfully use such information-operating means, the condition of prior written consent of the judge who is competent under a specific regulation must be fulfilled. This special regulation is defined in Art. 4a of Act No. 166/2003 Coll. on the protection of privacy against unauthorised use of information and technical means and on amendment and supplementation of certain acts (Act on protection against eavesdropping), as amended. Considering that the court is involved in the process of obtaining intelligence information, we believe that this information meets the requirements set out in Section 119(2) of the Criminal Procedure Code and may be used as evidence in criminal proceedings.

The grounds for criminal proceedings may come from intelligence information, even if this information is not considered evidence at this stage of the criminal proceedings. Pursuant to Section 196(1) of the Code of Criminal Procedure, law enforcement authorities may initiate a prosecution on the basis of their own findings or information obtained from other agencies, such as the Criminal Police, the Financial Administration or the intelligence services[11].

[11] A.Vaško, *Možnosti využitia…*, pp. 92–93.

3. The issue of legality

The Code of Criminal Procedure mandates that all evidence used in proceedings must be obtained lawfully. This principle of legality ensures that evidence has been acquired in accordance with applicable laws and without infringing upon fundamental rights and freedoms. Evidence obtained unlawfully is considered not only evidence acquired in direct violation of the law but also any evidence derived from such unlawfully obtained evidence. Evidence obtained in violation of the constitutional rights of individuals is explicitly inadmissible as it does not meet the requirements set forth in Section 119(2) of the Code of Criminal Procedure[12].

Legal theory also applies five criteria for evaluating the legality of evidence:

- whether the evidence was obtained from a source prescribed or permitted by law;
- whether the evidence was obtained and performed by a procedural subject authorized by law to do so;
- whether the evidence was obtained and performed at the procedural stage at which the procedural subject is authorized by law to search for and perform evidence in a procedural sense, i.e., such evidence that may serve as a basis for a decision in criminal proceedings, in particular for a court decision;
- whether the obtained and performed evidence relates to the subject matter of the proof in the given proceedings, i.e., whether it relates to the act which is the subject of the proceedings or to questions that must be decided by law in connection with this act;
- whether the evidence was obtained and performed in a manner prescribed or permitted by law[13].

The European Court of Human Rights' case law makes it clear that the Convention for the Protection of Human Rights and Fundamental Freedoms does not directly address the issue of admissibility of evidence in criminal proceedings. This issue is left to the national legislation of each State.

Although the ECHR does not undertake a detailed analysis of the admissibility of individual pieces of evidence, it focuses on the overall conduct of the proceedings. If it finds that the use of certain evidence has led to a violation of the right to a fair trial, it may find a violation of the Convention[14].

"Anything which may contribute to the proper clarification of the matter and which has been obtained from the means of evidence under this Act or under

[12] J. Záhora *et al.*, *Dokazovanie v trestnom konaní*, Praha 2013, p. 29.

[13] B. Repík, *Procesní důsledky porušení předpisů o dokazování v trestním řízení*, "Bulletin advokacie" 1982, p. 122.

[14] B. Mole, C. Harby, *Právo na spravodlivý proces. Sprievodca na aplikáciu čl. 6 európskeho dohovoru o ľudských právach*, Bratislava 2006, p. 49.

a special law may be used as evidence". The provision in question in the next sentence gives an example of what may serve as means of proof. "Means of proof shall include, in particular, questioning of the accused, witnesses, experts, reports and expert statements, on-the-spot verification of statements, reconnaissance, reconstruction, investigative experiment, inspection, objects and documents relevant to criminal proceedings, notification, information obtained by means of information technology or means of operational and search activities"[15].

The current legislation of the Slovak Republic includes a number of specific acts dealing with the issue of the use of information as evidence in criminal proceedings. While some of these laws explicitly regulate the conditions and manner of use of such information, others do not contain such provisions. Despite the absence of an explicit provision in some laws, there is a legal view that information obtained in accordance with these laws may be used as evidence in criminal proceedings under certain conditions. In the context of Section 119(3) of the Code of Criminal Procedure, the following are relevant as special provisions:

- Act No. 166/2003 Coll. on the protection of privacy against unauthorised use
- information-technical means and on amendment and supplementation of certain acts (Act on protection against eavesdropping),
- Act No. 1/2014 Coll. on the organisation of public sporting events and on amendments and supplements to certain acts,
- Act No. 18/2018 Coll. on the Protection of Personal Data and on Amendments and Additions to Certain Acts,
- Act No. 46/1993 Coll. on the Slovak Information Service, as amended,
- Act No. 171/1993 Coll. on the Police Force, as amended,
- Act No. 198/1994 Coll. on Military Intelligence, as amended,
- Act No. 4/2001 Coll. on the Prison and Judicial Guard Corps, as amended,
- Act No. 652/2004 Coll. on State Administration Bodies in Customs and on Amendments and Additions to Certain Acts, respectively Act No. 35/2019 Coll. on Financial Administration and on Amendments and Additions to Certain Acts,
- Act No. 236/2017 Coll. on the European Investigation Order[16].

4. Slovak Information Service

The Slovak Information Service (SIS) was established by Act No. 46/1993 Coll. as a complex intelligence structure covering both domestic and foreign areas.

[15] Section 119(3) of the Code of Criminal Procedure.

[16] A. Vaško, M. Lisoň, *Hrozby a riziká – objekty spravodajského záujmu*, 2020, No. 2.

Due to the specific nature of its tasks, the law allows the SIS to use special investigative methods, including information-technical means (ITM). These means enable the SIS to obtain information in a way that would not otherwise be possible, in order to fulfil its statutory duties[17].

The Slovak legal system contains the definition of the term information--technical means even in two legal regulations. According to the Criminal Procedure Code, Art. 10, paragraph 21, ITM for the purposes of this Act shall be understood as electrotechnical, radio-technical, photo-technical, optical, mechanical, chemical and other technical means and devices or sets thereof used in a classified manner in the interception and recording of traffic in electronic communication networks, visual, audio or video-sound recordings or in the search, opening and examination of parcels, if their use interferes with fundamental human rights and freedoms[18].

The second piece of legislation is the aforementioned Protection from Eavesdropping Act. Section 2 of this Act provides that for the purposes of this Act, ITM, in particular, electrical, radiotechnical, phototechnical, optical, mechanical, chemical and other technical means and equipment or sets thereof used in a classified manner in

- the retrieval, opening, examination and evaluation of mail and other conveyed items,
- obtaining the contents of messages transmitted over electronic communications networks, including the interception of telephone communications,
- making visual, audio, visual-audio or other recordings[19].

It is clear from the analysed provisions of the Act that the legislator, when defining the term "information-technical means", did not put emphasis on its technical parameters, such as its structure or composition. Instead, the focus was on the functionality and the purpose of the use of the means in question. The key criterion for classifying a means in this category is its ability to be used by public authorities to intrude into the privacy and obtain information about individuals.

A condition for the use of information obtained through the use of ITM as evidence in criminal proceedings shall be the making of a written record indicating the place, time and lawfulness of the use of ITM, to which the State authority shall attach the record and a verbatim transcript thereof. The definition of ITM in section 2 of the Act is the result of the aforementioned last amendment effective from

[17] M. Aláč, *Osobitosti použitia ITP v pôsobnosti Slovenskej informačnej služby* [in:] *Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní*, Praha 2017, pp. 268–276.

[18] Section 10(21) of Code of Criminal Procedure.

[19] Section 2 of Act No. 166/2003 Coll. on the protection of privacy against the unauthorised use of information-technical means and on the amendment and supplementation of certain acts (Act on the protection against eavesdropping).

1 January 2016, which also introduced a novelty, the principle of subsidiarity of the use of the means concerned under section 3(1), sentences cited: "if the achievement of the purpose would otherwise be ineffective or substantially impeded"[20].

Originally, the SIS had a so-called "pure intelligence profile", i.e. it was an intelligence service without executive powers and its task was to gather, aggregate and evaluate information on a defined range of threats. Its intelligence character was not expressis verbis expressed in the SIS Act, in which it was defined as a state body, but was implied by the definition of its material scope[21].

Act No. 444/2015 Coll. expanded or specified the material scope of the Slovak Information Service. With effect from 1 January 2016, the Slovak Information Service, within the scope of its competence, obtains, concentrates and evaluates information on:

- activities threatening the constitutional establishment, territorial integrity and sovereignty of the Slovak Republic,
- activities directed against the security of the Slovak Republic,
- activity of foreign intelligence services,
- organised criminal activity,
- terrorism, including information on participation in, financing or support for terrorism,
- political and religious extremism, extremism manifested in a violent manner and harmful sectarian groupings,
- activities and threats in cyberspace if they threaten the security of the State,
- the illegal international transport of persons and migration of persons,
- facts capable of seriously endangering or damaging the economic interests of the Slovak Republic,
- threat or leakage of information and things protected under a special regulation or international treaties or international protocols[22].

5. Intelligence and current threats to the national security

Intelligence services play also a significant role in obtaining and evaluating information relating to national security. However, their activity is not just a technically neutral activity, but a social and political matter. In recent years, there has

[20] Act No. 166/2003 Coll. on the protection of privacy against the unauthorised use of information-technical means and on the amendment and supplementation of certain acts (Act on the protection against eavesdropping).

[21] M. Aláč, *Osobitosti použitia*…, pp. 268–276.

[22] Act No. 444/2015 Coll.

been an increase in the prominence of various threats to national security emanating from both state and non-state actors, including the increased terrorist threat following the 2015 and 2016 attacks, the migration and refugee crises, as well as the rise of disinformation following Russia's annexation of Crimea in 2014. All of these threats have come to the forefront of public discourse in Central and Eastern European countries, including Slovakia. Intelligence services, which are the primary bodies responsible for gathering and assessing information on these threats, have played a crucial role in this debate.

The evolutionary development of society and the growing threat of organised crime have necessitated an adaptation of the scope of the Slovak Information Service. In order to be able to effectively counter the new security risk, which penetrated into all spheres of social life, Act No. 46/1993 Coll. on the SIS was amended by Act No. 256/1999 Coll. The Slovak Information Service has long operated in a classified mode. It was only in 2011 that it gradually started to publish its annual reports. These reports provide valuable information on SIS activities and its perception of security threats in the context of terrorism, the migration crisis, digital propaganda and Russian aggression. Despite the fact that SIS publishes its reports, the methods of constructing security threats in the context of domestic and foreign challenges remain under-researched in the Slovak literature. However, these constructions have a significant impact on the political and social discourse on individual threats and influence policy decision-making in the field of national and European security[23].

6. Conclusion

Reliable identification of the facts of a crime, as well as of its perpetrator, often poses a challenge for law enforcement authorities. For this purpose, it is necessary to resort to the use of other specific evidence – intelligence information.

The current status of the use of intelligence information in criminal proceedings can be characterised as theoretically possible, but only rarely implemented in practice. In our legal opinion, the current Criminal Procedure Code, Act No. 301/2005 Coll., allows the use of intelligence information in evidence provided that the legal requirements and conditions are met. In this context, it is necessary to pay attention to the issues of legality and admissibility of evidence in the context of national and international legislation, as well as the case law of the European Court of Human Rights.

[23] M. Kovanic, *The construction of threats by intelligence agencies: analysing the language of official documents in Slovakia*, "Critical Studies on Terrorism" 2021, Vol. 14, No. 1, pp. 117–138.

In support of the argumentation of the legality of the use of intelligence information as evidence in criminal proceedings, we can cite § 4a of Act on the protection against eavesdropping. The cited provision states that the use of information and intelligence means requires prior court approval. It follows from the foregoing that, in so far as the legislature has conferred such power on the courts and the use of the information thus obtained does not contradict the definition of evidence under the Criminal Procedure Code, the information thus obtained may be regarded as evidence in criminal proceedings.

The applicability of the results of intelligence activities in criminal proceedings stems from their ability to compensate for the lack of traditional evidence as defined in Art. 119(3) of the Code of Criminal Procedure. In cases where these conventional means of evidence are insufficient to fully clarify the facts, information obtained through the use of information-technical means or operational-search activities provides a necessary supplement to the missing information on the course of the criminal offence. However, it should be noted that the importance and status of intelligence information is also enshrined in the current legislation, which is not "perfect".

We anticipate that the issue of the use of intelligence will require increased attention in the near future, particularly in specific types of crime, such as international organised crime and terrorism, where its use will be necessary and indispensable.

Bibliography

Aláč M., *Osobitosti použitia ITP v pôsobnosti Slovenskej informačnej služby* [in:] *Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní*, Praha 2017.

Ivor J. *et al., Trestné právo procesné,* Bratislava 2010.

Ivor J. *et al., Trestné právo procesné 1*, Bratislava 2017.

Kovanic M., *The construction of threats by intelligence agencies: analysing the language of official documents in Slovakia*, "Critical Studies on Terrorism" 2021, Vol. 14, No. 1.

Marko M., Kohan P., *Legislatívna úprava operatívno pátracej a spravodajskej činnosti v Slovenskej republike* [in:] *Aktuálne otázky aplikácie kriminálneho spravodajstva v kontexte nových trendov v Európskej únii*, Bratislava 2018.

Mole B., Harby C., *Právo na spravodlivý proces. Sprievodca na aplikáciu čl. 6 európskeho dohovoru o ľudských právach*, Bratislava 2006.

Pikna B., *Nástroje evropského práva v oblasti získávaní důkazů při aplikaci operativně pátracích prostředků* [in:] *Sborník příspěvků z mezinárodního semináře uskutečněného na Policejní akademii ČR dne 2. listopadu 2004*, Praha 2004.

Pili G., *Intelligence and Social Epistemology – toward a Social Epistemological Theory ofIntelligence*, "A Journal of Knowledge, Culture and Policy" 2019, No. 33(6).

Repík B., *Procesní důsledky porušení předpisů o dokazování v trestním řízení*, "Bulletin advokacie" 1982.

Vaško A., *Možnosti využitia spravodajských informácií v trestnom konaní*, "Zborník z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2019" 2019.

Vaško A., S*pravodajská informácia – významný zdroj poznania pre trestné konanie*, Bratislava 2020, https://www.judikaty.info/cz/document/article/6901/ [access: 30.11.2024].

Vaško A., *Spravodajské informácie v trestnom konaní v slovenskej republike de lege lata* [in:] *Zborník pôvodných vedeckých prác, štúdií a odborných článkov Kriminálne spravodajstvo*, Bratislava 2022.

Vaško A., Lisoň M., *Hrozby a riziká – objekty spravodajského záujmu*, 2020, No. 2.

Záhora J. *et al.*, *Dokazovanie v trestnom konaní*, Praha 2013.

Legal acts

Act No. 300/2005 Coll., the Criminal Code, https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2005/300/ [access: 30.11.2024].

Act No. 301/2005 Coll., the Criminal Procedure, https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2005/301/ [access: 30.11.2024].

Act No. 124/1992 Coll. on the Military Police. https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/1992/124/20240715 [access: 30.11.2024].

Act No. 166/2003 Coll. on the protection of privacy against the unauthorised use of information-technical means and on the amendment and supplementation of certain acts (Act on the protection against eavesdropping). https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2003/166/20160101 [access: 30.11.2024].

Act No. 46/1993 Coll. on the Slovak Information Service, https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/1993/46/20240715 [access: 30.11.2024].

Act No. 404/2015 Coll. amending Act No. 166/2003 Coll. on the protection of privacy against the unauthorised use of information-technical means and on the amendment and supplementation of certain acts (Act on the protection against eavesdropping), as amended, https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2015/404/20160101 [access: 30.11.2024].