DOI: 10.52694/ThPSR.2024.3.8

Jacek Dworzecki
Marek Delong
Izabela Szkurłat

Prevention and detection fiscal crimes. Experiences of the Slovak Republic

Zapobieganie i wykrywanie przestępstw podatkowych. Doświadczenia Republiki Słowackiej

The article presents the methods and forms of operational and investigative work carried by the Slovak police in identifying and combating fiscal crimes. Also outlined are the forms of tax avoidance identified in Slovakia. IT detection tools, including databases, used by Slovak police officers in the fight against organized economic crime were discussed in detail.

Key word: Slovak Republic, tax crimes, crime prevention, crime detection, police

W artykule przedstawiono metody i formy pracy operacyjno-śledczej prowadzonej przez policję słowacką w zakresie rozpoznawania i zwalczania przestępstw podatkowych. Przedstawiono również formy unikania opodatkowania zidentyfikowane na Słowacji. Szczegółowo omówiono informatyczne narzędzia wykrywcze, w tym bazy danych, wykorzystywane przez słowackich policjantów w walce ze zorganizowaną przestępczością gospodarczą.

Słowa kluczowe: Republika Słowacka, przestępstwa podatkowe, zapobieganie przestępczości, wykrywanie przestępstw, policja

Introduction. Theoretical aspects of detection of tax crime

The detection work, correlated around such complex issues as tax evasion or tax fraud, is in its nature a cognitive action aimed at identifying the hidden characteristics of this kind of criminal behaviour, the action being based on the theoretical and methodological basis of the operational cognitive process. The correlates of the detection work, referring to the aforementioned phenomena, are the concepts of cognitive crime and process activities.

We can characterize the cognitive process of crime as a conscious, systematic operation of state organs and institutions which aim is to obtain, collect, classify, evaluate and analyse information about crime, specific crimes, perpetrators and victims, which consequently allows law enforcement authorities to initiate criminal proceedings and accusation of specific persons. The cognitive process of crime is based in particular on operational and procedural activities that fall within the scope of police activities.

According to the Slovak doctrine resulting from legal acts and literature, police activities should be understood as a system of methods, means, procedures and powers that are used by police formations as part of their statutory tasks to ensure public safety and order. Initiatives undertaken by these formations focus on many issues of social life, especially in the area of criminalization of social behaviour, administration, and security management. These activities are based on national legal regulations, ratified international agreements, as well as on the principles of professional ethics and scientific knowledge. The main goal of police operations is to fight crime and other antisocial behaviours, protect public order, human life and health[1].

Police activities carried out on the territory of the Slovak Republic include activities in the field of forensic technique, operational and exploratory work, investigative and preventive work as well as staff investigation. The basic division of activities undertaken as part of the operational and exploratory work as well as the investigation work is based on three forms:

[1] A. Filák, V. Porada, *Pojem, obsah a hlavní organizačne taktické formy policejně bezpečnostní činnosti*, „Policajná teória a prax" 2006, no. 4, p. 5-17.

- search activities (activities consisting in the search for people hiding from the justice system, perpetrators of crimes and missing persons);
- investigation work (procedural activities related to established crime);
- operational and exploratory work (activities related to disclosure crimes and criminal mechanisms, most often as a result of secret activities of the police)[2].

Searching activities involve finding specific, individual objects that exist and can be identified and distinguished from other objects of the same type. A positive effect of these activities is to stop, identify, bring or transfer the object sought[3].

Investigation work is a process that refers to registered crime that is known to law enforcement agencies. This process begins with the initiation of criminal proceedings and submission of a statistical report on a specific crime, which is recorded in the crime register kept by the Police Corps of the Slovak Republic.

Operational and exploratory work is usually correlated with hidden (undisclosed) crime, i.e. with crimes that were actually committed, but information about them did not reach the law enforcement agencies. Its positive result is the disclosure of acts previously unknown to the police. The methodological foundations of the detection activity in the framework of operational and exploratory work is created by a theory of reflex (mapping), „(...)because the detection of a crime consists in revealing and recognizing its mechanism and identifying the consequences of violating applicable legal norms, which clearly indicates the occurrence of a prohibited act. The detection process enriched with initiatives aimed at revealing the hitherto hidden forms and methods of criminal activity and factors determining its existence is in fact the process of obtaining, analysing and evaluating a series of information that is encoded in a concrete material situation directly related to the delict and physical preparator (pejorative, penalized changes occurring in the studied environment that can be revealed and deciphered are in their essence traces of crime)”[4].

The essence of the reflex theory is the ability of some (material) systems and objects to penetrate, interact and reflect in a different form the

[2] J. Nesnídal, *Neodvratnost trestního postihu a operativně pátrací činnost*, published by Forensic Laboratory of the Public Security Corps, Prague 1989, p. 80.

[3] *Spravodajská činnost'*, (ed. by) J. Stieranka et al., published by the Police Corps Academy, Bratislava 2013, p. 27.

[4] V. Porada, J. Straus, *Kriminalistická stopa*, „Kriminalistika” 1999, no. 3, p. 187.

properties of other systems and objects. Under the influence of a reflex (artificially initiated), changes occur in the mapping system. These changes indicate or reproduce the properties of the mapped system to some extent. The occurrence of a crime is one of the material phenomena of objective reality, during which the components of this crime interact (including primarily the actions of the perpetrator using means and tools at the scene), object or entity of crime, as well as the awareness of third parties, witnesses. The result of this interaction is the creation of mapping in the form of physical changes in the environment (material traces) and changes in human awareness (memory traces). From this point of view, the typical, cognitive objects are:

- the preparator;
- the object being attacked;
- used tools (e.g. financial instruments);
- victim, aggrieved entity;
- many other objects.

The aforementioned objects meet with each other at the time of a criminal event, as a result of which there are various contacts between them, including the mutual transfer of information. The transmission of this information may take place with varying intensity, and their content may be difficult to identify using modern technical means or other currently available solutions or tools.

Changes made by the perpetrator at the crime scene, which result from his individual characteristics and conduct, can be determined on the basis of specific signals (indicators), determinants and according to specific detection rules. These rules include, i.e.:

- the dependence of objects and phenomena of material nature (the behaviour of the perpetrator, his personality traits, e.g. the attitude to legal and ethical norms, find a reflection in reality - they identify him in the surrounding environment);
- occurrence of a cause and effect relationship (a particular state occurs when specific conditions are met - not otherwise);
- correlation - a typical process of occurrence of specific changes, which in the presence of analogous conditions should inevitably happen;
- uniqueness, individuality of certain situations (the ability to recognize crime signals is more or less a tendency, as confirmed by research

results, many crimes remain undisclosed), and the possibility of identifying differences between them[5].

There is no possibility of a crime in which the interacting entities would not provide each other with information about themselves, and thus with no change in the environment of the crime in which the perpetrator would carry out his unlawful activities.

The second correlate of the detection work are process activities. The disclosure of crimes is not a one-off operation or an episodic act, but a process that consists of relatively independent detecting work, essentially carried out in a pre-determined order. It could be said that the process of revealing crimes is a directional action, during which, in a pre-determined sequence while maintaining the hierarchy of priorities, various operational and investigative activities are carried out, aimed at identifying and revealing previously unknown factors that will help in the characterization of the investigated delict or its perpetrator. It should also be emphasized that this strictly cognitive process is a specific information analysis cycle, during which various operational activities can be carried out parallelly, dispersed asymmetrically at many levels of the initiated detection process. The aforementioned cycle is open and therefore absorbs many new information, which are then under development. The immanent component of the information analysis cycle are modern IT tools used to process, compiling and cataloguing of the acquired data[6].

Based on the assumptions that create the theory of forensic traces and forensic identification, which implement to the discussed process the activities involving acquiring, analysing and evaluating of information encoded in a concrete material situation, we can conclude that this cognitive mechanism is the sum of complementary actions which in particular include:

- obtaining preliminary information (indicator, signal) about the preparations, implementation or execution of a crime;
- gathering information enabling to expand the current state of knowledge about criminal activity;
- evaluation of information;

[5] M. Lisoň, J. Stieranka, *Organizovaná kriminalita v Slovenskej republike*, published by the Police Corps Academy, Bratislava 2004, p. 95.

[6] J. Dworzecki, J. Stieranka, *Wybrane możliwości identyfikacji (detekcji) deliktów skarbowych w realiach Republiki Słowackiej [Selected Possibilities of Identifying (Detecting) Fiscal Delicts in the Reality of the Slovak Republic]*, „Zeszyty Naukowe" ["Scientific Journals"] 2015, no. 1, p. 160-184.

- analysis of information;
- creation of logical conclusions.

The information about the occurrence of an activity deviating from the normal tax situation, which is commonly known and correlates with compliance with applicable legal regulations, should be considered as a signal of tax offenses. It may contain traces of information about a certain degree of probability regarding the causative actions taken in the preparation, committing or executing of a prohibited act, penalized in the legislative approach to tax issues.

The very notion of a signal has a multidimensional character, which is reflected in many pragmatic approaches in its formulation. In the first place, it is about obtaining preliminary information appearing in the vicinity of the observer and regarding the chosen phenomenon, on the basis of which the further process of its recognition takes place. This phase can also be identified as „capturing" appearing signals indicating the existence of a certain state, which due to its specificity, consisting, for example, of non-compliance with legal norms in force in a given environment, evokes in third parties suspicions about negative mechanisms and criminal behaviours occurring in this environment (both individually and collectively). By adopting a different optics, one can also interpret a given situation as „(...) a deviation from the public standards that are commonly known and correspond to the legal and social norms adopted by the general public"[7]. Such a state or situation, which is unacceptable in many respects, takes a concrete, tangible form, and this means that we will learn about their internal distractors through external signals. It should also be pointed out here that the antinomy of the aforesaid situation occurs in practice, which usually manifests itself in the sudden occurrence of changes of an external character, signalling the existence of internal problems.

In the implemented detection process, we cannot always find or properly identify the signals and symptoms of the criminal mechanisms we are looking for. The perpetrators of tax offenses use imperfections of the state's economic instruments and various legislation gaps. Taking into consideration the doctrine of criminal activities as always contrary to the social interest, it is understandable that the methods that the perpetrators

[7] I. Látal, *Příznaková analýza a možnosti jejího užití v policejní praxi*, „Kriminalistika" 1996, no. 1, p. 73.

use to achieve their own goals are implicit in nature and very often are developed in the smallest details.

The process of obtaining signals about tax delicts, the specificity of which makes that the execution of such acts is characterized by a high crime rate, is very complex and requires full and systematic coordination.

Making quasi-recapitulation of the above considerations, it should be pointed out that every criminal activity in the analysed area - both in the implementation phase and already completed - leaves traces of tax delicts in its immediate environment. In addition to the above conclusion, it should be added that the initiation of each detection activity can be based on seeking answers to three basic questions:

- Where can we obtain signals about tax offences?;
- Who can obtain credible signals about tax offences?;
- How can we obtain signals about tax offences?[8].

When looking for answers to the first question, the specificity of this kind of crime should be taken into account, including its characteristic features, known methods and forms of action of the perpetrators and traces left by criminals, as well as the very merits of committing a specific tax delict. Signals can be noticed in information appearing in the economic and social sector, in particular:

- in accounting conducted by natural and legal persons (especially on the basis of invoices issued and received);
- in tax declarations (of natural and legal persons);
- in bank operations (particularly cash and non-cash payments via bank accounts);
- in commercial transactions (especially when buying and selling movable and immovable property);
- in IT databases and in common information resources that are correlated in connection with tax proceedings and proceedings in customs matters[9];
- in other sources.

[8] J. Stieranka, J. Dworzecki, *Predchádzanie, zamedzovanie a odhal'ovanie daňových únikov a daňovej trestnej činnosti v Pol'sku a na Slovensku*, published by European Association for Security, Kraków 2016, p. 107-118.

[9] The term customs procedure should be understood as an organized process of applying the provisions of the broadly understood customs law or a series of correlated activities of customs authorities and persons who are responsible for the exercise of rights and obligations in relation to goods imported or exported from the national customs territory. Source: J. Kozakiewicz, *Postępowanie w sprawach celnych [Proceedings in Customs Matters]*, published by ABC, Warsaw 2002, p. 9.

As regards the second question, i.e. „Who can obtain credible signals about tax offences?", first of all, the entities (natural, legal) which activity in this area is determined by legal regulations and which conduct their core activity in the economic or social sector or in a broader milieu (the so-called legally obliged entities) should be identified. These include in particular:

- accountants;
- auditors (statutory auditors);
- employees of financial and accounting services in the public finance sector;
- bank employees;
- employees of other financial institutions;
- employees of entities dealing with real estate trading;
- other persons statutorily obliged to this type of activity[10];
- representatives of law enforcement agencies (especially members of the Police Corps of the Slovak Republic - units and organizational units fighting crime, economic crime, employees of the Crime Treasury Office, etc.);
- other natural and legal persons.

The answer to the third question: „How can we obtain signals about tax offences?" depends on the competences and statutory powers available to specific entities operating in the state, local government and private sector, as well as in other spheres of the social life of the country.

For the detection process carried out in the reality of the Slovak Republic, signals proving the tax delicts may penetrate through the aforementioned entities in various ways.

Use of currently available operational and explorative opportunities for detection of tax offences

The basic tool used by officers of Slovak internal security formation in the fight against tax crime are legal instruments (operational and procedural activities) included in legal acts of the rank of the act and in the

[10] Act of the National Council of the Slovak Republic of 2 July 2008 on the protection against the legalization of property resources derived from criminal activity and terrorist financing (Law Gazette No. 297 of 2008, part 113, p. 2350-2366).

executive regulations. The most important regulations in this respect include the Act No. 652 of the National Council of the Slovak Republic of 26 October 2004 on State Customs Authorities[11] and Law No. 171 of the National Council of the Slovak Republic of 6 June 1993 on the Police Corps[12].

In accordance with § 30, section 1 of the Act No. 652/2004, operational and exploratory activities mean „(...) the system of essentially secret methods of intelligence work, implemented by the tax administration to prevent, limit, detect and document criminal activity and its perpetrators; activities aimed at protecting certain persons, technical and physical protection of specific facilities and activities involving the observation of persons remaining in the operational interest"[13]. However, § 38a, section 1 of the Act No. 171/1993 indicates that the operational and procedural activities are „(...) a system of essentially secret intelligence activities carried out by the Police Corps to prevent, limit, detect and document criminal activity and its perpetrators; actions aimed at protecting certain persons, technical and physical protection of specific facilities; activities consisting in providing assistance and ensuring security to witnesses or protected witnesses at risk, protection of the state border and exploration activities implemented against persons and objects"[14].

In the Slovak doctrine of interpretation, the notions of operational and exploratory activities are perceived as a system, based on legal and union acts, of actions of secret, control and intelligence character that are carried out by criminal and counterintelligence services, using methods, forms and means of operation and exploration, with the aim of preventing, limiting, detecting and documenting crime, and determining their perpetrators and activities in the context of targeted search. Operational and procedural activities are perceived as a coherent system of organized, interdependent activities, measures and solutions that are used in an adequate and proportionate manner to the forecasted situations and threats. In this system, a deliberate, thoughtful and coordinated combination of activities of all the criminal forces of the Police Corps and the Treasury Administration was established. The use of operational and

[11] Source: The Act No. 652 of the National Council of the Slovak Republic of 26 October 2004 on State Customs Authorities, as amended. (Law Gazette No. 652 of 2004, part 276, p. 6464-6484).
[12] Source: The Act No. 171 of the National Council of the Slovak Republic of 6 June 1993 on the Police Corps, as amended. (Law Gazette No. 171 of 1993, part 46, p. 770-784).
[13] Source: § 30, section 1 of the Act No. 652/2004, on State Customs Authorities, as amended.
[14] Source: § 38, section 1 of the Act No. 171/1993, on the Polive Corps, as amended.

procedural activities by officers is to help in revealing crimes, identifying their witnesses and perpetrators, as well as in obtaining other important information about criminal behaviour and mechanisms, especially when it is not possible to obtain this information as a result of investigative or prosecution work or its acquisition is associated with huge financial outlays for the implementation of process activities. Therefore, a kind of „mission" of operational and procedural activities is creating favourable conditions for initiating and developing ongoing legal actions and facilitating making substantive decisions. Operational and procedural activities precede investigative work (operational identification, disclosure and documentation of crime) or are conducted in parallel to criminal proceedings. They form a comprehensive system which consists of the following basic elements:

- methods of operational and exploratory work;
- means of operational and exploratory work;
- forms of operational and exploratory work;
- forces of operational and exploratory work[15].

Methods of operational and exploratory work serve the effective and mostly secret use of means, forces and forms in police actions. We divide them into basic and specific ones. The basic methods of operational and exploratory work, which in accordance with current Slovak legal regulations can be applied depending on the operational situation, include:

- operational observation of goals;
- operational information gathering (police and administrative databases, police informers);
- operational control (taken against persons with operational interest, including the inspection of standard correspondence and correspondence carried out by means of electronic communication, recording the content of conversations with the use of technical means, recording sound or taking pictures);
- purposeful search[16].

Forms of operational and exploratory work are the methods of using forces and police resources to obtain or verify operational information.

[15] J. Meteňko, *Systémový prístup a teória operatívnych a spravodajských činností*, [in:] *Teoretická reflexe a identifikace společenských potřeb ve vazbě na aktuální problémy policejní praxe. Sborník z mezinárodní konference konané na Policejní akademii České republiky v Praze ve dnech 29.-30. září 2003*, (ed. by) V. Porada, A. Lukešová, published by The Police Academy of the Czech Republic in Prague, Prague 2004, p. 309-318.
[16] J. Tadanaiová, *Aplikácia kriminalisticko-technických metód v operatívno-pátracej činnosti*, „Policajná teória a prax" 2012, no. 4.

In the Slovak doctrine, the perception of this kind of secret activities includes:

- operational detection work, i.e. purposeful, systematic operation of officers performing operational work, the essence of which is to obtain information about the objectives remaining in the interest of a given service. This form of operational work can be carried out jointly with procedural acts or independently of the conducted investigation and investigation work.
- verification of operational information, i.e. purposeful, systematic operation of officers performing operational work, the essence of which is to test the credibility and confirm the usefulness of the information possessed;
- operational development, i.e. purposeful, systematic operation of officers performing operational work, under which optimal - in relation to the weight of the case being conducted - methods and means of operational work are used, in particular operational techniques necessary for effective control and response in the area of crime control[17].

The means of operational and exploratory work include persons, tools, and devices or their elements, due to which officers performing tasks of a secret nature can, i.e., more efficiently obtain and verify operational information, depending on the current needs of operational work.

Pursuant to § 38a, section 2 of the Act No. 171/1993, the operational and exploratory work forces are part of operational and exploratory operations carried out by specific Police Corps services[18]. These services include, e.g.: Criminal Police Service, Financial Intelligence Service, Property Protection Service, State Border Protection Service, Security Service

Constitutional State Officials, and Inspection Service. The purpose of these services is to prevent, reduce and detect intentional delinquencies and identify their perpetrators, in order to obtain reliable, satisfactory evidence enabling prosecution of those persons or obtain information to increase the effectiveness of protection of persons covered by security programs, endangered witnesses, informers and police agents.

Criminal Tax Administration Office, which is a specialized organizational unit in the field of, i.e., combating tax crime, performs operational

[17] *Bezpečnostnoprávna terminológia*, (ed. by) P. Ďurčo, published by the Police Corps Academy, Bratislava 2007, p. 104.

[18] Source: § 38, section 2 of the Act No. 171/1993, on the Police Corps, as amended.

work under § 31 of Act No. 652/2004. Among the available organizational and technical solutions as well as forms of operational and exploratory work available to the Tax Administration, the legislator pointed out:

- implicit observation of persons and objects, which, for the needs of the Tax Administration, is performed by the Criminal Office of the Tax Administration or the Police Corps at the request of the President of the Tax Administration, or an application of a person authorized by him;
- cross-border observation of persons based on international agreements in this respect, only on the grounds of granting permission for such activities by the President of the Tax Administration or a permission of a person authorized by him. The President of the Fiscal Administration or a person authorized by him applies to the authority of another country for permission to observe persons on the territory of that state, in accordance with the content of international agreements and arrangements concluded in this respect;
- controlled purchase;
- use of alarm systems and systems of technical protection of persons and property;
- use of an police informator or agent who will voluntarily and in an implicit manner obtain and provide information to the Tax Administration about crimes;
- legalization documents, i.e. documents (e.g. ID card, driving license, passport, birth certificate, marriage certificate, student ID), containing false data about the persons to whom the documents were issued. Thanks to these documents, which are issued and kept in a registry by the Tax Administration Criminal Office, the actual identity of an officer, witness or collaborator (informer, agent) with the Tax Administration is kept confidential.

Means and forms of operational-detection work which are used by the Police Corps officers have been covered by § 39 of the Act no. 171/1993. The act includes in this regard:

- confidential observation of persons and objects;
- system control over persons and means of transport;
- controlled purchase;
- criminal intelligence, including actions under cover, recruitment;
- use of legalization documents;
- alarm systems and protection systems of persons and property;

- cooperation with police informers;
- use of special objects, conspirational premises located at disposal of the Police Corps;
- confidentially supervised consignment[19].

All the above indicated components of operational-detection work have not been characterized in details within the act no. 171/1993, however their description may be found in the implementing regulations covered by the non-disclosure clause issued by the Ministry of Internal Affairs of the Slovak Republic.

Within the doctrine of actions realized by the officers of criminal forces of the Police Corps of the Slovak Republic it has been assumed that a confidential observation of people and objects is a form of operational-detection work which is subject to acquiring – in strictly specified by law timeframe – information on persons, objects (movable and non-movable) located in the operational interest of police officers. The observation is carried out in a confidential manner by police officers, police informers (recruited civilians with no public officer's status) or police agents, in places of public usability, in centres and shopping malls, entertainment spots, sport facilities and its purpose is to establish the criminal mechanisms and behaviours, identify perpetrators, secure important information as well as – as far as possible – secure traces necessary for the correct course of further process proceedings on the given case[20].

The use of alarm systems and technical protection of people and property systems, according to the act on Police Corps, a form of operational-detection work. These solutions which take the form of, among others, electronic, radio technical, optical, acoustic, mechanical, chemical, visual and spatial representation devices and their components, are used in a confidential manner in public usability places or other places (upon consent of persons managing them), for the purpose of controlling the state of safety and public order.

The objects and places maintained under the legend (special objects, underground apartments) are perceived as forms of operational-exploratory work. They are used for the purpose of increasing the degree of the realized conspiracy of confidential actions, such as observations, operational control, controlled purchase.

[19] Source: § 39 act no. 171/1993 on Police Corps as amended

[20] J. Meteňko, *Sledovanie v bezpečnostných činnostiach*, published by the Academy of Police Corps in Bratislava, Bratislava 2002, p. 87.

The term „criminal interview" ought to be understood as a form of operational-process actions consisting of confidential obtaining, analysing and assessing information by an officer who operates under permanent or temporary legend in the criminal environment or its immediate environment. Undertaken actions are targeted at creating conditions that would enable introducing a police agent to criminal groups or acquiring for cooperation persons who formerly functioned in a given criminal environment.

Confidentially supervised consignment is a form of operational-exploratory work realized by the officers of the Police Corps jointly with customs officers forming pat of Tax Authorities. Legal basis for this type of special actions is § 111, sec. 1-7 of the Act 301 of the National Council of the Republic of Slovakia from 24 May 2005 Code of Criminal Procedure[21]. In light of the provisions of the above specified act, the term of confidentially supervised consignment ought to be understood as monitoring of movement (postage, transport, delivery) of a consignment from the sender to the addressee, in case when the operational or process information indicate that it may contain (or is posted without an applicable formal permit): unlawful psychotropic, steroid drugs, psychoactive substances, poisons, precursors for production of drugs, drugs, nuclear material or other radioactive material, chemical substances of high risk, tampered or falsified money, securities, falsified, tampered or illegally produced tax stamps, stamps, seals and excise tax bands, payment cards or other electronic non-cash payment instruments, firearms, weapon of mass destruction, ammunition and explosives, cultural monuments and other objects requiring an adequate authorization or objects designated for crime commitment of originating from crimes.

The purpose of this form of operational-exploratory work is to identify the party (recipient) or parties (sender, recipient) responsible for the given consignment. Consent for implementing actions under confidentially supervised consignment in the course of the ongoing process works is issued by the President of the Senate of the Supreme Court of the Republic of Slovakia. Under verification activities or initial process actions, such a consent is issued by the prosecutor who supervises them. In urgent cases, in case when any delays in time may cause an irretrievable loss

[21] Source: Act 301 of the National Council of the Republic of Slovakia from 24 May 2005 Code of Criminal Procedure (Collection of Acts no. 301 from 2005, part 130, p. 3098 -3218).

of evidence, while the required consent cannot be obtained earlier, the officers of the Police Corps may commence this form of operational-exploratory work. In such cases the police officers inform the prosecutor without any undue delay of the initiated actions. Should, within the time of 48 hours from informing the prosecutor, he fail to issue the required consent, actions under the confidentially supervised consignment must be ceased and the obtained information cannot in any way be used and must be immediately destroyed on the basis of the binding in this scope provisions of law. In the framework of monitoring the consignment, the Police Corps may undertake joint actions with the Tax Authorities, necessary to enable its transfer onto the addressee from another country or handing over the consignment from one foreign country to another in a situation when the Republic of Slovakia is only a transit country. Actions in the framework of confidentially supervised consignment are ceased upon a written command of the prosecutor, should the accompanying circumstances indicate that it constitutes a serious threat to human life or health, may possibly cause a serious damage to property or there is a possibility of occurrence of other serious hazard. When a situation occurs in which there is no possibility of effective monitoring of the consignment, actions may be ended also without a prior, written command of the prosecutor. In the framework of actions targeted at ceasing the monitoring process of a consignment the officers of the Police Corps undertake actions targeted at neutralizing threats which are linked to the given consignment. Should the consignment reach beyond the borders of the country, the Police Corps hands over its monitoring to the appropriate state organ within the territory of which the consignment is located, pursuant to the binding agreements and international agreements. Actions related to the confidentially supervised consignment may on each stage of its monitoring be registered by means of audio-visual equipment.

Controlled purchase is a form of operational-exploratory work consisting of the purchase, sale and other method of transfer of goods the possession of which is forbidden or requires special permission[22]. Actions in the framework of controller purchase are undertaken by the officers of the Office of Special Actions of the Presidium of Police Corps (Department of Special Actions of the Police Corps, Department of Special

[22] Source: § 41a Act no. 171/1993 on Police Corps as amended

Operations of the Police Corps) and the National Criminal Agency of the Presidium of Police Corps.

System control of persons and transport means is – in accordance with § 39 of the Act no. 171/1993 – measure of operational-exploratory work, reflected by the use of police and administration and international data bases (i.e. Information System Schengen[23]) designated for the processing of data on entities, persons and objects located in the scope of operational interest of the officers.

Legalization documents are the means of operational-exploratory work thanks to which it is possible to formally hide an identity of police officer of the Police Corps, operating under legend, an important witness, person covered by police protection programme or police informant.

In accordance with § 69 of the Act no. 171/1993, for the purpose of creating a credible legend, fake personal data (including expanded information) which have been assigned to legended persons are placed within the database of the Police Corps, in the IT systems maintained by state administration institutions, systems at disposal of local self-governments, in databases of Slovak special services and in databases managed by natural and legal persons. All institutions of state administration, local self-government administration and natural and legal persons to whom the Police Corps submits a written request have a statutory obligation to pass the empty templates of the issued documents, printouts, statements, cards, certificates etc. In light of the binding provisions of the law, legalization documents cannot include: MP card of the National Council of the Republic of Slovakia, card of member of the government of the Republic of Slovakia, identity card of a judge, identity card of a prosecutor and diplomatic passports. For the purposes of actions realized by the Police Corps, legalization documents are issued and serviced by the registry of the Department of Documents and Records (in the scope of creating legalization documents of some employees of that cell it operates in the confidential mode) of the Presidium of Police Corps. The documents are issued on the basis of the decision of the Minister of Internal Affairs or persons authorized by him.

Cooperation with the police informators is a form of operational-exploratory work which is realized by the police officers of the Police Corps in the framework of their professional tasks. Within the Slovak

[23] J. Balga, *Systém schengenského acquis*, publisher. Veda, Bratislava 2009, p. 81.

practice, the term „police informer" ought to be understood as a natural person who voluntarily, in a confidential manner, passes under police detection actions, information on the criminal environment, criminals, criminal mechanisms etc. The Police Corps may carry out a register of police informers, who are used in the framework of specific operational actions[24]. Each informer is registered on a specific operational case and has a set up informer's card which contains his or her actual personal data, data of the assigned to them fictional identity, procedures of establishing contacts with the supervising police officer, established passwords for contacts and correspondences and other confidential details of cooperation. Informer's card, covered by the clause of „strictly confidential" may be found in a secured envelope, within operational case materials and may be accessed by the supervising police officer and in exceptional cases (provided for by the act) other, authorized in writing (by the leading police officer) police officer. Without consent of the police officer who maintains the informer's card it is possible to open it solely in case of death of such police officer or their complete inability to carry out official duties[25].

Officers of the Police Corps and the Criminal Office of the Tax Authorities cooperate with informers in a manner that enables them to obtain and pass on the information autonomously. The identity of an informer is strictly confidential and known solely to the police officers who carry out operational activities with participation of a given informer, police officer who recruited the informer for cooperation (in case when a police officer under legend was used for recruiting the informer) and the direct superior of the police officer carrying out operational activities[26]. Central Register of Informers is not maintained, despite numerous critical comments on the side of Europol representatives in this regard.

Police informer, while undertaking cooperation with the law enforcement, does not obtain any entitlements to which police officers are entitled in accordance with the Act on Police Corps. No civil-law agreement is concluded with him or her. In practice, this system functions on the principle of verbal arrangement, in the framework of which police

[24] Source: § 41 of Act no. 171/1993 on Police Corps as amended

[25] M. Fryštak, *Zamyšlení nad postavením informátora*, „Policista" 2004, no. 3.

[26] M. Fryštak, *Informátor jako jeden z nástrojů v boji s organizovaným zločinem*, [in:] *Nové jevy v hospodářské kriminalitě. Sborník z mezinárodní konference konané na Právnické fakultě Masarykovy univerzity v Brně v únoru 2005,* (ed. by) A. Nett, publisher Masaryk University, Brno 2005, p. 39.

expectations are passed on to the informer concerning the ongoing operational case and the form of remuneration (financial, in kind or other gratification compliant with the law).

In the opinion of experts a significant disadvantage of cooperation with informers, having an impact on lower (due to lower engagement) efficiency of their work is the lack of legal solutions enabling conclusion of a written, civil-law agreement covered by confidentiality clause. Such a document would enable optimal management of the process of cooperation with the police informer, regulating the manner of contacting them, specifying the subject, scope and purposes of cooperation, level of the agreed form of remuneration for the informer, methods and techniques of control and coordination and conspiracy of the carried out actions.

The key issue in the process of initiating an effective cooperation with police informers is the right choice of candidates. Proper selection depends, above all, from the experience of the police officer performing it. Furthermore, an important determinant while selecting a candidate for informer is the purpose of use of potential information obtained as a result of his or her actions. Police officers of the Police Corps and Criminal Office of Tax Authorities are not limited in the course of the recruitment process of informers by their nationality, so far criminal records, education, profession, religion, political views or age. Any person whose age, social competencies, life and professional experience, enable the correct and safe realization of the entrusted tasks may become an informer.

Within the environment of Slovak experts who deal with the issue of operational-exploratory actions a discussion concerning the lower age border for police informers is in place. On one hand, views are expressed that one should not limit by law the lower age border for persons who may become the informers, since this may narrow down the subject area in which operational cases are carried out and on the other hand, experts indicate that due to the risk which involves the sole form of cooperation with law enforcement, the informer must be able to conduct a real assessment of potential threats which requires a specific life maturity from them (non-recruitment of minors and juveniles). A good pattern of the discussed matter might be the legal solutions applied in Slovak military intelligence (military intelligence and military counter-intelligence),

which establish the lower age border of informers recruited for the purposes of armed forces, at the level of 18 year of age[27].

Limitations contained within acts no. 171/1993 and 652/2004 regarding verbal issues of co-employees indicate that the informer who acts on behalf of Tax Authorities or the Police Corps cannot be the officer of Slovak Intelligence Agency, soldier of the Military Intelligence and the officer of the Office of National Security.

Persons cooperating with the Slovak law enforcement as informers most frequently are driven by ideological motives (lawfulness, fight with crimes, care for undisturbed local, regional and national society development), economic (obtaining remuneration or other legally-allowed form of gratification) and personal (revenge, jealousy, attempt to eliminate competition with legally-available methods). The experiences of the Police Corps show that there were cases of undertaking cooperation with the police by a person who was excluded from the functioning of a given criminal group. Thanks to the operational support this informer re-commenced functioning in the criminal environment, however, driven by his own interest and disloyalty broke cooperation with the officers who had supervised him. In such a situation immediate actions are undertaken, targeted at detaining the police informer and neutralizing potential threats which might appear in relation to his actions.

Within the doctrine of operational-exploratory actions undertaken by the Police Corps and the Criminal Office of Tax Authorities on tax crimes, the network of informers is used, among others, for passing on fake information within the criminal environment or misleading ones, designated at disorganizing and deconspiring this environment. Furthermore, actions are undertaken consisting of introducing a police informer into such an environment, who after permeating to the structures of criminal groups gains trust of the invigilated group and helps the police in their process liquidation. Another method of operational actions designated to combat fiscal crimes is obtaining informers from that particular criminal environment or its immediate vicinity. Applying a specific method depends on the analysis of the operational situation of a specific case, while tasks passed on to the informers for realization

[27] Source: § 11, sec. 4 of the Act no. 198 of the National Council of the Slovak Republic from 30 June 1994 (Collection of Acts no. 198 from 2004, part 58, p. 1022 -1031).

are adjusted to their individual capacities, skills and the environment in which they operate.

The informer must be aware of the threats stemming from realization of the tasks entrusted to them. If they receive information on a real danger for them or their closest ones, the police officers undertake actions – based on separate provisions, targeted at ensuring physical or technical protection for them until the time of establishing the real nature of such a threat.

The police officer who supervises the informer within his actions must be guided by the binding provisions of law, care for a broader social interest and principles of professional ethics. The supervising officer cannot in any way encourage the informer to break the law. The officer is obliged to conduct regular check-ups of the manner of realization of tasks entrusted to the informer. The informer cannot obtain information in a manner non-compliant with the binding provisions of the law.

The Police Corps of the Slovak Republic, while carrying out cooperation in the framework of international operational-exploratory and investigation actions, may move the police informer (upon their written consent) for further supervision of the organs from a different country, within the area of which the actions are realized. The same mode of proceeding occurs in case of acceptance from the foreign partners of an informer operating within the territory of the Republic of Slovakia.

While attempting to compare the efficiency of detection actions realized in the scope of identifying and competing fiscal crimes, there is no possibility of a conclusive indication of solutions which are optimal. Upon the assessment of efficiency of detection actions which were undertaken one must consider the specificity of individual tax-payer categories, used criminal practices as well as other negative determinants which factually impact the shape of fiscal crimes. Therefore one ought to note that the best method of assessment of efficiency of detection actions will refer to individual elements of criminal actions, that is for the type of tax in which criminal groups got interested, modus operandi of perpetrators, accompanying circumstances of a crime and entities dealing with detection works. If a detection entity has at its disposal the knowledge about two elements which form criminal actions, its chances for a positive end effect of the conducted work actually increase.

Unfortunately it is not possible to carry out a reliable percentage division that presents the impact of individual components on the end result of a fiscal crime, since the available statistics do not include such data.

It possibilities of identification in the fight against fiscal crimes

Criminal actions referring to the area of taxes become increasingly sophisticated. Criminals constantly improve their methods, show a significant „creativity" in acting. Law enforcement, especially their specialized institutions, such as the Police Corps or Criminal Office of Tax Authorities must react fast to these threats. Implementing new procedures and solutions in the realized detection work, especially in the scope of identifying criminal mechanisms, is a sine qua non conditions for effective fight against fiscal crimes.

From amongst new solutions targeted at an effective fight with fiscal crime the implementation of which is currently being considered, implemented or modified for legal order of the Slovak Republic and the current doctrine of actions of the Police Corps and Tax Authorities (facilitating the so far applied solutions) the following may be found:

- Introducing strict tax supervision over the so called risk entities, through launching procedures of initial registration, proper registration and realization of strict tax supervision;
- Solutions consisting of the processing of gathered, additional information with the use of new, interactive tools and IT databases;
- Progressive methods of obtaining information.

Introducing a new supervision over the so called risk entities was covered in point 19 of the National Plan of Combating Tax Crimes. The basic assumption for this solution is to cover with a detailed supervision of the newly registered tax entities in the functioning of which the carried out analysis indicated the occurrence of factors of an increased risk. This form of monitoring would cover also the entities registered previously, in case of which the occurrence of increased risk factors was also identified. Strict supervision would be realized solely at a time necessary for the entity to reach the level of higher tax discipline that is until removal of legal and organizational shortcomings in the current functioning or until the moment of being deleted from the register of economic activity. Strict supervision would initially concentrate on:

- Newly registered tax entities with a specified risk degree;
- Newly registered tax entities towards which no risk degree was set (tax administrator registered a tax entity without carrying out an analysis

of a risk degree, since in the period of registration there were no negative signals which would indicate tax threats, stemming from the functioning of such an entity);
- Newly registered tax entities with a specific risk degree which formed part of reliable consortiums, corporations, economic associations and other, legally allowed forms of economic corporation.

Furthermore, detailed supervision, apart from the above indicated categories of tax entities, ought to cover the entities which strive for reimbursement by the state of significant VAT tax amounts (level of amount specified as significant would be specified on the basis of practice stemming from experiences of tax bodies) as well as entities attempting to lower their own tax liabilities.

The procedure of strict supervision would consist of three stages:
- Initial registration;
- Proper registration;
- Realization of strict tax supervision.

At the stage of initial registration, proper location-wise (for the seat of the applicant) unit of Tax Authorities to which the tax entity would submit a written application for registering in the register of VAT tax payers, in case of disclosing negative signals which reflect tax threats stemming from the side of registered entity would undertake actions targeted at verifying them. The field branch applies to the Directorate (central organizational unit with its seat in Banska Bystrica) of Tax Authorities on carrying out an analysis of risk factors and issuance of the opinion on tax feasibility and legal feasibility of the verified entity as well as persons acting on its behalf, including partners (in case of partnerships); In the framework of the initial registration, apart from actions targeted at obtaining an opinion on the entity, also a field inspection will be undertaken, consisting of carrying out an inspection at the place of carrying out economic activity by the entity, especially in terms of verifying the reality of its factual possibilities, in the scope of carrying out the declared activity as per the application for registration.

At the stage of proper registration the tax administrator of the field unit, based on the opinion and recommendations obtained from the Directorate of Tax Authorities, and pursuant to his own findings (including those stemming from the field inspection) undertakes a decision regarding acceptance or rejection of an application submitted by the entity for registering in VAT tax payers' registry. Since field tax administrator may

register entities without prior application for opinions about them, the Directorate of Tax Authorities, under preventive actions, ought to carry out tax risk analysis on an ongoing basis concerning registered entities and send to the proper facilities the results of such analyses for further use. The information regarding rejected applications will be sent to the Directorate of Tax Authorities for further operational use, analytical, training and evaluation purposes. The tax Administrator from the field unit should, within the information passed on to the Directorate:

- Include data on the non-registered entity;
- Indicate whether in the frames of the stage of initial registration any negative signals speaking of tax threats, stemming from the side of the registered entity have been disclosed;
- indicate which arrangements were made in the framework of the field inspection of the place of conduct of activity by the entity;
- indicate a cause of application rejection.

In the framework of realization of the third stage, that is strict tax supervision, after the passing of the first period of settlement of tax by the registered and monitored entity, tax administrator will carry out the so called local control, directed in particular at:

- verifying the correctness of information contained by the entity in application for registration within the register of VAT tax payers, including:
  - locating the place of conduct of activity;
  - turnover (in economic dimensions);
  - territorial scope of realized commercial transactions and provided services;
  - number of persons employed;
  - manner of carrying out the accounts;
- verification of the scope of factual economic activity led by the entity, including establishing which goods it produces/sells, which services it provides:
  - whether it only produces/sells goods or provide services indicated in the application;
  - whether it expanded its activity in an unauthorized manner;
  - whether it produces/sells goods or provides services which in their matter or course may constitute a tax risk factor;
- control of actual resources of the carried out economic activity, including:

– whether the entity really carries out economic activity;
– whether it has at least minimum resources and possibilities to conduct a declared form of activity at its disposal (i.e. Warehouses, personnel, assortment).

Applications from the field inspection will constitute the basis for assessing the tested entity, especially in the context of occurrence of risk factors within its activity and an opinion elaborated on their basis regarding the entity will be sent to the Directorate of Tax Authorities. Furthermore, the commission appointed on the field level of tax authorities will make decisions as to further mode and manner of conduct of strict tax supervision over the entity. In the framework of the decision, the planned for realization tasks will be indicated, among others, regarding the inspection nature (i.e. Field controls), their time, place, number, manner of documenting and consolidation of the obtained results. If the carried out actions indicate a significant irregularities in the functioning of an entity in the context of its fiscal obligations, and the entity fails to adhere to the cautions issued by the Tax Authorities, it will be possible – upon fulfilling the statutory premises – to delete this entity from VAT tax payer register. Whilst, in case of fulfilling by an entity covered by supervision of all the post-control recommendations and a permanent (verified in the space of five years) adherence to the rules of legal and organizational nature, the field tax administrator may terminate the strict tax supervision. The decision regarding termination of the strict tax supervision will be sent to the Directorate of Tax Authorities along with its justification.

The above characterized solution, consisting of intensifying control actions towards economic entities with unclear specificity will allow the tax administrator not only to identify these entities, but also to remove them from the country's economic space.

The second solution which will allow for effective fight with tax crimes is a more efficient processing of the gathered data on an additional, auxiliary nature with the use of new, interactive IT tools and IT systems and databases. The term „data processing" must be understood as an analysis and correlation of data saved in the police IT systems, including for instance: PATRMV, PATROS, PATRDOC, PATRZBRANE[28],

[28] Source: Regulation of the Minister of Internal Affairs of the Slovak Republic no. 30/2007 regarding servicing police databases. PATRMV – database on the sought transport means; PATROS – database on persons missing and identities of found human bodies; PATRDOC – database of missing and found documents; PATRZBRANE – database of missing firearms.

IPOLDAT[29], WPOLDAT[30], ZOP[31], ACHERON[32], EMON[33], in databases of other organs of state administration of the Slovak Republic (i.e. data bases of tax offices, customs offices, property registers, communal databases), in Europol, Interpol, SISI and EU databases. Obtaining additional operational information is possible also thanks to the use of legally allowed access to databases of legal persons, i.e. banks, insurance companies, tourist agents, capital funds. The broadest catalogue of access authorizations to IT systems and databases maintained by legal persons within the territory of the Slovak Republic is possessed by: Slovak Intelligence Agency, Military Intelligence Services (Army Intelligence and Army Counter-Intelligence) as well as the Police Corps and Tax Authorities.

The officers of Police Corps and Tax Authorities, while carrying out actions designated at combating tax crimes, most frequently avail of the information gathered and processed in IPOLDAT, WPOLDAT, ZOP and ACHERON systems.

IT System IPOLDAT, integrated with a manual operational-tactical information register, provides the officers who realize operational-exploratory work with data regarding:

- Crime perpetrators,
- Current methods of committing crimes and methods and techniques of covering up traces;
- Tactics of operations of the perpetrators;
- Repeated manner of perpetrator's actions (associations of modus operandi);
- Specific types of crimes (spatial association of similar crimes);
- Frequently attacked objects and persons within the territory of the Slovak Republic;

[29] Source: Regulation of the Minister of Internal Affairs of the Slovak Republic no. 161/2012 regarding servicing automated IPOLDAT system and manual operational-tactical registry.
[30] Source: Regulation of the Minister of Internal Affairs of the Slovak Republic no. 162/2012 regarding servicing automated WPOLDAT system and manual operational-tactical registry.
[31] Source: Regulation of the Minister of Internal Affairs of the Slovak Republic no. 74/2009 regarding servicing database of persons remaining in the scope of interest of the Police Corps. ZOP - registry of persons remaining in the scope of interest of the police.
[32] Source: Regulation of the Minister of Internal Affairs of the Slovak Republic no. 93/2010 regarding servicing the comprehensive system of criminal analysis ACHERON.
[33] Source: Regulation of the Minister of Internal Affairs of the Slovak Republic no. 50/2007 regarding servicing of the monitoring system of persons and means of transport.

- Conducted dactyloscopy data and similar for comparative purposes of samples of deoxyribonucleic acid (DNA);
- Criminal events;
- Legitimized persons;
- Movement of mechanic vehicles;
- IPOLDAT system consists of the following subsystems:
- Subsystem „Situational information" which enables search, analysis and processing of data entered into the system via situational reports;
- Subsystem „Events" (preview – without the possibility of entering data), which constitutes a component serviced by WPOLDAT system;
- POLDAT subsystem which enables registry of selected operational-detection actions as well as tactic activities and information in the scope of detected crimes;
- Subsystem „Person control" which enables entering data from activities of legitimizing and personal control;
- Subsystem „Movement of mechanical vehicles" which enables verification of data regarding the movement of mechanical vehicles.

Manual registry of operational-tactical information contains data concerning methods and tactics of acting of crime perpetrators; information regarding the level of crime on a given territory and other useful information in prevention, identification and detection of crimes as well as their perpetrators. The database covers:

- Photographs of known perpetrators and photographs from crime scenes;
- Registry of persons remaining under police observation;
- Registry of characteristic behaviours and body marks and tattoos of crime perpetrators along with photographic documentation;
- Registry of pseudonyms and fake surnames which are used by crime perpetrators or persons remaining under police observation;
- Data from dactyloscopy cards and samples of deoxyribonucleic acid (DNA);

Information concluded in the register refer to crime perpetrators, regardless of their age, gender and circumstances excluding penal responsibility, as well as describing the manner and tactics of acting of these perpetrators. Register of perpetrators (data are entered into the system on the basis of the so called B card) is maintained in consideration of the so called crime category and age. Tri-profile photograph with dimensions

of 6x13 cm or a photograph in digital format constitutes a component of B card.

Register of surnames of known perpetrators is elaborated alphabetically and removal of data from the register involves a simultaneous removal of all other information related to a given person.

Register of characteristic behaviours and body markings as well as tattoos contains data regarding all individual features of physical appearance of the registered perpetrators as well as covering the data on their disorders and psychological features (of permanent nature). Register is elaborated according to the division into sexes, division for individual body parts, disorders and psychological features as well as in consideration of the age of persons registered.

Register of pseudonyms and fake surnames, maintained in alphabetical order, contains data on fake personal data which are used by crime perpetrators, most frequently in the place of their residence.

Dactyloscopy cards and DNA samples (either with a unique number) are collected for process or comparative purposes and contain, apart from the collected material, also the data of police officers who collected the samples and a date and time of the conduct of a given activity.

Data to IPOLDAT system are entered on the basis of registration cards filled out by police officers who conduct operational-detection, investigation actions or actions in the scope of criminal technique.

Another IT system remaining at the disposal of the Police Corps is the so called WPOLDAT, in which the following registry is carried out:

- Criminal events, crimes and their perpetrators;
- Movement of mechanical vehicles;
- Absence of persons at work;
- Convoys protecting valuable objects and cash.

This system is used both in operational-detection actions, especially in the context of planning detection activities, and for facilitating actions of administrative nature which are realized by the Police Corps.

WPOLDAT system consists of the following subsystems:

- „Passwords, system" enabling administration of the entire system;
- „Vetting" which enables control over persons availing of this or other police system and granting access to them into specific databases, as well as allowing for creation of criminal reports (summaries);
- „Events" which enables registering in the data system events by persons authorized to do so;

- „POLDAT" which enables registering selected operational-tactical data and criminal data in the scope of crimes so far undetected;
- „Person control" which enables registering information about persons remaining under police observation, movement of vehicles and other objects remaining under police observation;
- „OTE Cards"[34], which enables registering statistical reports on crime levels;
- „Number of persons", enabling registration and verification of the presence of persons at a place of duty/work performance, in accordance with the information on personal register in individual field units of the Police Corps, including control of entry of organized convoys protecting valuable objects and cash;
- „Correction of code books", enabling corrections of safety codes and communications assigned to convoys organized by the Police Corps. Corrections may be carried out by authorized ordering parties of the convoy and system administrators.

Register of persons remaining under police observation (ZOP) is a nationwide policy IT system. This system gathers, processes and discloses information on persons appearing in the ongoing penal cases carried out by the police as well as in its operational actions. The main database which creates ZOP system contains the following information:

- Data on personal data of persons remaining under police observation (including first name, surname, maiden name, date of birth, place of birth, previous surnames, PESEL number);
- Verification of data identifying a person with data contained in the nationwide system „Population register";
- Nationality of person remaining under police observation (citizen of the Slovak Republic, foreigner);
- Status of person (alive, deceased);
- Supplementary data on persons remaining under police observation (their pseudonyms, used fake surnames, photographs an likenesses);
- Identifier of persons remaining under police observation, consisting of the police unit code of the unit which carried out the process activities and from the individual case number;
- Statistical, catalogue classification of crimes;

[34] OTE – operational-tactical information card.

- manners of completion of shortened preparatory proceedings, investigations or prosecutions;
- Commitment of crimes under influence of alcohol or narcotic drugs, drugs;
- Commitment of crimes with the use of firearms;
- Place of permanent residence of a person remaining under police observation.

Second database (Archive) of ZOP system contains archive information moved from the main database, including:

- Information on suspected persons occurring in the carried out investigation (including a detected or unresolved one) in a criminal case;
- Information on suspected persons occurring in the carried out criminal case (including in a detected or unresolved one) older than 80 years, whilst the last materials on the case must be elaborated fifteen years before and must concern the so called crimes of severe nature, including: contract killing, murder, assault offence, rapes, sexual abuse, human trafficking, terrorism – indicated in the Order of the Ministry of Internal Affairs no. 74/2009;
- Information on suspected persons occurring in the conducted criminal case (including detected or unresolved) older than 70 years, whilst the last materials on the case must be elaborated twenty years before, and neither of the forbidden acts as to which police proceedings were carried out fulfils the criterion of the so called crime of severe nature;
- Information on suspected persons occurring in a single criminal case older than 20 years, which does not fulfil the criterion of the so called severe crime.

In case of repeated commitment of a crime by persons remaining under police observation, in the framework of systematic update of information in ZOP system, data on the person contained in the database Archive are moved to the main database. Update of the system occurs:

– In a 24-hour cycle, data are entered and corrected manually, by the employees of cells which deal with police statistics based on the elaborated by the officers statistical sheets and summaries;
– Automatically, in strictly specified terms (in an annual cycle);
– Periodically, through manual moving of data on persons from the database Archive to the main system database.

Information on the person remaining under police observation are made available by the cell (single person position, division, department)

of police statistics, located in field units of the Police Corps (in the scope of basic data; substantive equivalent of Polish Departments of Criminal Intelligence KWP), and in exceptional situations, central system administrator. The basis for granting information is the submission of a written motion (in a machine printed version or in the form of computer printout) on verification of the criminal record of the person remaining under police observation. The application ought to contain: first name and surname (including maiden name), PESEL and place of birth of the verified person. Criminal information (in the basic version) regarding the verified person is granted within 48 hours from obtaining the application by the appropriate cell.

Access to the police systems is also granted to the so called persons authorized, having individual, electronic access keys and authorized to use the internal IT network of the Ministry of Internal Affairs of the Republic of Slovakia. These include most frequently the police officers of Slovak special services (civilian and military), employees of the National Security Office and employees and officers of the selected formations, realizing tasks related to internal security, i.e. Tax Authorities. Information on persons remaining under police observation are stored in police databases for 100 years (counting from the date of birth of these persons), after which time they are removed at the level of central administrator of these systems.

The administrator of the register of persons remaining under police observation is the Department of Administration of Police Databases of the Presidium of the Police Corps. The register contains personal data on the carried out criminal cases and the information related, which were gathered in the space of several decades. Currently these information, in electronic or digitalized form, are most frequently used by police officers and employees of the Police Corps and by other authorized institutions and formations.

The system of comprehensive criminal analysis ACHERON is an autonomous application created on the basis of a model of client-server interaction, with a digital transfer of data. This system shows, analyses, processes and discloses (at the application of authorized persons) the information regarding preparation, attempt and improvement of crimes. The system enables creating information regarding networks and criminal links, combines casual relationships with the behaviours of the criminals, and offers a wide range of data of intelligence character. ACHERON the

administrator of which is the Department of Administration of the Police Databases of the Presidium of Police Corps, works both on unclassified information and on those covered by „Classified" clause. The functioning of the system is also supported – in the scope of technical maintenance of connections – Division of IT, Telecommunications and Safety of Data Transfer of the Ministry of Internal Affairs and in the scope of information flow – Department of Criminal Analysis Management of the Presidium of Police Corps in Bratislava. IT potential of the system is formed by structured data, as well as information unselected from the sets which refer, among others, to persons, organizations, items, vehicles, transport means, places, accounts and bank operations which constitute a zone of interest for the police officers realizing operational-exploratory work, carrying out preparatory proceedings of investigations and other process actions.

The source of data for the system are:

- Information contained in the reports of police officers carrying out operational-exploratory work;
- Information obtained in the course of investigation actions;
- Information contained in other databases, integrated with ACHERON;
- Information stemming from open sources of information (coming from the means of mass media, internet, social media);
- Information coming from safe and verified, resort, national and international sources.

ACHERON is integrated with Europol databases and allows for an automatic exchange of information via the national communication interface Dataloader.

Whilst, one must include the following to the IT systems and databases which are used by Tax Authorities in combating fiscal crimes:

- ISFS-SD – basic IT system of Tax Authorities, consisting of the subsystems, integrated databases and browsers as well as accompanying applications, including:
  - DWH – application with data base, called Data Mining which thanks to the use of mathematical-statistical methods specifies the degree of risk as well as the height of the required financial security for the newly registered, so called risk entities;
  - AIS-R – basic analytical subsystem for combating fiscal frauds;

– VIES – EU system concerning exchange of information regarding VAT;
– Analytical subsystem of processing control reports;
– OIS KUFS – subsystem of operational information of the Criminal Office of Tax Authorities;
– ANDAT KUFS – analytical database of the Criminal Office of Tax Authorities.

Subsystem of operational information OIS KUFS and analytical database ANDAT KUFS which allows to gather, archive, process and transfer and use information on persons (natural, legal) who have breached the binding customs provisions or tax provisions or if there is a justified suspicion that such actions will be committed by them.

The role of analytical subsystem AIS-R is to classify threats related to the accounting activity of taxpayers and to register, analyse and identify the so called risk factors in order to prevent fiscal crimes. The subsystem realizes:

- The analysis and processing of organizational data on tax entities;
- Analysis and processing of information on cooperation with tax entities, their organizational and economic connotations etc.;
- Pursuant to the accepted operational criteria, it carries out a multiple-layer analysis of connections (personal, business) occurring between economic entities (the so called criminal analysis);
- Typing, based on the accepted selection criteria and their combinations of the potential so called risk subjects, for the purpose of covering them with individual supervision;
- The subsystem has analytical reports elaborated by state, self-government and private institutions;
- The subsystem offers specific data, enabling classification of tax entities, based on criminal analysis created from the information originating from other databases (not only Tax Authorities).
- Analytical subsystem on fiscal frauds AIS-R, searches for connections, interactions between specific entities, and the obtained results are presented in a graphic format (correlation diagrams, schemes etc.). The summary of data refers not only to the current information, but it may also analyse data and statistics with an archival status.

VIES system enables an exchange of information regarding VAT and it is an electronic instrument which is administered by the European Commission. VIES discloses, among others, the information on the

existing VAT number, VAT number which was not activated for the purposes of internal EU transactions and registration which has not yet been completed, since some EU countries require in their internal tax regulations a separate registration for internal EU registration. The Slovak Republic implemented the main principles of creating and functioning of the VIES system (including browser) along with its accession to the EU on 1 May 2004. One ought to point out that VIES is not a centralized IT tool of EU. Information regarding the national databases are automatically distributed to VIES of an interested EU member state by means of CCN/CSI network. Servicing this type of IT instrument in the realms of the Slovak Republic is carried out by the employees of the Department of International Administration Cooperation with the Directorate of Tax Authorities.

The analytical subsystem for the processing of control reports is an IT tool allowing for the search and identification of tax entities which in their operations avoid tax obligations, perform fiscal crimes or indicate the so called tax risk, that is circumstances accompanying their so far activity reveal that they may commit crimes or fiscal abuses. The subsystem shows data gathered in the IT bases of Tax Authorities and external sources. While analysing the obtained data, the subsystem reveals irregularities proving potential criminal behaviours. They are then subjected to an automated, expert analysis targeted at detecting the entire criminal mechanism.

Due to the fact that the obtained and processed data contain information covered by the act on personal data protection[35], they refer, among others, to sensitive data, company secrets etc., the administrator devotes a lot of attention to the subsystem. Safety of the processed data is guaranteed, among others, by the solutions contained in the adequate IT technologies, thanks to the procedures of administrative data service, as well pursuant to personalizing employee responsibility of the Directorate of Tax Authorities for servicing data packages.

[35] Source: Act no. 122 of the National Council of the Republic of Slovakia from 30 April 2013 on personal data protection as amended (Collection of Acts no. 136 from 2014, part 46, p 1054 -1080).

Special technical means for identification and combating fiscal crimes

Special technical means which are applied within the territory of the Slovak Republic in operational-detection actions targeted at preventing and fighting crimes, including fiscal crimes, include solutions encompassed in the Act no. 166 of the National Council of the Republic of Slovakia from 24 April 2003, on privacy protection against unauthorized use of information-technical means (colloquially - Act on protection against bugs)[36].

Information-technical means have been encompassed in the act as special, electrotechnical, radio technical, photographic, optical, mechanical, and chemical and other types of means and devices or their parts, used in an unclassified manner upon:

- Identification, opening and analysis of postal consignments or other deliveries;
- Bug or other form of telecommunication control[37];
- Analysis and use of video, sound recording or other technical form of recording reality.

Cited act no. 166/2003 specifies the conditions which are necessary for applying information-technical means. Within operational-detection actions with the use of special technique, police officers of the Slovak state security formations may avail only of such means which allow for an immediate identification of end telecommunication device, prevent deletion of data identifying the device and prevent removal of the time of bugging and the registered telecommunications transmission.

Information-technical means may be used solely in case of actions targeted at: ensuring safety and protection of the state, prevention and detection of crime or protection of constitutional rights and freedoms. Application of technical-information means may limit the basic rights and civil freedoms only in a specific scope and for the time not exceeding the necessary objective defined by the Act, in connection with which they have been used. Data obtained as a result of applying this sort of

[36] Source: Act no. 166 of the National Council of the Republic of Slovakia from 24 April 2003 on protection of privacy against unauthorized use of information-technical means as amended (Collection of Acts no. 166 from 2003, part 78, p 925 -928).

[37] J. Čentéš, *Podsłuch w słowackim postępowaniu karnym*, „Przegląd Policyjny"2013, no. 2, p. 128-142.

technical special means may be used solely for the purpose of fulfilling constitutional tasks imposed on the state.

Information-technical means may be used solely after obtaining a written consent of the court to which the application for their use was submitted. The consent is issued for a limited period of time, not exceeding six months. Within the undertaken operational-detection actions it is possible to simultaneously use several technical special means, but the scope of their use must correspond to the limitations covered by the consent granted by the court. If a necessity arises of the discussed means to be applied in places which are not publicly accessible, the court issues also a consent for access to these objects of police officers. Should justified circumstances occur, which require prolonging of application of information-technical means, the court may grant consent for continuation of operational actions with their use for the subsequent six months. The following must be included in an application for the use of information-technical means:

- Type of special technique means, place of its application, period in which it is to be applied, data on the person towards whom this means will be applied;
- Information on the previous, inefficient or significantly limited detection action undertaken in the case, in which application of special technique means was used. Along with the information, one ought to pass onto the court also documents referring to the undertaken, ineffective operational-detection actions in the given case;
- Causes for which information-technical means must be applied.

The court will undertake decision on the basis of a complete application which in case of noting any defects of formal nature must be returned to the applicant for supplementation. The judge who granted consent for the application of information-technical means is obliged to monitor the duration of causes for their application. In case of establishing these causes, the judge will without undue delay undertake decision on terminating the application of special means.

The Police Corps may, in exceptional situations, without the previously obtained court consent, apply the information-technical means:

- Should a justified suspicion of occurrence of a crime appear, which may be prevented by the police with the use of information-technical means;

- In case, when any delays in applying these means could cause a threat to life and health or property of significant sizes.

In case of existence of special situation, the Police Corps is obliged to inform the court of applying – without prior consent – information-technical means at the time not exceeding an hour from the moment of their factual use. In accordance with § 4 sec. 3 of the Act no. 166/2003, the police officers are obliged within six hours from commencing actions with the use of special technique (without a required, written consent of the court) to provide the court with an adequate application in which the actual time of applying the above indicated means is specified. In case of lack – within twelve hours from submitting the application – decision of the court approving the application or in case of rejection of approval of application, actions with the use of special technique must be unconditionally terminated. The information obtained at that time cannot be used in any form and their commission destruction is to take place within 24 hours from the time of obtaining them, in the presence of the judge, who did not approve the application[38].

Not only is the court obliged to monitor the reasonableness and duration of causes of use of special technique means. Also the institution which applies it is obliged by the law to immediately cease its actions if circumstances on the basis of which the consent for use of these means was issued no longer prevail. Institutions authorized by law to avail of information-technical resources are obliged to carry out written registers regarding applying this type of means in the carried out operational-exploratory actions. The copy of sound, image recording or audio-video recording which were obtained in the framework of the use of special technique may be passed solely onto the law enforcement organ of appropriate factual and local jurisdiction or onto the institution of justice. The recording may be used solely in the scope specified by law as a proof in the case. The submitted recording cannot in any way be multiplied or passed on to other institutions by the organs of law enforcement or justice.

If information obtained thanks to the special technique constitute a proof in the penal proceeding, the organ authorized is obliged to elaborate a written protocol in which the following will be included: place, time

[38] Source: § 4 and 5 of the Act no. 166 of the National Council of the Slovak Republic from 24 April 2003 on privacy protection against unauthorized use of information-technical means as amended (Collection of Acts no. 166 from 2003, part 78, p 925 -928).

and legal or factual basis of using these funds. Also a stenographic record ought to be attached to the protocol from the heard sound material or audio-video recording. Information obtained under the carried out actions which in their content do not refer to the case in relation to which means of special technique have been applied but the content of which contains other, disclosed criminal behaviours, may be used in the penal proceeding only when they refer to crimes in case of which this type of means was applied as allowable by law.

The National Council of the Slovak Republic, under its statutory authorizations, carries out control of lawfulness of adhering to the binding legal acts twice a year, including the act no. 166/2003. The commission on verification of validity of applying information-technical means appointed for this purpose after carried out activities elaborates a report covered by confidentiality clause, whereby information on all the operational actions are covered with the use of special technique, as well as their validity, results, persons responsible etc. Due to the fact that actions with the use of information-technical means significantly interfere with constitutional rights and freedoms, including above all the right to privacy, are covered by special supervision of the central state administration organs and entities creating an autonomous judicial power.

Other sources of information used for identifying fiscal crimes and deviating from the tax obligaiton

Slovak law enforcement organs obtain information on fiscal crimes not only as a result of their operational-exploratory work. Also natural and legal persons who pass on the information of this type of criminal acts via official notifications or anonymous submissions constitute a significant source. The information most frequently are sent by natural persons who function within the economic sector of the country and amongst notifications stemming from economic entities these information originate most often from their direct market competitors. The most frequent motives (official ones) by which persons submitting notifications of committed fiscal crimes are driven include care for safety of state finances and active control of adhering to the binding provisions of the law. Other motives, especially in case of anonymous submissions, include personal motives

(revenge, envy, breach of good name) and economic ones (liquidation or weakening of competitions, expected benefits stemming from disorganization in economic space).

A significant source of information on potential fiscal crimes are also official submissions to tax administration bodies, local self-government bodies and other institutions functioning in social-economic space of the country. These entities realize tasks under their statutory obligations of control nature as a result of which signals are often identified and facts displayed, confirming the existing irregularities of fiscal nature or the accompanying crimes in this scope.

A significant issue is the quality of information submitted to the law enforcement regarding the suspicion of fiscal crime commitment or of deviating from fiscal obligations, since it is this substantive level and burden of proof that decide whether a penal procedure will be initiated or whether operational-exploratory actions will be implemented (operational detection work, verification of operational information, operational working out) targeted at obtaining reliable proofs in investigated cases. Notifications on fiscal crime commitments which are passed on by law enforcement bodies from other countries also constitute an immanent element of fight with this form of crime within the area of the Slovak Republic.

An important, detection role within identifying the signals regarding fiscal crimes is played by monitoring by the officers, state officials and journalists of open information sources (information stemming from the mass media, internet, social media). Investigating journalists disclose on various occasions the information which constitute a proof of occurrence of criminal mechanisms and behaviours incompliant with the law, including fiscal crimes.

Cooperation upon gathering and obtaining information used for identification and compating fiscal crimes

Bilateral, multi-level cooperation in the scope of preventing and fighting fiscal crimes, undertaken by Slovak safety institutions is an indispensable element of effective fight with this form of crime. The most intense joint country actions are led by the officers from the Police Corps

and Tax Authorities, supported conceptually and in the scope of process supervision by representatives of General Prosecution. Furthermore, international cooperation in the customs, fiscal and police cooperation areas is considered as extremely efficient. All these actions result in a synergistic effect in the form of regularly reported increase in fiscal crime detection and thus – smaller losses for the state budget and greater fiscal impacts, especially in the scope of value added tax.

Fiscal goods are the solution which consists of creating supernumerary, specialized, tripartite task teams. In accordance with point no. 33 of the National Plan of Counteracting Fiscal Crimes, since 1 October 2013, teams consisting of a tax expert, [39]prosecutor and investigating officer commenced their operations, with a task of counteracting severe fiscal crimes. Members of the expert teams represent Tax Authorities, General Prosecution and the National Criminal Agency Presidium of the Police Corps. At the central level, the representatives of the above specified institutions meet four times a year in order to discuss the currently realized joint detection actions. Whilst, at the level of detection, the officers and employees of the engaged institutions realize cases with specific division into task areas. The function of detection task coordinator, realized under Tax Cobra is performed by Tax Authorities, consisting of:

- in analytical scope:
  - identification, based on the information gained in the framework of operational, analytical and control work, the cases of which must be subjected to detection work, under Tax Cobra;
  - analytical support of task teams of Tax Cobra through disclosure of all necessary data (statistical, operational, correlated information) stemming from the national and foreign databases (to which the Slovak Republic has access);
- in the scope of coordination of actions:
  - organizing meetings with experts included into the tasks teams of Tax Cobra;
  - coordination of information exchange between external institutions and task teams in the framework of the realized cases;
  - coordination of tax controls, undertaken by tax offices at the indicated entities, based on the suggestions of the task teams;

[39] In practice the task teams, pursuant to interinstitutional understandings have been in place since June of 2012.

- in the scope of expert cancelling:
  - Organizing trainings and consultations for the officers and prosecutors with participation of expert speakers, representing the Tax Authorities or other country and foreign financial and tax institutions.

Actions undertaken in the framework of the Tax Cobra are characterized by high efficiency, since thanks to this solution, within the initial two years, almost 46 million Euro was saved, the reimbursement of which was wrongly claimed from the state by tax frauds. From amongst the identified applications for undue VAT tax, the most frequent cases concerned trade in such items as: stone, diesel fuel, grains, ferrous metals, construction steel, toners, grain, sugar, meat, wood, wine and used vehicles.

International cooperation which occurs between customs organs and tax authorities of the EU is supported by an IT solution VIES which allows for and exchange of information regarding tax entities carrying out inter-union trade transactions. VIES system automatically receives data collated from periodical declarations, monthly or quarterly declarations elaborated by VAT tax payers, who provide services or export/import goods to/from other EU states. Data in the form of files (so called L1QD) are passed on to other EU states, which thanks to this have a possibility of comparing information on trade transactions concluded between their tax payers and the Slovak entities. Through this, Tax Authorities obtain information on intra-EU transactions and services provided, obtained or concluded by the Slovak tax-payers, thanks to which they may establish the level of tax which a given entity is obliged to pay as a service recipient. Foreign data with amounts are then compared with the information indicated by national tax-payers in VAT declarations. Within the model situation, the compared data ought to be ideally even. Otherwise, the disclosed discrepancies are subjected to verification realized by the tax administrator. VIES system compares the value of goods which constitute the subject of a tripartite transaction and the other recipient is obliged to repay the tax. Data concerning the values of goods contained in declarations are comparable with the market value accepted by the VIES system. This rule of exchange of information constitutes the basis for fiscal control over trade transactions realized under the unitary EU market.

Apart from the regularly distributed L1QD FILES, the VIES system enables also obtaining information on the Slovak entities obtaining goods

from outside the country's territory. Such information may be grouped on the following four levels:

- L1 (level 1) – information obtained by way of electronic circulation; which concern the total value of obtained (in the course of the last quarter) goods by all Slovak VAT tax-payers;
- L2 (level 2) – information obtained by way of electronic circulation which concern the total value of purchased (during the last quarter) goods by specific, selected (for control) Slovak VAT tax-payers. The verification carrying out institution obtains information about the amount of purchased goods from data provided by the suppliers;
- L3 (level 3) – information obtained pursuant to an application submitted by means of the Department of International Administrative Cooperation of Directorate of Tax Authorities to a conceptually adequate foreign tax institution. Submission of an application is justified in case of insufficient level of information disclosed on levels 1 and 2. In the framework of actions undertaken on this level, one may obtain information, among others, on the debatable invoices, concluded agreements between tax entities, specific trade relations existing between the national and foreign tax entities. The application is elaborated on SCAC 2004 form which thanks to the uniform form is transparent for all tax institutions of the EU states, which significantly impacts the speed of mutual communication.

The access to VIES system is also ensured, by means of WebDIS application, for the Slovak employees of the field tax offices. This application offers the possibility of carrying out comparisons of data stemming from the VIES system with the information contained in VAT declarations and allows for an automated identification of the occurring differences in figures. At the same time, VIES allows the tax administrator and controller to obtain information on untrue identification numbers of foreign purchasers – VAT payers which are covered in the registers maintained by the Slovak suppliers, including direct verification of these numbers.

Police cooperation in an international dimension, including actions designated against tax criminals, are based above all on cooperation in the framework of Europol and Interpol. The most broadly used analytical instrument is the Information System of Europol (hereinafter: EIS), which allows to identify the links occurring between data passed

on by member states and third countries[40]. The system contains data referring to the following persons:

- suspected of committing a crime;
- participating in a crime the specificity of which falls subject to substantive competencies of Europol;
- convicted of a crime, the specificity of which falls subject to substantive competencies of Europol;
- towards who there is a justified suspicion of committing a crime, the specificity of which falls subject to substantive competencies of Europol.
- Furthermore, EIS may be used for elaborating data:
- on the suspected occurrence of a crime, including the alleged place, time and type of crime perpetrator;
- on criminal means and mechanisms which have been applied or which may be applied for committing a crime, including information on legal persons;
- on entities dealing with detection of a specific crime, including the case number and other correlated data;
- on suspicions towards specific natural and legal persons, as to their participation in organized crime;
- On court judgements referring to cases the specificity of which is subject to substantive competencies of Europol.

Entities authorized to enter or obtain data from EIS are the central, police organizational units of EU member states, authorized liaison officers of the police and management and persons authorized, constituting the Europol's personnel. The national unit/cell of police on international cooperation is responsible for cooperating with EIS (responsible among others for coordinating the information exchange). This entity sends, updates or removes national information passed on by EIS and passes on the data entered into the system by other countries.

Automated transfer of information and personal data gathered in the IT system of the Ministry of Internal Affairs of the Republic of Slovakia and the Police Corps occurs by means of the national communication

[40] Source: Art. 11-13 – Decision of the Council of European Union 2009/371/JHA from 6 April 2009 establishing the European Police Office (Europol) (Official Journal of the European Union, L 121/37, announced on 15.05.2009).

interface Dataloader[41]. National Office of Europol, placed in the structure of the Office of International Cooperation of the Police Presidium of Police Corps in Bratislava, grants the selected officers the right of access to EIS after completion of training in the scope of servicing individual applications for this system. Data gathered in EIS are structured which enables searching for information regarding actions, persons, criminal groups, means of tele information communication, means of transport, explosive devices (including materials), firearms, payment means, identification documents (true and fake), currency, financial operations, bank accounts, drugs, chemical agents, nuclear materials etc. National police organs authorized for exchange of information with EIS have an encrypted connection with Europol headquarters which enables the transfer of confidential data (for confidentiality clause -„Classified").

EIS is supported by the Network Safety Application for Information Exchange (called SIENA), which enables fast, safe access to the system and exchange of information on operational, intelligence or strategic nature between Europol, member states of that organization and the third countries, with which the European Police Office has a concluded cooperation agreement. Within the process of construing and implementing SIENA, significant emphasis was placed on data protection and confidentiality of their transfer, whilst at the same time, establishing all legal regulations in this scope. SIENA application which operates since 1 July 2009 underwent in 2010 a modification which facilitated expansion of access to it onto other EU institutions, i.e. European Unit of Court Cooperation (called: Eurojust), as well as Interpol or state agencies of Australia, Canada, Norway, Switzerland and the United States.

The officers of Slovak police or intelligence formations only in exceptional cases (i.e. If delays in the operations may lead to the loss of proof or prevent pre-emption of a crime) may establish direct contact with the Contact Point of the Slovak Republic at Europol in Hague, of which they are to immediately inform the National Europol Office.

EIS system, fully supported by the functional indexing application, enables the use of information contained in the working files for analytical purposes. Indexing application is a tool which allows for verification

[41] Source: Order of the Minister of Internal Affairs of the Slovak Republic no. 29/2009 on national communication interface Dataloader to the automated transfer of information and personal data from the information systems of the Ministry of Internal Affairs of the Slovak Republic and the Police Corps to the Information System Europol (EIS).

and controlling of data on persons, objects, telephone numbers etc. The objective of this analysis, based on the accepted operational assumptions, is to create an image of:

- the structure of criminal groups;
- tasks of individual members of criminal groups or roles of persons participating in the criminal mechanism;
- method of functioning of the crime perpetrator (modus operandi);
- routes of money and goods transfers;
- sequences of events accompanying the criminal mechanism or specific crime.

Within the detection process upon processing of an indexing application for data located in EIS system, seemingly insignificant single data may occur, such as telephone numbers which after an in-depth analysis will facilitate disclosure of international criminal links or enable contact of the investigating officers from various countries, who carry out operational or investigations activities correlated around the same perpetrator (perpetrators) of a crime. This type of analytical approach enables identifying the so called weak points of criminal actions and through this, allow for establishing the direction of further intense actions which must be implemented for the purpose of deepening the so far state of knowledge.

Obtaining information on the criminal environment, its structure, links or methods of functioning, enables the takeover by adequate officers of proper methods in order to counteract crimes, including for instance launching of combined investigation teams (called JIT) and implementation groups, consisting of the officers of police formations of the interested countries[42]. Within the EU regulations referring to the analysis of working files the scope of data was indicated in detail which are to be subjected to explication and persons who may have access to such data as well as the length of their storage were identified[43]. These are, with regards to a natural person, such data as personal data, description of physical appearance, special markings or information enabling individual identification, information on profession and qualifications of persons,

[42] Source: http://gazeta.policja.pl/997/archiwum-1/2017/numer-142-012017/137712,Wspolne-zespoly-sledcze.html [access 10.10.2018].

[43] Source: Decision of the Council of European Union 2009/371/JHA from 6 April 2009 establishing the European Police Office (Europol) (Official Journal of European Union, L 121/37, announced on 15.05.2009) and Decision of the Council of European Union 2009/936/JHA from 30 November 2009 on approval of implementing regulations concerning the working files for the purposes of appropriate analyses by Europol (Official Journal of European Union, L 325, announced on 11.12.2009).

data on economic situation of persons, data on the manner of behaviours of persons, their personal contacts as well as information about the means of tele technical communication or transport means used by them. Data concerning the groups of persons include information on cases, potential perpetrators and witnesses. Cooperation between organizational entities of the Police Corps with Europol was regulated by means of an Order of the Minister of Internal Affairs of the Slovak Republic no. 4/2012 on international police cooperation realized by means of the National Office of Europol.

The tele-transmission system of Interpol, marked with I-24/7, enables an exchange of information between National Offices of Interpol from member states of this organization and the headquarters of Interpol in Lyon. The component of the system are the databases administered by law enforcement from individual member states of Interpol, to which access is granted – apart from the National Offices, also to the authorized police services[44]. The primary databases of which the system comprises include:

- NOMINALS – information on persons;
- DNA – information on gathered DNA profiles;
- FINGER PRINT – fingerprints;
- ICAID – photographs of children being the victims of crimes;
- SLTD – stolen and lost identity documents;
- SAD – stolen and lost official documents;
- SMV – stolen mechanical vehicles;
- WOA – stolen works of art.

Written application concerning cooperation (exchange of information) with a foreign partner, interested unit of the Slovak police or other authorized body is submitted to the National Office of Interpol, forming part of the Office of International Cooperation of the Police Presidium of Police Corps in Bratislava. The application ought to contain:

- first name and surname of application author and contact data;
- brief reason for application submission;
- description of action to which the application relates;
- data on persons covered by operational interest and their nationality;

[44] A. Szumski, *Sieć teletransmisyjna Interpolu jako narzędzie międzynarodowej współpracy policyjnej*, [in:] *Nowa Kodyfikacja Prawa Karnego*, t. 28, (ed. by) T. Kalisz, publ. Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2012, p. 313-324.

- data allowing for identification of entities, official documents, identity documents;
- Degree of priority (that is reply in standard mode - 10 days, urgent - 3 days, very urgent - 24 hours, immediate - immediately).

If an application does not contain a degree of priority, standard mode of granting answers is applied, while the „very urgent" or „immediate" modes of replies are reserved solely for exceptionally severe crimes or cases of occurrence of urgent situations. The officers may in exceptional cases apply for granting information directly to a foreign partner, of which they immediately are obliged to inform the National Interpol Office. Under international cooperation in border regions, the units of Police Corps may carry out actions with foreign partners without mediation of the National Office of Interpol in Bratislava. The applying unit is responsible for correctness of data covered in the application, for the use of obtained information solely for work purposes as well as for abiding by the instructions concerning the proceeding with information granted by the entity making these information available. If the reason conditioning the cause of submitting the application ceased to exit, the entity making an application is obliged to immediately inform the National Interpol Office of this fact.

The exchange of information in a situation in which the Police Corps or other Slovak service is an entity to which the application is sent from a foreign partner, it is carried out analogically to the above indicated principles. The difference occurs only in case of the accepted degrees of priority in granting replies, that is replies in standard mode - one month, urgent - 10 days, very urgent - 3 days, immediate - up to 24 hours. If the Slovak addressee of an application is unable to pass full reply to the applicant, it informs the National Interpol Office of this fact, whilst at the same time passing on the incomplete reply and indicating the timeframe that will be needed for elaboration of full reply. Cooperation under Interpol was regulated by means of the Order of the Minister of Internal Affairs of the Slovak Republic no. 51/2009 on international police cooperation, realized by means of the National Interpol Office.

Conclusion

Fiscal crime in its essence is definitely one of the most dangerous, anti-state phenomena which constitutes a real threat to the entire community which forms a country. Disturbing opinions of part of the Slovak society regarding lack of threats for the country safety which would stem from fiscal crimes cannot be left without reaction from the institutions and state organs as well as more aware citizens.

Actions undertaken within the territory of the Slovak Republic in the scope of counteracting fiscal crimes constitute a certain setup of connected vessels, since the use for this purpose of a broad catalogue of methods of operational-detection work as well as IT and modern technical solutions in a synergistic manner impacts the increase of detection of this form of crime.

Bibliography

Legal acts:

Decision of the Council of European Union 2009/371/JHA from 6 April 2009 establishing the European Police Office (Europol) (Official Journal of the European Union, L 121/37, announced on 15.05.2009).

Decision of the Council of European Union 2009/936/JHA from 30 November 2009 on approval of implementing regulations concerning the working files for the purposes of appropriate analyses by Europol (Official Journal of European Union, L 325, announced on 11.12.2009).

Act No. 171 of the National Council of the Slovak Republic of 6 June 1993 on the Police Corps, as amended. (Law Gazette No. 171 of 1993, part 46).

Act no. 198 of the National Council of the Slovak Republic from 30 June 1994 (Collection of Acts no. 198 from 2004, part 58).

Act no. 166 of the National Council of the Republic of Slovakia from 24 April 2003 on protection of privacy against unauthorized use of information-technical means as amended (Collection of Acts no. 166 from 2003, part 78).

Act no. 652 of the National Council of the Slovak Republic of 26 October 2004 on State Customs Authorities, as amended. (Law Gazette No. 652 of 2004, part 276).

Act no. 301 of the National Council of the Republic of Slovakia from 24 May 2005 Code of Criminal Procedure (Collection of Acts no. 301 from 2005, part 130).

Act of the National Council of the Slovak Republic of 2 July 2008 on the protection against the legalization of property resources derived from criminal activity and terrorist financing (Law Gazette No. 297 of 2008, part 113).

Act no. 122 of the National Council of the Republic of Slovakia from 30 April 2013 on personal data protection as amended (Collection of Acts no. 136 from 2014, part 46).

Regulation of the Minister of Internal Affairs of the Slovak Republic no. 30/2007 regarding servicing police databases. PATRMV – database on the sought transport means; PATROS – database on persons missing and identities of found human bodies; PATRDOC – database of missing and found documents; PATRZBRANE – database of missing firearms.

Regulation of the Minister of Internal Affairs of the Slovak Republic no. 50/2007 regarding servicing of the monitoring system of persons and means of transport.

Regulation of the Minister of Internal Affairs of the Slovak Republic no. 74/2009 regarding servicing database of persons remaining in the scope of interest of the Police Corps. ZOP - registry of persons remaining in the scope of interest of the police.

Regulation of the Minister of Internal Affairs of the Slovak Republic no. 93/2010 regarding servicing the comprehensive system of criminal analysis ACHERON.

Regulation of the Minister of Internal Affairs of the Slovak Republic no. 161/2012 regarding servicing automated IPOLDAT system and manual operational-tactical registry.

Regulation of the Minister of Internal Affairs of the Slovak Republic no. 162/2012 regarding servicing automated WPOLDAT system and manual operational-tactical registry.

Order of the Minister of Internal Affairs of the Slovak Republic no. 29/2009 on national communication interface Dataloader to the automated transfer of information and personal data from the information systems of the Ministry of Internal Affairs of the Slovak Republic and the Police Corps to the Information System Europol (EIS).

Monographs:

Balga, J., *Systém schengenského acquis*, publisher. Veda, Bratislava 2009.

Bezpečnostnoprávna terminológia, (ed. by) P. Ďurčo, published by the Police Corps Academy, Bratislava 2007.

Fryštak, M., *Informátor jako jeden z nástrojů v boji s organizovaným zločinem*, [w:] *Nové jevy v hospodářské kriminalitě. Sborník z mezinárodní konference konané na Právnické fakultě Masarykovy univerzity v Brně v únoru 2005*, (ed. by) A. Nett, publisher Masaryk University, Brno 2005.

Kozakiewicz, J., *Postępowanie w sprawach celnych* [Proceedings in Customs Matters], published by ABC, Warsaw 2002.

Lisoň, M., Stieranka, J., *Organizovaná kriminalita v Slovenskej republike*, published by the Police Corps Academy, Bratislava 2004.

Meteňko, J., *Sledovanie v bezpečnostných činnostiach*, published by the Academy of Police Corps in Bratislava, Bratislava 2002.

Meteňko, J., *Systémový prístup a teória operatívnych a spravodajských činností*, [in:] *Teoretická reflexe a identifikace společenských potřeb ve vazbě na aktuálni problémy policejní praxe. Sborník z mezinárodní konference konané na Policejní akademii České republiky v Praze ve dnech 29.-30. září 2003*, (ed. by) V. Porada, A. Lukešová, published by The Police Academy of the Czech Republic in Prague, Prague 2004.

Nesnídal, J., *Neodvratnost trestního postihu a operativně pátrací činnost*, published by Forensic Laboratory of the Public Security Corps, Prague 1989.

Spravodajská činnosť, (ed. by) J. Stieranka et al., published by the Police Corps Academy, Bratislava 2013.

Stieranka, J., Dworzecki, J., *Predchádzanie, zamedzovanie a odhaľovanie daňových únikov a daňovej trestnej činnosti v Poľsku a na Slovensku*, published by European Association for Security, Cracow 2016.

Szumski, A., *Sieć teletransmisyjna Interpolu jako narzędzie międzynarodowej współpracy policyjnej*, [in:] *Nowa Kodyfikacja Prawa Karnego*, t. 28, (ed.by) T. Kalisz, pub. Wroclaw University publishing, Wrocław 2012.

Articles:

Čentéš, J., *Podsłuch w słowackim postępowaniu karnym*, „Przegląd Policyjny"2013, no. 2.

Dworzecki, J., Stieranka, J., *Wybrane możliwości identyfikacji (detekcji) deliktów skarbowych w realiach Republiki Słowackiej [Selected Possibilities of Identifying (Detecting) Fiscal Delicts in the Reality of the Slovak Republic]*, „Zeszyty Naukowe" ["Scientific Journals"] 2015, no.1.

Filák, A., Porada, V., *Pojem, obsah a hlavní organizačne taktické formy policejně bezpečnostní činnosti*, „Policajná teória a prax" 2006, no. 4.

Fryštak, M., *Zamyšlení nad postavením informátora*, „Policista" 2004, no. 3.

Látal, I., *Příznaková analýza a možnosti jejího užití v policejní praxi*, „Kriminalistika" 1996, no. 1.

Porada, V., Straus, J., *Kriminalistická stopa*, „Kriminalistika" 1999, no. 3.

Tadanaiová, J., *Aplikácia kriminalisticko-technických metód v operatívno-pátracej činnosti*, „Policajná teória a prax" 2012, no. 4.

Internet sources:

http://gazeta.policja.pl/997/archiwum-1/2017/numer-142-012017/137712,Wspolne-zespoly-sledcze.html [access 10.10.2018].