Special intelligence means for collecting evidence of organised criminal activity in Bulgaria

Maria Yordanova

All means and methods provided for in the *Criminal Procedure Code* are employed to prove an organised criminal group and its activity, as are the provisions of the *Law on the Special Intelligence Means*, which regulate the application of specific operational techniques (surveillance, wiretapping, following, penetration, marking and monitoring correspondence and computerised information, controlled delivery, trusted transaction and investigation through an undercover officer) and the respective technical devices. The provisions of the *Law on the Protection of Persons at Risk in Relation to Criminal Proceedings*, the *Law on Combating Trafficking in Human Beings*, the *Law on the Electronic Communications*, the *Law on the Protection of Classified Information*[1], the *Law on the Forfeiture to the State of Assets Acquired from Criminal Activity*, the *Convention for the Protection of Human Rights and Fundamental Freedoms* etc. are also relevant to the process of gathering evidence.

Special intelligence means can play an important part in the investigation and proving of crime and **above all of organised crime** considering its specificities. Unlike traditional investigative methods, special intelligence means are applied without the subjects' knowledge and involve an interference with their private life.[2] Considering these circumstances, effective safeguards are needed against turning them into an instrument of arbitrary interference and abuse.

---

[1] The law exempts from the conduct of background investigation judges, prosecutors, lawyers and investigating magistrates, who have access by right to classified information of all levels for the duration of holding office respecting the "need to know" principle, where the information is for the purposes of the case concerned only (Item 7 of Article 39 (1) and Item 3 of Article 39 (3) of the Law on the Special Intelligence Means). In Judgment No. 6 of 18 November 2004 in Constitutional Case No. 7 of 2004 (promulgated in the State Gazette No. 104 of 26 November 2004), the Constitutional Court called attention to the fact that court is best positioned to verify the need of such access and the scope of information that should be accessible and decreed: "Upon the exercise of public powers conferred for the protection of rights, there is also a risk of abuse. The judicial discretion as to whether access should be granted to information, which constitutes an official secret and contains personal data ensures that the law will not be violated. In order for the court to make a decision, the request for access to an official secret by an investigating magistrate or a prosecutor must be reasoned."
All persons, in the course of or in connection with the exercise of their constitutional right to defence, are granted access to classified information of all levels for the time needed for the exercise of their right to defence and respecting the "need to know" principle (Article 39a of the Law on the Special Intelligence Means).

[2] For further details in this respect, see Judgment No. 528 of 29 January 2010 in Criminal Case No. 585 of the Criminal College, Third Criminal Department of the Supreme Court of Cassation, for the Year 2009.

In the *Criminal Procedure Code* (Section VIII of Chapter Fourteen), special intelligence means are described as **a method of collecting evidence in its own right in the pre-trial proceeding.** A detailed framework of the use, arrangements and application of special intelligence means as a method for "the prevention and detection of serious offences according to the procedure established by the *Criminal Procedure Code*" is provided for in in the *Law on the Special Intelligence Means* and, at the level of secondary legislation, in *Instruction No. 1 of 22 March 2004 on the Work and Interaction of the Preliminary Investigation Authorities*.

The variations in the framework under the *Criminal Procedure Code* and under the *Law on the Special Intelligence Means* are usually attributed to the diverging intended purposes and scopes of application of the two laws[3]. The regime under the *Criminal Procedure Code* serves the purposes of pre-trial proceedings and is applied by the pre-trial authorities. The pre-trial authorities apply the regime under the *Law on the Special Intelligence Means* as well, but the latter also serves a specified circle of special services, which apply it for prevention and other operational purposes. This approach of the legislator, however, hardly merits uncritical acceptance. Considering that the subject matter of regulation restricts important constitutional rights of citizens and other rights of the parties to the procedure, the approach should be exceedingly careful, accurate, rational, and precluding the risk of disparate interpretations and abuse.

The risks discussed above materialise in the framework outside the *Criminal Procedure Code*. Regardless of whether and how far it serves its declared purpose: prevention and detection of serious offences, this framework not always can simultaneously serve the purposes of collecting evidence in a criminal proceeding. Therefore, if it comes to the institution of a criminal proceeding, the data collected could not be used as admissible evidence (apart from several exceptional cases expressly provided for in the law) while the collection of new data may have become impossible. Along with that, there are other variations due to non-synchronisation of the provisions in the statutory instruments, which differ in rank and were adopted at different points of time.

1. Definition and scope of application of special intelligence means

[3] Паунова, Л. и П. Дацов, Организирана престъпна група [Paunova, L. and P. Datsov, Organised Criminal Group], Ciela, Sofia, 2010, pp. 150 ff.

The different statutory instruments define special intelligence means in a similar way. The existing definitions, however, display certain nuances, which do not reflect the objective divergence in their intended purpose.

According to the *Criminal Procedure Code*, special intelligence means are **technical devices:** electronic and mechanical facilities and substances serving to document controlled persons and sites, and **operational techniques:** surveillance, wiretapping, following, penetration, marking and monitoring correspondence and computerised information, controlled delivery, trusted transaction and investigation through an undercover officer [Article 172 (1)].

According to the *Law on the Special Intelligence Means* (Article 2), special intelligence means are **technical devices and operational techniques for their deployment**, which are defined in a way identical to the *Criminal Procedure Code*. The general definition of special intelligence means, however, is also bound to the preparation of **physical means of proof**: film recordings, video recordings, audio recordings, photographs and marked objects. Along with that, the *Law on the Special Intelligence Means* briefly defines each one of the operational techniques, whereas they are merely listed in the *Criminal Procedure Code*. Besides this, the *Law on the Special Intelligence Means* expressly states that the deployment of the operational techniques must be documented by means of photographing, video recording, audio recording and filming on **physical storage media** (Article 11).

Instruction No. 1 on the Work and Interaction of the Preliminary Investigation Authorities refers to the *Law on the Special Intelligence Means*, but its definition of special intelligence means departs to a certain extent from the definition contained in the law. The variation is in the list of physical means of proofs that are prepared: in addition to the ones listed in the law, the Instruction includes presentation slides [Article 160 (1)]. The provision defining the operational techniques [Article 160 (3)], too, has not been brought into conformity with the version of the law effective as from 29 April 2006 and, respectively, with the new *Criminal Procedure Code* and does not include the three new techniques added there: **controlled delivery, trusted transaction, and investigation through an undercover officer**.

In defining the scope of special intelligence means, the various statutory instruments also exhibit certain variations other than those attributable to their diverging intended use. The *Criminal Procedure Code* admits the use of special intelligence means by the pre-trial authorities during the investigation of **serious intentional offences** expressly specified in the *Criminal Procedure Code*, including offences related to an organised criminal group, provided the

relevant circumstances cannot be **established** in another manner or their establishment involves excessive difficulties. The *Law on the Special Intelligence Means* expressly specifies the cases in which special intelligence means can be used: only where this is necessary for the prevention and detection of serious intentional offences according to the procedure established by the *Criminal Procedure Code* and the requisite data cannot be **collected** in another manner. Apart from the insignificant terminological disparity, the scope of application under the *Law on the Special Intelligence Means* does not include the cases where the establishment of the circumstances involves excessive difficulties. On this point, there is no reason why the framework should take a different approach and it should be aligned.

As the Constitutional Court notes in its position, when special intelligence means are used, the privacy of the persons under surveillance is invaded by technical devices and operational techniques, thereby affecting citizens' rights enjoying constitutional protection (Articles 32 to 34 of the *Constitution*) and international recognition (Article 8 of the *Convention for the Protection of Human Rights and Fundamental Freedoms* and Article 17 of the International Covenant of Civil and Political Rights), which necessitates the use of special intelligence means only as a subsidiary method to the other methods of proving "if the relevant circumstances cannot be established in another manner or their establishment involves excessive difficulties".[4] The Supreme Court of Cassation, too, consistently upholds such a position, as it invokes the requirement of the law that special intelligence means be applied when the other traditional investigative methods have been exhausted or have failed to produce a result. A breach of this requirement is defined as a substantial breach of procedure and a ground for reversal. Some of the cases considered give the Supreme Court of Cassation grounds to conclude that the authority, which requested the deployment of special intelligence means, is unfamiliar with the requirements of the law and misleads the controlling authority.[5]

In line with its purpose, the *Law on the Special Intelligence Means* provides for a scope of application of special intelligence means beyond pre-trial proceedings: for the prevention and detection of serious intentional offences and in respect of **activities related to the protection of national security.**

[4] Judgment No. 10 of 28 September 2010 in Constitutional Case No. 10 of 2010. Promulgated in the State Gazette No. 80 of 12 October 2010.

[5] Judgment No. 528 of 29 January 2010 in Criminal Case No. 585 of the Criminal College, Third Criminal Department of the Supreme Court of Cassation, for the Year 2009.

In this connection, Article 12 of the *Law on the Special Intelligence Means* specifies the scope of application of special intelligence means both in terms of persons and sites. These are:

- persons about whom data have been received and in respect of whom a reasonable presumption can be made that they are preparing to commit, are committing, or have committed serious offences;
- persons about whose actions data have been received and in respect of whom a reasonable presumption can be made that they are used by the persons of the above group without being aware of the criminal nature of the activity carried out;
- sites for establishment of the identity of the persons belonging to the groups referred to above;
- persons and sites related to national security;
- persons who have consented in writing to the use of special intelligence means for the protection of their life or property.

Instruction No. 1 departs from the framework of the law and admits the application of special intelligence means in respect of persons about whose actions data have been received or in respect of whom a reasonable presumption can be made that they are used by any **other persons** without being aware of the criminal nature of the activity carried out (i.e. not only by the persons about whom data have been received and in respect of whom a reasonable presumption can be made that they are preparing to commit, are committing or have committed serious offences, as is the case in the law). This provision expands the scope of application of special intelligence means in conflict with the law and should not be applied.

The cited discrepancies justify the need to align the secondary legislation with the provisions of the special law, and the provisions of the special law with the provisions of the *Criminal Procedure Code*. Moreover, a **uniform regime for use of special intelligence means** has to be adopted, with all matters of principle being laid down in the *Criminal Procedure Code* with a reference (which is not in place at present) to the special law, which should further elaborate these matters of principle and describe in detail the individual cases.

2. Procedure for use of special intelligence means

The *Criminal Procedure Code* defines in general terms the procedure for the submission of a request for use of special intelligence means, the authorisation to use such means, and the procedure and period for their deployment

for the **needs of criminal proceedings**. For use of special intelligence means in pre-trial proceedings, the supervising prosecutor must submit a **reasoned request in writing** to the court [Article 173 (1)].

Article 13 of the *Law on the Special Intelligence Means* thoroughly amended and supplemented in 2008 and partially revised in 2009, specifies the persons who, acting within their authority, may request the use of special intelligence means and use the data and physical evidence collected by such means:

- Directorate General for Combating Organised Crime, Criminal Police Directorate General, Security Police Directorate General, Border Police Directorate General, Internal Security Directorate, regional directorates of the Ministry of Interior, and specialised directorates (with the exception of the Technical Operations Directorate), territorial directorates and stand-alone territorial departments of the State Agency for National Security;
- Defence Information Service and Military Police Service under the Minister of Defence;
- National Intelligence Service;
- the supervising prosecutor, who must submit a reasoned written request to the court for the use of special intelligence means in a pre-trial proceeding [Article 13 (2)].

After the revisions of the *Law on the Special Intelligence Means*, several institutions were excluded from the list of authorities authorised to request the use of special intelligence means. These include the Prosecutor General, the Supreme Prosecutor's Office of Cassation, the Supreme Administrative Prosecutor's Office, the Military Prosecutor's Office of Appeal, the prosecutor's offices of appeal, the Sofia City Prosecutor's Office, the district and military district prosecutor's offices, the National Investigation Service and the respective investigation services (the new version of the provision reflects the changes in the structure of the police and the Ministry of Defence, as well as in pre-trial proceedings). With good reason, the right of the prosecutor's office to request use of special intelligence means is limited to the supervising prosecutor considering his or her role in the pre-trial proceedings, which is consistent with the *Criminal Procedure Code*.

Authorities other than those listed above may neither request nor use special intelligence means (Article 13 (3) of the *Law on the Special Intelligence Means*). Instruction No. 1 reproduces an older version of Article 13, which is why the list of these authorities does not correspond to the one defined in the

law. This provision is illegal and should not be applied. Its retention, however, albeit hypothetically, may cause confusion which could slow down the granting of authorisation for use of special intelligence means, which in turn could delay or frustrate the investigation.

The mandatory information to be included in the request for use of special intelligence means is provided for in the statutory instruments, but the provisions of the *Criminal Procedure Code* and the *Law on the Special Intelligence Means* are not completely identical in this respect. The *Law on the Special Intelligence Means* enumerates the mandatory items in greater detail:

- complete and exhaustive indication of the facts and circumstances warranting a presumption that a serious offence is being prepared, is being committed or has been committed which necessitate the use of special intelligence means;
- full description of the actions taken so far and of the results of the preliminary check or the investigation;
- data identifying the persons or sites in respect of whom or which the special intelligence means are to be used;
- period of use;
- operational techniques, which are to be deployed;
- authorised official who is to be informed of the results of the use of special intelligence means [Article 14 (1)].

According to Article 173 (1) and (2) of the *Criminal Procedure Code*, the request of the supervising prosecutor must contain the same mandatory items, which are described in more general terms. Due to the fact that only the supervising prosecutor may request the use of special intelligence means in the pre-trial proceeding, the mandatory items in his or her request do not include data about the authorised official who is to be informed of the results of the use of special intelligence means.

The *Criminal Procedure Code* requires **additional mandatory information** to be included in the request in two cases. Where an investigation through an undercover officer is requested, the head of the entity which arranges and implements this investigation or a person authorised by this head must present to the authorising authority **a declaration in writing by the officer** that he or she is familiar with his or her duties and tasks under the specific investigation. The declaration is kept by the authorising authority and, instead of personal data of the officer, it states his or her personal identification number assigned by the entity which arranges and implements the investigation through an un-

dercover officer (Article 173 (3)]. Where the special intelligence means are used with the consent of the person in respect of whom they are used, the **written consent** of that person must also be attached to the reasoned request [Article 173 (5) and Article 14 (2) of the *Law on the Special Intelligence Means*).

The authorisation to use special intelligence means is granted **in advance** and **the court is the only authority authorised to grant it**. The legislator specifies the judicial authority to which the request must be addressed depending on the jurisdiction in terms of the investigated offence and, in certain cases, depending on the profession of the accused. The general rule is that the request should be addressed to the president of the district court or to a vice president expressly authorised by that president (in the case of Sofia City this would be the Sofia City Court). In cases to be heard by the **specialised criminal court**, the authorisation is granted in advance by the president of that court or by a vice president authorised by that president [Article 174 (3) of the *Criminal Procedure Code*]. Authorisation to use special intelligence means in respect of members of the armed forces is granted by the president of the respective district military court or a vice president authorised by that president.

Where deployment of special intelligence means is requested in respect of a **judge or the administrative head or the deputy administrative heads of a district court**, the authorisation is granted by the president of the competent appellate court or a vice president expressly authorised by that president.

The court, which has been approached with the request, must decide immediately after receipt of the request, and the court's act together with the request are handed back to the requesting authority [Article 174 (1) to (5) of the *Criminal Procedure Code* and Article 15 of the *Law on the Special Intelligence Means*). The *Criminal Procedure Code* provides for the keeping of a **register** of the requests submitted and the authorisations granted.

The use of special intelligence means itself is **arranged and implemented** only by the respective entities: the Specialised Directorate "Operational technical operations, specialised unit for arrangement and implementation of investigations through an undercover officer" of the Ministry of Interior, or the Specialised Technical Operations Directorate of the State Agency for National Security [Article 175 (1) of the *Criminal Procedure Code* и Article 20 (1) of the *Law on the Special Intelligence Means*]. The Minister of Interior or a deputy minister authorised in writing by that Minister and, respectively, the Chairperson of the State Agency for National Security or a deputy chairper-

son designated in writing by that Chairperson, acting on the basis of a written authorisation received from the respective court, is supposed to issue a **written order** for the deployment of the special intelligence means by the relevant entity. Depending on which directorate deploys the special intelligence means, orders down the chain of command are given by the head of the relevant directorate or a deputy head authorised by that head. A simplified procedure is provided for as an exception, where a request for use of wiretapping has been submitted by the Internal Security Directorate of the Ministry of Interior in respect of an employee of the Ministry: the Minister of Interior may propose to the Chairperson of the State Agency for National Security to issue a written order for deployment of this operational technique by the Agency's Specialised Technical Operations Directorate after obtaining the written authorisation of the court.

Unlike the above, in connection with the option to use special intelligence means for activities related to national security, the National Intelligence Service and the intelligence services of the Ministry of Defence may possess and deploy special intelligence means within the limits of their powers [Article 20 (2) of the *Law on the Special Intelligence Means*].

Legislation provides for exceptions from the standard procedure for use of special intelligence means in a situation of **urgency**. In the *Criminal Procedure Code*, such option is provided for only in respect of a single technique: **investigation through an undercover officer** [Article 173 (4)]. Such an officer may be used in urgent cases by an order of the supervising prosecutor, where this is the only possibility to perform the investigation. The supervising prosecutor has discretionary powers to determine whether the situation is urgent and whether other options to perform the investigation are available. The prosecutor's decision is subject to validation by the respective court within 24 hours. The activity of the undercover officer is discontinued unless the court grants authorisation within 24 hours. The court must also rule on whether the information collected should be retained or destroyed.

The *Law on the Special Intelligence Means* provides for possibilities to deploy **all types special surveillance means** in urgent cases, and their deployment may commence immediately after obtaining the written authorisation from the court, without complying with the ensuing ordering procedure described above. The *Law on the Special Intelligence Means* lacks a definition of "urgent case", and discretion is vested in the **authorised heads of the respective directorate**. The only requirement set by the law is that the Minister of Interior or the deputy minister authorised in writing by that Minister or,

respectively, the Chairperson of the State Agency for National Security or the deputy chairperson authorised in writing by that Chairperson, **be notified immediately**.

It is recommended to further elaborate the framework, establishing clear criteria as to which situations can be treated as urgent cases and introducing a requirement that the notification should provide reasons justifying the urgency of the case.

In cases of an **imminent risk** of intentional offences being committed or a **threat to national security**, according to Article 18 of the *Law on the Special Intelligence Means*, the special intelligence means may be used even without authorisation from the court, only on the basis of an order of the Minister of Interior or of a deputy minister authorised in writing by that Minister or, respectively, of the Chairperson of the State Agency for National Security or a deputy chairperson authorised in writing by that Chairperson. Such use is discontinued unless validated by the court within 24 hours. With the granting of authorisation, the court also validates the actions taken so far and rules on the retention or destruction of the information collected.

The special intelligence means may be used **within up to two months** after the authorisation is granted. Where necessary, this **period** may be extended by not more than four months following the same procedure applicable for obtaining the initial authorisation. Thus, the overall period may not exceed six months [Article 175 (3) and (4) of the *Criminal Procedure Code* and Article 21 of the *Law on the Special Intelligence Means*]. Upon expiry of the authorised period, the use of special intelligence means is discontinued *ex officio* by the entities authorised to apply them.

Apart from this case, the *Law on the Special Intelligence Means* provides for other grounds for discontinuing the deployment of special intelligence means. These grounds fall into two groups. The first group covers the cases in which the objective has not been achieved or the use of special intelligence means does not produce results. In such cases the authorities that have requested authorisation approach the entities deploying the special intelligence means with a written request to discontinue the use. The second group includes three cases in which the use of special intelligence means may not commence or may be aborted by the deploying entity: first, when there is a risk of exposure of the operational techniques; secondly, where the application of special intelligence means becomes impossible; and thirdly, where the tasks assigned pose a risk to the life or health of the undercover officer or of his or her ascendants, descendants, siblings, spouse or persons with whom the officer is in

a particularly close relationship [Article 22 (1) to (3)]. Regardless of the grounds for discontinuing, the specialised entity applying the special intelligence means is obliged, immediately after discontinuing the use, to notify in writing the court, which granted the authorisation, and the authority that requested the authorisation and issued the order for the use of the relevant special intelligence means. For the second group of grounds, the notification must be **reasoned**. The logic behind the last-mentioned requirement is that the deploying specialised entity has discretion to decide whether to discontinue the use or not to use special intelligence means.

The *Criminal Procedure Code* lists the same grounds for discontinuing the use of special intelligence means [Article 175 (5)] without dividing them into groups. Provisions are also made for a written notification to the authority, which granted the authorisation. The latter, in the cases where the information collected is not used for the preparation of physical means of proof, must order its destruction [Article 175 (6)]. By virtue of the *Criminal Procedure Code*, in all cases in which the application of special intelligence means is discontinued, the notification must be reasoned. It is recommended that the requirement of the *Criminal Procedure Code* for a reasoned notification be introduced for all grounds under the *Law on the Special Intelligence Means*.

The authorities, which requested authorisation for the use of special intelligence means, are obliged to assist the entities deploying these means with up-to-date information concerning the identity of the persons and sites subjected to the special intelligence means [Article 23 *Law on the Special Intelligence Means*].

3. Physical means of proof and evidential value of data obtained using special intelligence means

The *Criminal Procedure Code* lays down the procedural rules for investigation using special intelligence means. What matters most to proving in the criminal procedure are the **results** of the deployment of special intelligence means and their use. They are subject to some of the general rules of the *Criminal Procedure Code* for the preparation of physical means of proof and their attachment to the case and the special provisions of the *Criminal Procedure Code* and the *Law on the Special Intelligence Means*. The court and the pre-trial authorities are bound to collect and verify, *inter alia*, the physical means of proof prepared using special intelligence means in the cases provided for by the Code [Article 125 (2) of the *Criminal Procedure Code*).

Under the *Criminal Procedure Code*, two of the operational techniques: controlled delivery and trusted transaction, serve to collect physical evidence,

while in an investigation through an undercover officer the officer is interrogated as a witness [Article 172 (4)]. Apart from the general rules for the preparation of physical means of proof, the *Criminal Procedure Code* does not make any express provisions on the way of preparing means of proof using the rest of the operational techniques. The *Law on the Special Intelligence Means* lists the physical means of proof, which are prepared using special intelligence means: **film recordings, video recordings, audio recordings, photographs and marked objects** [Article 2 (1)]. These are in fact different types of documenting depending on the technical device used.[6]

New types of physical means of proof will probably emerge as a result of technological advances. Due to the fact that the use of special intelligence means usually violates certain personal rights [e.g. a temporary restriction of the inviolability of the home and the confidentiality of correspondence and of other communications – Article 1 (2) of the *Law on the Special Intelligence Means*] and there is a risk of interference with private life, **legislation in this sphere must be exhaustive and consistent and, moreover, must be regularly updated.**

As a rule, physical means of proof obtained using special intelligence means are prepared in duplicate and within 24 hours after their preparation are sent sealed to the prosecutor who requested and the court which granted the authorisation [Article 176 (1) of the *Criminal Procedure Code*]. By way of exception (introduced by the *Law Amending and Supplementing the Criminal Procedure Code* effective as from 28 May 2010), the prosecutor who requested the authorisation may warrant the preparation of the physical means of proof **in more than two copies** [Article 176 (2)]. This is possible only where the data obtained using special intelligence means in another criminal proceeding or at the request of some of the specialised authorities authorised to request deployment of special intelligence means under the *Law on the Special Intelligence Means* are also used for proving. In this case, too, a sealed copy of the physical means of proof must be sent within 24 hours after their preparation to the court, which granted the authorisation, and the rest of

[6] The Constitutional Court holds that most of the operational techniques, and in particular surveillance, wiretapping, following, penetration, marking and monitoring correspondence and computerised information, are associated with direct preparation of physical means of proof such as film recordings, video recordings, audio recordings, photographs and marked objects (See Judgment No. 10 of 28 September 2010 in Constitutional Court No. 10 of 2010, promulgated in the State Gazette No. 80 of 12 October 2010).

the copies must be sent to the prosecutor so as to be attached to the relevant criminal proceedings.

The physical means of proof obtained using special intelligence means are recorded in a report drawn up according to the terms and procedure established by the *Criminal Procedure Code*. Taking into consideration the principle that reports drawn up in this manner constitute written means of proof of the performance of the relevant actions, of the procedure according to which these actions were performed and of the evidence collected (Article 131 of the *Criminal Procedure Code*), the legislator establishes **special requirements for the report of the physical means of proof** obtained using special intelligence means.

Firstly, the report must be signed by the head of the entity which prepared the physical means of evidence and must contain specified mandatory information: an indication of the time and place of deployment of the special intelligence means and the preparation of the relevant physical means of proof, the identity of the person under surveillance, the operational techniques and technical devices used; a transcript of the content of the physical means of proof [Article 132 (2) of the *Criminal Procedure Code*]; and the conditions under which the results of the use have been perceived [Item 5 of Article 29 (4) of the *Law on the Special Intelligence Means*].

Secondly, the request for use of the special surveillance means, the written consent of the persons to use such means for the protection of their life, health and property in the cases provided for in the law, the authorisation for use of the special intelligence means and the order of the competent authority according to the procedure established by the *Law on the Special Intelligence Means* must be attached to the report [Article 132 (3) of the *Criminal Procedure Code*].

Thirdly, **the physical means of proof attached to the case** [Article 132 (4) of the *Criminal Procedure Code*] constitute an integral part of the report and are retained according to the established procedure [Article 29 (5) of the *Law on the Special Intelligence Means*]. Sketches, layouts, schemes and other graphic representations may also be attached to the report [Article 29 (6) of the *Law on the Special Intelligence Means*].

To be valid, the report must conform to these requirements. Along with them, a separate provision of the *Criminal Procedure Code* [Article 172 (5)] requires that all materials prepared using special intelligence means, including computerised data, collected and recorded by special technical devices, **be attached to the case.**

The legal rules governing the evidential value of the data obtained through special intelligence means is very important for the effectiveness of justice as well as for the balance of the rights and interests of the parties in the procedure. The general rule is that only results obtained within the limits of the submitted request for the use of special intelligence means are admissible in the criminal proceeding. There are two exceptions to this rule. One of the exceptions applies to the cases where in the course of the deployment of the special intelligence means data are found concerning another serious intentional offence, the investigation of which allows for the use of such means as well [Article 177 (2) of the *Criminal Procedure Code*). The other exception permits the use of the data obtained through special intelligence means in another criminal proceeding or at the request of some of the specialised authorities authorised under the *Law on the Special Intelligence Means* for proving a serious intentional offence (the investigation of which also allows for the use of such means) [Article 177 (3) of the *Criminal Procedure Code*]. The appropriate and lawful use of these exceptions may be very productive when investigating offences committed by an organised criminal group, which are usually closely linked both in terms of the members of the group and the acts committed by them.

The procedure for the preparation of physical means of proof in the course of deployment of special intelligence means is described in detail in Chapter Four of the *Law on the Special Intelligence Means*. The framework takes into consideration the specificities of the broader scope of application of the law. The results of the use of special intelligence means are documented on paper or on another data medium by the respective authority of the specialised entity of the Ministry of Interior or the State Agency for National Security immediately after these results are obtained [Article 25 (1)]. This medium, immediately after its preparation, is sent to the authority that requested the use of special intelligence means accompanied by the items received during the controlled delivery or trusted transaction. The authority that requested the use of special intelligence means may also receive, upon request, the prepared photographs, recordings, sketches and layouts. The specialised entities, which implement and arrange the special intelligence means, are bound to keep the physical medium within the period of use of the special intelligence means and to prepare the physical means of proof.

The *Criminal Procedure Code* obliges **computer information service providers** to assist the court and the pre-trial authorities in the collection and recording of **computerised data** through deployment of special technical de-

vices. However, this obligation applies only when it is necessary for the detection of the offences listed in the Code and the requirements for the deployment of special intelligence means are met. The request for assistance must be reasoned and conform to these requirements of the law. Otherwise, providers may refuse to provide assistance.

In order to be incorporated as evidence in the case and to be admissible in the procedure, the means of proof must be prepared in compliance with the rules for their preparation. This compliance is checked during the **verification and assessment** of the evidentiary material, which are pivotal in the proving process.[7] Due to the specificity of the special intelligence means, the pre-trial authorities and the court, while verifying the evidence collected by such means, have to perform all necessary actions to verify the truthfulness of the evidentiary materials (and, respectively, of the means of proof) and the compliance with the established procedure for their collection.[8] Any breach of this procedure, as listed below, would render the results of the deployment of special intelligence means inadmissible in the procedure and may frustrate the criminal prosecution:

- the use of special intelligence means was not requested by the respective authority;
- the request was inadmissible;
- the authorisation granted by the court exceeded the limits of the request submitted;
- the order of the respective authority for the deployment of special intelligence means did not correspond to the authorisation granted by the court;
- the special intelligence means were deployed after the authorisation's period of validity had expired;
- the special intelligence means were deployed without authorisation, and an authorisation was not granted within the established 24-hour time limit;
- the physical means of proof were not prepared according to the procedure established in the law;

[7] For details see Павлов, С., Наказателен процес на Република България, обща част [Pavlov, S., Criminal Procedure of the Republic of Bulgaria: General Part], Sibi, Sofia, 1996, pp. 343-348.

[8] According to an express provision of the Criminal Procedure Code [Article 125 (2)], the court and the pre-trial authorities must collect and verify, inter alia, the physical means of proof prepared using special intelligence means.

- the report on the preparation of the physical means of proof does not comply with the requirements provided for in the law;
- the physical means of proof were not sent within 24 hours to the prosecutor who requested and the court, which granted the authorisation for the use of special intelligence means.

Non-compliance with the procedure and the manner for the collection of physical means of proof by special intelligence means has serious negative consequences.

In the first place, such non-compliance may lead to infringement of fundamental personal rights and freedoms and of the fundamental principles of criminal procedure, which has an adverse impact on the collection of evidence as well. Such would be the case if the physical means of proof prepared using special intelligence means do not cover the entire period during which these means were deployed or the entire information collected (e.g. wiretapping in which separate phrases are taken out of the overall context of the conversation).

In the second place, such non-compliance may directly impede the proving of the criminal offence. In such cases the criticism is often levelled at the court without taking account of the specific reasons for presenting inadmissible evidence and for failing to prove the charge.

Insofar as the preparation of physical means of proof is an exclusive responsibility of the respective specialised entities and is implemented secretly, the actions of these entities have to be strictly regulated and to be subject to control by the heads of these entities and the authority that requested the use of special intelligence means. Responsibility should also be sought in cases of violations, which lead to compromised evidence or allow for the use of these instruments for inappropriate pressure. Concrete proposals for legislative amendments include the introduction of:

- time limits for the preparation of the physical means of proof;
- requirement that all results obtained during the entire period of the use of special intelligence means be transformed into physical means of proof;

- absolute prohibition to use the original information recorded on the physical medium under Article 24 of the *Law on the Special Intelligence Means* in the criminal proceeding.[9]

According to the *Law on the Special Intelligence Means* the presidents of the district courts or of the courts of appeal who granted authorisations for use of special intelligence means must include in their annual reports to "data about the number of authorisations granted and physical means of proof prepared" [Article 29 (8)]. A review of these data in recent years shows that **the requests submitted and the authorisations granted for application of special intelligence means tend to increase**.[10] At the same time, the use of such means in more than half of the cases is **unproductive**. This conclusion is based on a comparison between the number of authorised special intelligence means and the number of physical means of proof prepared after their use. Summarised information on the same issues can also be found in the first annual report for 2010 of the **parliamentary subcommittee** for oversight and monitoring of the procedures for the use of special intelligence means and for access to traffic data under Article 250a (1) of the Law on the Electronic Communications. According to that report, in 2010 the Bulgarian courts granted 15,864 authorisations for the use of special intelligence means, issued 134 refusals, and 3,388 physical means of proof were prepared.[11].

The information from the biggest courts, where the majority of cases related to organised criminal groups are also concentrated, illustrates this trend even more convincingly[12]. Thus, in 2010 the Sofia City Court[13] granted a total of

[9] The current version of the Law on the Special Intelligence Means also provides that this information be recorded on paper or on another data medium and that it must correspond to the information contained in the physical medium under Article 24, which must be kept by the specialised entities deploying the special intelligence means, but no sanctions are provided for non-compliance with this requirement.

[10] The number of requests and the number of authorisations granted do not correspond to the number of pre-trial proceedings because in many cases one request is submitted for the deployment of multiple operational techniques.

[11] According to the data released in the same report, special intelligence means were deployed in respect of 5,763 persons, and the Minister of Interior personally authorised special intelligence means in 142 urgent cases of a threat to national security. However, not a single Bulgarian citizen was notified according to the procedure established by Article 34h of the Law on the Special Intelligence Means that his or her communications and movements had been unlawfully monitored.

[12] According to the Report on the Application of the Law and on the Operation of the Prosecutor's Office and of the Investigating Authorities in 2010 (http://www.prb.bg/main/bg/Information/2076/), the largest number of pre-trial proceedings of significant public interest in connection with organised crime in 2010 (two-thirds of all pre-trial proceedings) were supervised at the Sofia City Prosecutor's Office, the Plovdiv District Prosecutor's Office, the Varna District Prosecutor's Office and the Burgas District

6,213 authorisations under the *Law on the Special Intelligence Means*, issued **15 refusals**, and received **709 physical means of proof**. Until 10 May 2010, when the *Law Amending and Supplementing the Law on the Electronic Communications* entered into force, vesting competence to authorise access to data in the president of the regional court or a judge authorised by that president, the authorisations numbered 4,942. By comparison, in 2009 the same court granted 3,662 authorisations under the *Law on the Special Intelligence Means* and 5,449 authorisations under the *Law on the Special Intelligence Means* and the *Law on the Electronic Communications*, issued 15 refusals, and received 329 physical means of proof[14]. Things are similar at the Plovdiv District Court, which has the country's second heaviest caseload after the Sofia City Court. According to the 2010 activity report of the Plovdiv District Court, it was approached with a total of **1,761** requests for use of special intelligence means (936 by the prosecutor's office and 815 by the Ministry of Interior and the State Agency for National Security), granted **1,751** authorisations, and received **197** physical means of proof. This means that in the predominant number of cases the application of special intelligence means did not contribute to prove the case during the trial.

In 2010, the Burgas District Court, which has the country's fourth largest number of magistrates and the fourth heaviest caseload after the Sofia City Court and the Varna and Plovdiv district courts, granted **697** authorisations for use of special intelligence means, of which **399** were requested by prosecutors and **298** were requested by heads of the authorities referred to in Item 1 of Article 13 (1) of the *Law on the Special Intelligence Means* (regional directorates of the Ministry of Interior, Directorate General for Combating Organised Crime, Criminal Police Directorate General, Border Police Director-

---

Prosecutor's Office, and the largest number of indictments in connection with oganised crime were submitted to the court by the Sofia City Prosecutor's Office (35), the Plovdiv District Prosecutor's Office (10) and the Varna District Prosecutor's Office (10).

[13] In 2010, a General Assembly of the Criminal Department of the Sofia City Court discussed whether the use of special intelligence means gives the court grounds to examine the case behind closed doors under the terms established by Article 263 (1) of the Criminal Procedure Code. The deliberations resulted in the conclusion that if the data obtained as a result of the use of special intelligence means do not constitute a state secret because they do not pose a threat to national security or to the sovereignty of the country, the publicity of the court hearing should not be restricted. See 2010 Annual Activity Report, General Assembly of Judges of the Sofia City Court, 14 March 2011.

[14] After the amendments to the Law on the Electronic Communications (effective as from 10 May 2010), the Sofia Regional Court was approached with 5,121 requests under Article250a (1) of the Law on the Electronic Communications, on which 1,114 refusals were issued.

ate General and the State Agency for National Security) .[15] In the preceding two years, 466 special intelligence means were authorised for 2009 and 236 for 2008. At the same time, a total of **131** physical means of proof were received for 2010. A total of **24** pre-trial proceedings involving physical means of proof were submitted to the Burgas District Court in 2010 with an indictment or a plea bargain agreement. The court's annual activity report concludes that the "effectiveness" of the use of special intelligence means for the court's geographical jurisdiction was **18.8 %** as a proportion of the total number of authorisations and **49.8 %** as a proportion of the number of persons.[16] As few as 41 authorisations, or 5.88 % of their total number, were issued for the protection of national security.

The report concludes with good reason that the numerous requests for special intelligence means deployed when the traditional investigative methods have not produced a result **prove just as unproductive for the detection of the offences within the court's geographical jurisdiction.**

For the same period (2010), the Haskovo District Court granted **657** authorisations for application of special intelligence means, and as few as **53** physical means of proof were prepared.[17]

The reports of the prosecutor's office also note a steep upward trend in the requests for use of special intelligence means. In 2010 such requests increased by 31.4 % compared to 2009 and about two and a half fold compared to 2008. According to consolidated statistics for 2010, requests were submitted for deployment of 11,618 techniques (up from 8,843 for 2009 and 4,690 for 2008), of which the courts granted 11,402 (98.1 %). Prosecutors drew up 3,427 requests for information, on which 3,104 responses were provided or

[15] Wiretapping is the most widespread technique, with 384 authorisations granted (55 % of the total number of authorisations).

[16] See Годишен доклад за дейността на Окръжен съд – Бургас, и районните съдилища от Бургаски съдебен район за 2010 г. [2010 Annual Activity Report of the Burgas District Court and the Regional Courts within its Geographical Jurisdiction]. According to the report, 255 of the requests were for natural persons and eight requests were for sites for the purpose of establishing the identity of persons engaged in criminal activity. Special intelligence means were deployed in respect of 263 persons, of whom 16 requested to be wiretapped because of threats against their life and property giving their consent in writing in line with Article 12 (2) of the Law on the Special Intelligence Means. Of the 697 authorisations granted, most were requested for detection of the following offences: organised criminal group (Article 321 of the Criminal Procedure Code); offences against the monetary and credit system; robbery, theft, blackmail; Article 308 (2) of the Criminal Code; fraud; money laundering; cross-border smuggling; offences against the administration of government; bribery etc.).

[17] Отчетен доклад за работата на Окръжен съд – Хасково – 2010 г. [2010 Activity Report of the Haskovo District Court].

90.6 %. These trends are attributed to various factors: the 22 % increase from 2009 of the number of newly instituted cases of significant public interest; the invigoration of the activity of the law-enforcement authorities in countering organised crime; or the increased complexity of serious crime (increased number of participants, higher degree of organisation and more sophisticated means used by offenders to impede and neutralise their detection).[18]

Along with these objective reasons, however, one cannot ignore the temptation of the investigating authorities to resort more frequently to collection of evidence by special rather than by conventional means of proving.

Risks of the growing use of special intelligence means

"The figures for 2010 and the tendency of a substantial increase in the special intelligence means used invite the alarming conclusion that this method of proving is used all too often in the practice of investigation rather than as an exception as provided for in the law. Due to the excessive use of special intelligence means, the investigating authorities may lose interest in performing other investigative actions and prerequisites emerge for abuse of the data collected by special intelligence means. Therefore, it is imperative to review the legislation in terms of the list of offences in respect of which it is admissible to collect evidence by special intelligence means. A legislative revision is needed to tighten the control over the use of special intelligence means, including a restriction of their use through economic levers (imposing a limit on the number of special intelligence means and levying a fee on the use of such means) and to improve the effectiveness of the control, including the control exercised by the court, over the destruction of the physical means of proof prepared if they cannot be used in the investigation."

Source: Report on the Application of the Law and on the Operation of the Prosecution Service and of the Investigating Authorities in 2010.

The lack of consolidated statistics based on uniform criteria and covering criminal proceedings in their entirety makes it impossible to arrive at an exact figure for the success rate of the application of special intelligence means.

4. Problems in the practice of application of special intelligence means

The low productivity of the use of special intelligence means, as well as the numerous abuses and violations, are due to problems of various nature: flaws

[18] See Доклад за прилагането на закона и за дейността на прокуратурата и на разследващите органи през 2010 г. [Report on the Application of the Law and on the Operation of the Prosecutor's Office and of the Investigating Authorities in 2010], (http://www.prb.bg/main/bg/Information/2076/).

in the legal framework and its synchronisation, exceedingly broad range of offences to which special intelligence means are applicable, the behaviour and the insufficient professional qualification of some of the participants in the special intelligence means deployment procedure, lack of reliable safeguards against abuses and violations of fundamental human rights and of a comprehensive and effective system of independent control over the use of special intelligence means.

- **Problems in connection with the operational techniques used as special intelligence means**

The current version of the law provides for several operational techniques that can be used as special intelligence means: surveillance, wiretapping, following, penetration, marking and monitoring correspondence and computerised information, controlled delivery, trusted transaction, and investigation through an undercover officer.

The most frequently used technique is **wiretapping**,[19] defined as "aural or another manner of acquisition of oral, telephone or electronic communication of persons under surveillance through the use of technical devices" (Article 6 of the *Law on the Special Intelligence Means*). As evident from the definition, wiretapping may be implemented using **various technical devices**, whereas the authorisation is granted only for the operational technique and not for the technical device. This circumstance, however, is not always taken into consideration by the courts and some courts **do not admit as evidence** the information, which was collected through the authorised operational technique but without indicating the technical devices to be used. The Supreme Court of Cassation does not share this approach to the assessment of the evidence, describing it as not conforming to the effective legal framework and denying the prosecutor's office the opportunity to argue the case for the prosecution[20]. The future legal framework, however, should require that the request and the authorisation for the use of special intelligence means must specify both the operational technique and the possible technical devices because the latter are

[19] According to the prosecutor's office, the operational techniques most frequently used in 2010 were wiretapping (58.1 %), surveillance (20.7 %) and following (19.7 %). See Доклад за прилагането на закона и за дейността на прокуратурата и на разследващите органи през 2010 г. [Report on the Application of the Law and on the Operation of the Prosecutor's Office and of the Investigating Authorities in 2010] (http://www.prb.bg/main/bg/Information/2076/).

[20] Judgment No. 516 of 16 December 2009 in Criminal Case No. 539 of the Criminal College, Third Criminal Department of the Supreme Court of Cassation, for the Year 2009.

also part of the special intelligence means and they, too, restrict rights and are susceptible to abuse.

Wiretapping is an important technique for the detection of the criminal activity and the participants in the group. The application of this technique, however, involves a number of risks. Firstly, not all recordings but only those pointing to the commission of an offence may be presented before the court. Secondly, the court cannot determine whether an offence has been committed only on the basis of the transcripts outside the overall context. Thirdly, the recordings of intercepted conversations can often create a wrong impression because they are taken out of context: it is not known what the persons discussed before the recorded portion, the intonation is difficult to apprehend etc. The court must require and listen to the full recordings instead of reading the transcripts submitted by the prosecution, but even in this case some of the risks cannot be avoided. In reality, there are also problems with proving the actual identity of the party talking on the telephone because mobile phone SIM cards often cannot be linked directly to the accused parties, the accused cannot be induced to talk so as a voice identification expert examination could be performed, etc. That is why wiretapping should rather provide the investigating authorities with clues to the collection of other evidence and not be used as a principal method, as is the prevailing practice at present.

The *UN Convention against Transnational Organized Crime* recommends the use of special investigative techniques, such as controlled delivery, electronic and other forms of surveillance, as well as undercover operations. Other international instruments and acts of the EU also call attention to the significance of these methods for the collection of evidence. In a number of countries, their deployment produces good results in the detection of organised criminal groups and their leaders. In Bulgaria, the new operational techniques and types of special intelligence means: **investigation through an undercover officer, controlled delivery and trusted transaction**, introduced for the first time in the new *Criminal Procedure Code* and defined in the *Law on the Special Intelligence Means*, still lack a detailed and systematic regulation and are not used sufficiently.

The *Law on the Special Intelligence Means* (Article 10c) defines an undercover officer as "an officer of the respective services under the Law on the Ministry of Interior or the Law on the Defence and Armed Forces, or an officer of the National Intelligence Service, who has been empowered to establish or to maintain contacts with a person under surveillance in order to obtain or to discover information about the commission of a serious intentional

offence and about the manner in which the criminal activity is organised". The *Law on the Ministry of Interior* and the *Law on the State Agency for National Security* state that only officers designated by the heads of the respective agencies may perform the functions of undercover officers.

The use of undercover officers by the Ministry of Interior is described in greater detail in a *Council of Ministers Ordinance on the Arrangements for the Use of Undercover Officers by the Ministry of Interior*. The Ordinance formulates the purposes of this technique in broader terms than the definition in the *Law on the Special Intelligence Means*, *viz.* use not only for the purposes of collecting evidence in criminal procedure but also for prevention, as well as for activities related to national security. The Ordinance also describes the functions of the officer for the achievement of these purposes which, in most general terms, boil down to "infiltrating the entourage or the circle of persons who present a lawfully established interest to the authorities of the Ministry of Interior, using their cover to implement surveillance of such persons, to obtain data about planned, prepared, committed or completed serious intentional offences and for the purposes of protection of national security" [Article 5 (1) of the Ordinance].

The still scanty publications on this subjects[21] call attention to the insufficient and incomplete framework of the investigation through an undercover officer: the lack of rules governing the powers of the officers, the authorised and unauthorised activity, the grounds for release from criminal responsibility for an offence committed upon deployment of this operational technique, the express prohibition of the provocation to commit an offence, the link with the operational technique of trusted transaction and the consequences of this etc.

Statistics show that, albeit on an incomparably smaller scale than the rest of the special intelligence means, investigation through an undercover officer together with trusted transaction is already applied. The official data, as far as available, vary but a study conducted by the RiskMonitor Foundation found that the district courts countrywide granted a total of 35 authorisations for 2009, of which 15 were granted by the Plovdiv District Court and 14 by the

[21] Паунова, Л. и П. Дацов, Организирана престъпна група [Paunova, L. and P. Datsov, Organised Criminal Group], Ciela, Sofia, 2010, pp. 170-185; Смедовска-Тонева, Р., Специални методи за борба с организираната престъпност – агенти под прикритие [Smedovska-Toneva, R., Special Methods to Combat Organized Crime – Undercover Agents], RiskMonitor Foundation, Sofia, 2011.

Sofia City Court, whereas the number reached 63 in 2010, including 47 granted by the Sofia City Court.[22]

Since its introduction, the deployment of the operational technique of "investigation through an undercover officer" has given rise to controversy. According to one school of thought, this is an extraordinary means, which must be resorted to only as an exception, either to complement other means of proof or when proving by other means is impossible,[23] but it is nevertheless a suitable instrument for the detection and prevention of serious offences and for the collection of inside information admissible in the criminal procedure. According to the opposite views, this figure of undisclosed identity, transplanted from the criminal procedure of other countries, does not conform to the Bulgarian context and its use in this country leads to the collection of inadmissible evidence instead of facilitating the collection of evidence.

Because of the still rare use of this instrument in practice, however, the legal framework is the main target of criticism for the time being. Part of this criticism concerns Article 173 (3) of the *Criminal Procedure Code* which, as amended in 2010, provides that the declaration of the undercover officer must state the personal identification number assigned to him or her by the entity which arranges and implements the investigation through an undercover officer. The unavailability of personal data makes it impossible for the court, which authorises the use of this operational technique, to establish that the declaration originates precisely from the person who signed it. To this end, it is proposed that data identifying the person be included in the declaration, while only the identification code be entered into the register of requests and authorisations, which is not open to public inspection. At present the information identifying the undercover officer may be provided to the supervising prosecutor and to the court only after a reasoned written request to the Minister of Interior or the Chairperson of the State Agency for National Security or, respectively, their empowered deputies [Article 123a (3) of the *Criminal Procedure Code*].

Another shortcoming of the current legal framework is the short period for deployment of special intelligence means, which applies to this technique as well. Due to its specificity, however, a longer period needs to be provided for,

[22] See Смедовска-Тонева, Р., Специални методи за борба с организираната престъпност – агенти под прикритие [Smedovska-Toneva, R., Special Methods to Combat Organized Crime – Undercover Agents], RiskMonitor Foundation, Sofia, 2011. p. 25.

[23] Паунова, Л. и П. Дацов, Организирана престъпна група [Paunova, L. and P. Datsov, Organised Criminal Group], Ciela, Sofia, 2010, p. 170.

so that this technique could achieve its intended purpose. At present the undercover officers, if at all used, are often withdrawn at a very early stage of the investigation. As soon as a charge is initially brought, the officer is practically withdrawn because otherwise he or she, too, will have to be arrested. And once withdrawn, the undercover officer becomes practically unusable because his or her participation is already exposed. On the other hand, if not withdrawn without being charged or arrested together with the rest of the participants, the risk of his or her exposure is heightened considerably because suspicions arise why his or her conduct was left without consequences. In principle, when a decision is made to use an undercover officer in a particular investigation, this officer must be left until the end, until the detection of the entire group. This may sometimes take a long time, and if bringing charges is rushed, as is the practice in Bulgaria, the chances of the investigation getting to the rest of the participants recede.

Some operational techniques are used without a clear idea about their essence and how to distinguish them from the physical means of proof prepared upon their deployment. Usually, case law helps overcome this tendency, reconcile the conflicting case law of the lower courts, and close gaps in the operation of the authorities deploying the special intelligence means with a view to collecting admissible evidence. Thus, Judgment No. 809 of 7 January 2010 in Civil Case No. 15538 of the Civil College, First Civil Department of the Supreme Court of Cassation, for the Year 2008, confirms that marked money is not special intelligence means. Referring to Article 2 (1) and (3) of the *Law on the Special Intelligence Means*, the Court emphasises that "the marking of the money is an operational technique employed as a special intelligence means", whereas the money itself is physical evidence prepared through the use of this technique. Therefore, the Court holds that the use of marked money in a police operation is not subject to the rules applicable to the special intelligence means.

On the other hand, the case law of the Supreme Court of Cassation contains some debatable solutions to the problems arising from the disparate interpretation and application of the legal framework of special intelligence means. Judgment No. 504 of 22 November 2005 in Criminal Case No. 1072 of the Third Criminal Department of the Supreme Court of Cassation for the Year 2004 calls attention to the two categories of written authorisations by the respective authorities regarding the procedure, manner and modalities of the use of special intelligence means, whose obtaining is mandatory but which arguably have different legal relevance to the valid collection of evidence. The

Supreme Court of Cassation confirms that the availability of an authorisation from the court at the time of collection of physical means of proof through special intelligence means makes this evidence absolutely valid. At the same time, while emphasising that to be legally conforming, the collection of physical evidence by special intelligence means must have its logistical support ordered before the commencement of their use, the Court admits a departure from this requirement. The Supreme Court of Cassation holds that if an authorisation of the Minister of Interior, "which has the sole objective of ensuring the technical execution of the first authorisation", was issued after the commencement of the use of special intelligence means, the breach is insignificant provided that the use conforms to the period and type of special intelligence means determined in the court authorisation. "Whether this authorisation will coincide in time or will succeed the authorisation by the authority under Article 111a of the Criminal Procedure Code, this will not vitiate the validity of the action itself: the collection of physical means of proof through special intelligence means, as long as this authorisation is available, has been granted by the Minister of Interior, and the step was performed by the technical directorates of the Ministry of Interior provided for in Article 20 of the Law on the Special Intelligence Means" An argument supporting this reasoning is found in Article 17 of the *Law on the Special Intelligence Means*, which allows for the commencement of the deployment of special intelligence means in urgent cases immediately after obtaining the written authorisation from the court, of which the Minister of Interior or the deputy minister authorised in writing by that Minister must be notified immediately. This position, expressed on a specific case, rejects the thesis that the lack of a preceding order by the Minister vitiates the evidence. This position, however, should not be made universally applicable, thus asserting a practice of non-compliance with the law. The urgent case is an exception, which must not become a rule. Besides this, even in an urgent case validation by the court is required within 24 hours, whereas the interpretation of the Supreme Court of Cassation does not impose such a restriction. Once the law obliges the court to decide on the request immediately, it would justified that the Minister of Interior (or the deputy minister authorised by that Minister) and the Chairperson of the State Agency for National Security (or the deputy chairperson authorised in writing by that Chairperson) should also issue an order with the least possible delay after the authorisation is obtained. The exception, which the law admits, applies only to the urgent cases and the imminent risks discussed above.

Achieving better results in the investigation and collection of evidence of organised criminal groups requires more sophisticated methods, including the introduction of new techniques using technological advances, such as GPS tracking.

- **Problems in connection with the control over the use of special intelligence means**

The cases of abuse of special intelligence means and the rows surrounding these cases, which have recently become public, as well as the broad-scale use of such means even when this is not necessary, brings to the fore the problem of control over their application.

In a new Chapter Four A, the *Law on the Special Intelligence Means* describes the control and monitoring of special intelligence means. The control as to the lawful use of special intelligence means is a responsibility of by the heads of the competent entities, which deploy them (Article 34a), i.e. the control is internal rather than independent.

Since the end of 2009[24], amendments entrusted monitoring to a committee of the National Assembly. This is a standing subcommittee with the Legal Affairs Committee and is supposed to implement the parliamentary oversight and monitoring provided for in Article 34b of the *Law on the Special Intelligence Means* and Article 261b of the *Law on the Electronic Communications.* The parliamentary oversight includes the procedures for the authorisation, deployment and use of special intelligence means, the retention and destruction of the information obtained by such means, as well as the protection of citizens' rights and freedoms against unlawful use of special intelligence means. The committee was elected by the National Assembly on 22 December 2009 and operates according to internal rules adopted by the National Assembly on 11 February 2010. Annually, on or before 30 April, the subcommittee presents an activity report to the Legal Affairs Committee, which must consider the report and lay it before the National Assembly not later than 31 May. Although the subcommittee has been operating for a relatively short period of time and in almost complete secrecy, usually meeting behind closed doors, the prevalent opinion is that it lacks the capacity to perform the duties assigned to it by the law. The subcommittee members themselves also share this opinion. At the same time, the discussion about the need to set up

[24] The amendments repealed the provisions inserted in 2008, which entrusted monitoring to a National Bureau for Control over the Special Intelligence Means.

effective mechanisms for tightened control has not yet produced tangible solutions.[25]

As the sole authority empowered to grant authorisations, the court determines whether the legal prerequisites apply and whether the request for the use of special intelligence means in respect of particular person(s) suspected of the commission of an offence is well founded. The court must ascertain that the relevant circumstances cannot be established in another manner or their establishment involves excessive difficulties. Deployment of special intelligence means is inadmissible without such an examination. In most cases, however, the court is not familiar with the case in detail, does not have the operational file at its disposal, and its assessment is based only on the facts and circumstances stated by the specialised services or by the prosecutor and on their conclusion that another technique is impossible to deploy. This may affect the objectivity of the court's judgement. This is probably the reason for the small number of refused authorisations.[26] There is a widespread opinion among judges that the reasoning of the requests is very often perfunctory, which impedes the examination. The rules of jurisdiction are also often circumvented in order to secure an "amenable" court or judge to grant the authorisation. Since no other control mechanism exists, it is within the powers of each court to reject requests submitted in breach of the rules of jurisdiction.[27] The court may also be misled – either because of the ignorance of those services and authorities or deliberately, in a bid to gain easier access to the use of special intelligence means or even to use them for a purpose other than intended. The rows in 2011 alone (over the unauthorised wiretapping of the Director of the National Customs Agency and the cases of massive-scale

[25] The amendments to the Law on the Special Intelligence Means regarding the control over the use of special intelligence means, moved by opposition parties (the Bulgarian Socialist Party and the Movement for Rights and Freedoms), were voted down on 1 June 2011 by the government majority, which pledged to come up with a draft of its own. The rejected motion provided for the establishment of a seven-member public council with the Minister of Justice to control the retention and destruction of information obtained by special intelligence means, exclusion of the supervising prosecutors from the range of authorities authorised to request special intelligence means etc.

[26] According to the 2010 Annual Activity Report of the Burgas District Court, the refusals to deploy special intelligence means, including the refusals of requests to extend the period for their use, are most often due to unjustified necessity.

[27] See Доковска, Д., Изказване на кръгла маса "Необходими законодателни промени в нормативната уредба на СРС [Dokovska, D. Statement at a Round Table on Legislative Amendments Needed in the Statutory Framework of Special Intelligence Means], in Praven Svyat magazine, 21 February 2011 (http://www.legalworld.bg/show.php?storyid=22619).

wiretapping without confirmation that deployment of this operational technique was warranted and necessary) are symptomatic in this respect.
To have an impartial and effective *ex ante* control by the court, the authorities empowered to request authorisation must act responsibly, professionally and under an enhanced internal control system. This is all the more imperative considering that the court is excluded from the subsequent control over the deployment of special intelligence means and their use for the preparation of physical evidence. The court does not need to be charged with the overall control, but once it has granted authorisation for the use of special intelligence means, it must be afforded access to the information about the particular case, so that it would be clear at any time thereafter what has been requested and what has been used. In this connection, it is necessary to develop further the keeping of a **register of the requests submitted and the authorisations granted**, describing in detail the circumstances to be recorded in the register, the time limits, the responsibility for keeping and maintaining this register, as well as safeguards for its *bona fide* handling. This is all the more necessary because, according to the current framework, the request itself is sent back to the requesting authority,[28] and the register is not open to public inspection. This necessity is obvious in respect of discontinuing the deployment of special intelligence means. In such case, the law provides that the court, which granted the authorisation, be given an immediate reasoned notice in writing and order the destruction of the information gathered unless it will be used for the preparation of physical means of proof [Article 175 (6) of the *Criminal Procedure Code*]. The court, however, is not vested with powers to exercise subsequent control over compliance with the order issued and cannot impede a possible misuse of undestroyed information.
The shortcomings of the Bulgarian model of using special intelligence means, and especially those affecting human rights, have prompted the lodging of applications against Bulgaria at the European Court of Human Rights and obtaining judgments against the State. These defects are systematised in the Judgment delivered on 28 June 2007 in a case, which originated in application no. 62540/00 lodged by the Association for European Integration and Human Rights and Mihail Ekimdzhiev. The Court held that Bulgaria had violated Article 8, Article 13 and Article 6 § 1 of the Convention for the Protec-

[28] It is also debatable whether this provision should be revised as well and that the court should keep a copy of the request in compliance with the appropriate confidentiality arrangements.

tion of Human Rights and Fundamental Freedoms.[29] The Judgment found that the persons subjected to surveillance are not notified of this fact at any point of time and under any circumstances and the lack of information (after the Supreme Administrative Court held that the information is classified) prevents them from seeking redress for unlawful interferences with their rights. The Court concludes that **Bulgarian law does not provide sufficient guarantees against the risk of abuse** in the use of special intelligence means and does not provide effective remedies against their improper use and for redress for unlawful interference with human rights. Such mechanism of apprising persons where their communications and movements have been unlawfully monitored exists in a number of other European countries. The other important conclusion is that Bulgarian law **does not contain a sufficiently effective apparatus for controlling** the use of special intelligence means. The European Court of Human Rights sees a risk of abuse of authority if the overall control is entrusted solely to the Minister of Interior, who not only is a political appointee but is directly involved in the commissioning of special intelligence means, and neither the Minister nor any other official is required to regularly report to an independent body or to the general public of the overall operation of the system or on the measures applied in individual cases. In its Judgment (paragraph 87), the Court, referring to some of its earlier judgments, cites the example of independent control bodies existing in other countries: a special board elected by the Parliament, an independent commission or a special commissioner holding or qualified to hold high judicial office, or a control committee consisting of persons having qualifications equivalent to those of a Supreme Court judge. The court argues for the need of independent external control. Executing the Judgment of the Court, legislative amendments were undertaken and led to the establishment of the parliamentary subcommittee. Its brief practice demonstrates, however, that this solution does not adequately address the deficiencies discussed.[30]

In conclusion, organised criminal activity includes offences, which are more complicated, involve a larger number of participants, participants have various

[29] See Case of Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria (Application no. 62540/00), Judgment of 28 June 2007, European Court of Human Rights.

[30] The subcommittee's first report does not provide information about the number of citizens who have been notified that they had been unlawfully subjected to special intelligence means. The members of the subcommittee admit that it does not have the capacity to verify the lawful deployment of special intelligence means or to inform the citizens (for further details, see Praven Svyat magazine, news, http://www.legalworld.bg/show.php?storyid=23327).

roles etc. This specificity has an impact on the process of investigation and proving and usually requires more time and resources than conventional crime. Apart from the adequacy of the legal framework, the success of proving such criminal activity also depends on a whole range of interconnected factors: professionally knowledgeable and experienced investigating authorities, skilled in collecting relevant and admissible evidence, the professionalism and integrity of judges, prosecutors and defence counsel, the guaranteeing of the fundamental principles of criminal procedure and ensuring the right to defence, as well as the availability of up-to-date and sufficient technical equipment and logistics for the entire process.

The case law of organised criminal group cases built up in Bulgaria so far, still scanty as it is, creates the impression that the evidence collected is quite often not convincing and sufficient enough to support sentences of conviction corresponding to the case for the prosecution. The detection and proving of the criminal activity of organised criminal groups reveal a number of problems.

Special intelligence means, interrogation of protected witnesses, search and seizure etc. are the methods for the collection of evidence most often used in organised crime cases. The pre-trial authorities do not employ each and all envisaged procedural methods for collecting evidence. The most commonly used methods are wiretapping, as well as surveillance and following. Investigation through an undercover officer and controlled delivery are resorted to much more rarely. At the same time, the lack of independent control over the deployment of special methods spells risks of unlawful application of these methods and use of the information collected.