LEGAL ISSUES REGARDING SECRET COMMUNICATION SURVEILLANCE IN SERBIA

Milosevic Milan[1], Matic Goran D. [2]
[1]ALFA University, Belgrade, Faculty for Education of the Executives,
Novi Sad, Serbia
milanmilos@gmail.com
[2] Office of the Council on National Security and Classified Information Protection,
Republic of Serbia

***Abstract**: The measures regarding secret communication surveillance are an effective tool for the protection of national security and counter the most severe forms of criminality. At the same time, they represent a possible prevention of new and very dangerous criminal acts, which, due to its complexity, a high-level of conspiracy of the perpetrators and subsequent potential impact on the regular course of the criminal proceedings, cannot prove using usual process means. Therefore, the practical application of these measures is related to the procedural requirements based on the principles of proportionality and subsidiarity, including the approval and the control of the court.*

***Keywords**: communications, secret surveillance, permitting, legal proceedings, the national security*

1. INTRODUCTION

In the broadest sense, the measures regarding secret communication surveillance include acoustic surveillance of premises, vehicles and the man himself; acoustic surveillance of telephone and radio communications (fixed, mobile and satellite phones); locating via text messaging on the mobile phone network, etc. In practice, these measures are usually based on the interception and recording of telephone and other conversations. On the other hand, the secret surveillance over communication can be operational (administrative), and judicial. The administrative is the one implemented in order to preserve the national security of the country, while the court one is conducted to obtain evidence for criminal proceedings. Therefore, communication surveillance can be effectively used in preventive and repressive purposes.

The legal basis for the implementation of surveillance is generally associated with Article 20 of Constitution of the Republic of Serbia from 2006, which stipulates the conditions under which it is possible to exercise limits for human and minority rights by the competent authorities. The specific provisions of application of the measures for the secret com-

munication surveillance in Serbia can be found in the Code of Criminal Procedure, the Law on Organization and Jurisdiction of Government Authorities in combating organized crime, corruption and other serious offenses, the Law on Organization and Jurisdiction of Government Authorities in War Crimes , the Police Act, the Law on the Security Information Agency and Military Intelligence Agency Act and the Military Security Agency.
The main subjects of state communications surveillance in Serbia are the police (MUP SBPOK) and internal security services (BIA, VBA); at whose request the judicial authority approve the use of secret surveillance in a concrete case. Thus, for example, the War Crimes Chamber in Belgrade in 2005 approved measures for secret surveillance for a total of 89 persons, i.e. 352 telephone numbers. It is interesting that the applicant for the determination of such measures in the vast majority were BIA, while VBA and SBPOK MUP done it only in a few cases.[1]

2. JUDICIAL COMMUNICATION SURVEILLANCE

Judicial communication surveillance means interception of calls defined by the rule, as investigative activity in the course of criminal proceedings by the judicial authorities. In countries where appropriate legislation was previously adopted, the practical application of this measure is related to the procedural requirements based on the principles of subsidiarity and proportionality. Specifically, in the UK, Hungary, Turkey and other countries, a so-called judicial surveillance is possible only if there is serious doubt that organized crime or other serious crime is committed or planned to commit, and provided that it is not possible to investigate this using other, standard methods and tools (witnesses, expert testimonies, documentary evidence, etc.)
At the same legal principles is based an action of supervision and communication with other technical devices and optical recording, which in our criminal procedure legislation was introduced by the Code of Criminal Procedure from 2001. Article 232 of actual CCA provides that the investigative judge, based on the written and reasoned request of the prosecutor, to police and security services can be ordered surveillance and recording of telephone conversations and other communications or other technical devices and optical recording entities for which there is a reasonable doubt that either alone or with other people committed crimes against the constitutional order or security, against humanity and international law, with elements of organized crime, bribery, extortion and abduction. The offenses with elements of organization, a legislator in Article 232 of the CCA expressly counts forgery and "money" laundering, illicit production and trafficking of narcotic drugs, illicit trafficking in weapons, ammunition or explosive substances and human trafficking. To order the communication surveillance, investigative judge needs, according to the Article 232 of CCA, just grounds to suspect that a person has committed the offense, i.e. to have a person who is suspected of committing such act.
Provisions of Articles 166-170 of the CCA from 2011, whose application is delayed until mid-2013, however, in particular procedures for organized crime and war crimes apply from the 15 January 2012, and this measure is intended as a proof of the actions called

1 Dilparić M., „*Mera prisluškivanja u postupcima za krivičnih dela ratnih zločina* ", Nova rešenja u krivičnom zakonodavstvu i dosadašnja iskustva u njihovoj primeni, Udrženje za krivično pravo i kriminologiju, Zlatibor, 2006, p. 440

"surveillance over communication." It means the measures of secret surveillance in the narrow sense ("monitoring and recording of communications is done via telephone or other technical means or surveillance over electronic or other address of the suspect"), including "seizure of letters and other mail." This also includes the collection of data through the acquisition and analysis of the outgoing-incoming calls listing from a subscriber's phone number (so-called, metering).[2]

Application of "the secret surveillance over communication" is possible for organized crime and war crimes, but also for the acts of a political crime (assault on the constitutional order, incitement to violent overthrow of the constitutional order, diversion, sabotage, espionage, disclosure of state secrets, inciting national, racial and religious hatred and intolerance, conspiracy to unconstitutional activity, and others), and for the following offenses: aggravated murder, kidnapping, acquisition and possession of pornographic material and usage of a minor in pornography, extortion, money counterfeiting, money laundering, illicit production and trafficking of drugs, illegal manufacture, possession, carrying and sale of arms and explosives, illegal border crossing and smuggling, abuse of power, trading in influence, bribery, human trafficking, and crimes in Article 98 paragraphs 3 – 5 of the Data Secrecy Act.

The same goes for crime prevention and disruption of proof, if done in conjunction with some of the foregoing offenses. Finally, the secret communication surveillance, under certain conditions, can be applied to cyber crime offenses (unauthorized use of copyright works and objects of related rights, damage to computer data and programs, computer sabotage, computer fraud and unauthorized access to a protected computer, computer network and electronic data processing).

Postal, telegraph and other companies and individuals registered for the transmission of information have the obligation to allow the execution of these measures to competent authorities (police, BIA, VBA). Such obligation of public telecommunications operators stems from the provisions of Articles 54 and 55 of the Telecommunications Act, and the provisions of Article 168 of the CCA from 2011. In addition, it is important to point out that the provisions of Article 233; Paragraph 4 of CCA stipulates that the material obtained contrary to the provisions set forth above, and without the order of the procedure cannot be used to make a court decision. It is believed that this provision in the CCA of Serbia introduced elements of evidence concept known as "the fruit of the poisonous tree," which is very influential in the Anglo-American procedural law.[3]

3. OPERATING (PREVENTIVE) COMMUNICATION SURVEILLANCE

According to the position of the doctrine and practice of the European Union, operational and administrative communication surveillance (wiretapping and recording of telephone and other conversations) usually security services implement, and judicial or other authorities determine it, to protect the security and defense of the country. In Serbia, this

[2] Mijalković S.; Manojlović D., „*Pribavljanje listinga telefonskog pretplatničkog broja građanina - kontroverze u radu nacionalnih sistema bezbednosti*", Strani pravni život, broj 2/2008, pp.150-168.

[3] Škulić M., *Organizovani kriminalitet Pojam i krivičnoprocesni aspekti*, Dosije, Beograd, 2003, pp. 252-254

communication surveillance can be determined exclusively by the judicial authorities and implemented by the security services - BIA and VBA.

Articles 13 and 15 of the Law on the Security Information Agency provide a the possibility of deviation from the principle of inviolability of letters and other correspondence from the Security-Information Agency (BIA), if this is necessary for security reasons. Under these provisions, the proposal of the Director of BIA, the implementation of measures must be approved by the decision of the President of the Supreme Court of Serbia or by the authorized judge within 72 hours of submission. The approved measures may apply during six months and not exceeding twelve months.

Once the reasons of urgency demands it, especially in cases of domestic and international terrorism, a deviation from regular procedures may be ordered by the director of the BIA, with the prior written approval of the President of the supreme court of Serbia or authorized judges. After the decision, the Director of BIA shall submit a written proposal within 24 hours of receiving the approval of the President of the supreme court of Serbia or an authorized judge, to make a decision. The decision to continue implementing appropriate measures or to suspend them is taken within 72 hours of the submission of the proposal, i.e. decision on suspending the measures must be explained in writing.

Article 30 and 31 of the Security Services Act from 2002 prescribe the use of special means and methods by VBA. Certain means and methods include the monitoring and surveillance of individuals with the use of technical means for documenting and monitoring of mail and other means of communication. Communication surveillance is justified, if the task under Article 8 of the Law on Security Services cannot be performed by applying the provisions of Article 28 of the above-mentioned law (relating to the collection of data) or any other way that would not require a disproportionate risk and endangering people's lives. Only in this case, VBA can use special tools and methods for collecting secret information, which temporarily limit the constitutional and statutory rights and freedoms, and relate to the control of the means of communication among other things.

For administrative surveillance, the task of Article 8 relate to intelligence and other activities of foreign agencies, organizations and persons directed against the Serbian Army and the Department of Defense, as well as domestic and international terrorism and subversive activities directed against the commands, units and institutions of the Army and Department of Defense. Special tools and methods VBA could apply upon the approval of the Court, under the conditions and in the manner prescribed by the CCA. The proposal for the implementation of measures submits the Director of VBA or a person authorized by him/her.

According to the Article 12 of the Law on VBA and VOA from 2009, which was recently renewed, VBA, as in the previous law, could independently perform secret electronic surveillance over IT and telecommunications systems without access to their content, and to collect data on telecommunications traffic and location of the users (metering). For the application of these measures, the Director of VBA or a person authorized by him was in charged, and there was an obligation to keep proper records.

However, the Constitutional Court with its decision made on 24 May 2012, cancel this controversial application of the provisions of Article 12, Paragraph 1 point 6) and Paragraph 13 of the Law on VBA and VOA, noting that this differs from the guaranteed right to privacy of communications and obligations for court to decides about this deviation, all in accordance with the views expressed in the practice of the European Court of Human

Rights.[4] In the meantime, this attitude was embedded in the text of the Law on Amendments and Supplements to the Law on VBA and VOA, which was adopted in early 2013, so that VBA can now apply metering only to the extent of the reasoned decision of the Supreme Court. In addition, VBA in terms of the article 12, item 6) to 8) in relation to Article 14 of innovated Law on VBA and VOA, maintained the possibility of the application of other methods of communication surveillance, but only with the approval of the Supreme Court of Appeal.

Regarding the protection of the citizen's right to privacy, it is considered that, although the Law on the Security Information Agency does not contain adequate provisions, a citizen has the right to be informed about the measures regarding the secret communication surveillance. It is believed that the method of treatment in these cases is not regulated by the Security Intelligence Agency - BIA, but the Law on Free Access to Information of Public Importance, in terms of Article 5, paragraph 2 of Article 11 of this Law.[5]

Particularly interesting is the question of the ability to monitor communications by the Ministry of Internal Affairs (MUP). We are talking about "targeted measures of search", which criminal police conducts in the form of administrative surveillance, while according to the content of these measures it is much closer to the "classic" wiretapping. The provision of Article 83 of the Police Act provides the application of measures of communication surveillance by authorized police officers, and the requirements, competence regarding decision-making and its implementation. In particular, stipulates that in order to arrest and bring before the competent authority of the person who is reasonably suspected of having committed an offense for which the law prescribes a prison sentence of four years or more and for whom international arrest warrant was issued, and when the police cannot realize capture and arrest using other measures, i.e. if something like that is related to disproportionate difficulties, it is possible to take some of the special investigation methods established by provisions of the CCA.

The measures of the targeted search, on the written and reasoned proposal of the Director of the police, approved by the decision of the President of the Supreme Court of Serbia or authorized judge within 72 hours of submission. The approved measures typically can be implemented in period of six months and not exceeding twelve months. Once the reasons of urgency demands that, a departure from regular procedures, can be approved by the President of the Supreme Court of Serbia or authorized judges.

After making the decision, chief of police shall submit a written proposal within 24 hours of receiving the approval of the President of the Supreme Court of Serbia or an authorized judge, in making a decision. The decision to continue implementing appropriate measures or their suspension, must be taken within 72 hours of the submission of the proposal i.e. the decision to suspend the measures must be explained in writing. Data collected on measures of targeted search cannot be used as evidence in criminal proceedings, and once the target search is finished, must be delivered to the president of the supreme court of Serbia or an authorized judge, who shall destroy them, and shall make a record.

[4] For example, the decisions in the cases of Klass and Others v. Germany from September 6, 1978. Malone v. the United Kingdom, August 2, 1984, etc.

[5] Ivošević Z., „Prisluškivanje", Izbor sudske prakse, broj 9/2005, p.26

4. RESUME

Measures of secret communication surveillance are an effective tool for the protection of national security and counter the most severe forms of criminality. At the same time, they represent a possible prevention of new and very dangerous criminal acts, which, due to the complexity of offenses, the high level of conspiracy of the perpetrators and subsequent potential impact on the regular course of the criminal proceedings, which cannot be proved by the usual process means.

The main subjects of state communication surveillance are the police and the security services (BIA, VBA), which use them for the preservation of national security or protection of other interests. It should be noted that the jurisdiction of the government entities sometimes overlap and hampers the efficiency and effectiveness of legal regulation. In addition, to the legislature is always easier to define communication surveillance for the needs of police and court proceedings, then when it comes to internal security services and their work to protect national security[6]. The question of the application of communication surveillance by the private security sector, which is beyond the control of the competent judicial or other authority is also interesting. For example, there is no law that regulates the work of detectives in Serbia.

Especially interesting is the question of implementation of control measures regarding communication surveillance. We think that in the future, in addition to existing remedies, it is going to be necessary to find other ways to control the implementation of these measures by the executive, judicial and legislative branches. This system of supervision and control by the various government bodies (checks and balances), would completely rule out or minimize the possibilities of misuse and arbitrariness in their application for the needs not envisaged by the law (personal, economic, etc.).

BIBLIOGRAPHY:

[1] Dilparić M., "Mera prisluškivanja u postupcima za krivičnih dela ratnih zločina ", Nova rešenja u krivičnom zakonodavstvu i dosadašnja iskustva u njihovoj primeni, Udrženje za krivično pravo i kriminologiju, Zlatibor, 2006.
[2] Ivošević Z., "Prisluškivanje", Izbor sudske prakse, br. 9/2005.
[3] Ilić G., "Odstupanje od nepovredivosti tajne pisma i drugih sredstava opštenja", Revija za kriminologiju i krivično pravo, br 1/2003.
[4] Mijalković S.; Manojlović D., "Pribavljanje listinga telefonskog pretplatničkog broja građanina - kontroverze u radu nacionalnih sistema bezbednosti", Strani pravni život, br. 2/2008.
[5] Milosavljević B., Prisluškivanje - naši propisi i evropski standardi, www.ccmr-bg.org/analize/org
[6] Milošević M., «Mere ciljane potrage", Revija za bezbednost, br. 12/2009.
[7] Motto C.; June D., Undercover, CRC Press, Boca Raton, 2000.
[8] Paoli L., Fijnaut C., «Organized Crime and Its Control Policies», European Journal of Crime, Criminal Law and Criminal Justice, No. 3/2006.
[9] Škulić M., Organizovani kriminalitet: Pojam i krivičnoprocesni aspekti, Dosije, Beograd, 2003.

[6] Milosavljević B., *Prisluškivanje - naši propisi i evropski standardi,* www.ccmr-bg.org/analize/org