UDK 342.738:343.91-05]:343.132

LIMITATION OF THE RIGHT TO PRIVACY BY SECRET OBSERVATION OF THE SUSPECT'S COMMUNICATION

Saša Knežević
full professor
Faculty of Law, University of Niš
knez@prafak.ni.ac.rs

Ivan Ilic
assistant professor
Faculty of Law, University of Niš
ivan@prafak.ni.ac.rs

Abstract

The right to privacy is one of the fundamental human rights. However, the illumination of modern types of crime (especially organized crime) requires the use of technical achievements that necessarily limit the privacy of the persons to whom these measures have been applied. Thanks to scientific and technological progress, interpersonal contacts take place with the absence of the time distance required to move information from the sender to the recipient. It is realistic to expect that the authority of criminal proceedings can hardly resist the temptation to supplement evidence with the insight into the intimacy of the defendant (or suspect). Thus, achievements of scientific and technological progress are the legacy that makes it easier and adorn human life, but it is also "restless Faust" who is tempting a man at every step. Certainly, scientific and technical achievements "provoke" the legislator, as well as the police and judicial authorities in the process of clarifying the criminal case. A delicate task is set before the legislator. The provisions of the law must be such as to provide for the suppression of perpetrators of criminal offenses (especially organized crime), who in the performance of their activities of criminal character use the most modern scientific and technical achievements. On the other hand, a border must be determined, dividing legally from unlawful interference with private life, which must not be crossed by the police and judicial authorities, engaged in the criminal prosecution of perpetrators of criminal offenses.

Key words: *the right to privacy, secret surveillance, special investigative actions;*

General remarks

Some serious crimes result in extremely serious violations of social goods. In addition, these crimes are committed by persons of a specific psychological profile, who approach their own criminal activity from the positions of professional engagement, directed to the realization of material profit. Therefore, crimes committed in various organized forms are hardly revealed

by classical means of proof. Modern legislation, having in mind these circumstances, envisages a wider range of specialized means of proof, which provide the possibility of institutional response to serious crimes of organized crime, war crimes and other extremely serious crimes.

Special investigative techniques, directed to the detection and processing of the most serious crimes, the Serbian legislation terminologically denotes as *Special means of proof* (Articles 161-187 of the Code of Criminal Procedure of Serbia). These are means that dramatically increase the possibility of discovering and proving serious crimes. However, these actions include secret monitoring of the conduct and communication of the suspect, without any knowledge of the suspect that he/she is the object of supervision by the prosecuting authorities. In this way, the privacy of the suspect is revealed, with the existence of a real possibility of finding out facts that are not relevant to the prosecution of the crime, as well. Therefore, there is a danger of an unauthorized insight on the intimacy of the persons subject to a secret observation. It is precisely this danger that requires strict legality when applying these measures.

The latent possibility of exceeding the permitted insight into the intimacy of the suspect is not the only danger that threatens the human rights of those who come under the impact of these measures. They are undertaken in pre-trial proceedings, when there is a minimum degree of conviction about the criminal offense and the perpetrator - suspicion. Therefore, these measures are being undertaken when the possible proved guilt of the suspect is still far from the horizon of an organized social reaction to unlawful behavior. The effectiveness of the criminal-law reaction obviously placed in the shadow the possibility of limiting the elementary human rights of persons under which conspiratory supervision measures are applied.

Strict legality in the application of specialized means of proof requires that legal norms determine clear substantive and formal legal conditions for the application of these measures. In addition, it is necessary to limit their time use, as well as to determine the procedure with evidence collected through the use of specialized means of proof. In particular, the handling of data, which has not been designated as the subject of the secret conduct by prosecuting authorities, should be regulated. Legal norms must exclude the possibility of using the received data for non-processing purposes.

From evidential actions that can violate the privacy of citizens, the broadest application the *search of the apartment and persons* and, to some extent, the *physical examination of the defendant.* These are regular (classical) means of proof. The Criminal Procedure Code also prescribes specialized means of proof - surveillance of the suspect's communications; secret surveillance and recording; computer search of data; controlled delivery and a hidden investigator. In the following exposition, the focus of our attention will be the secret observation of the suspect's communications. But before that, we will refer to the international legal and constitutional protection of citizens' privacy.

1. International and constitutional protection of privacy

The right of citizens to protect privacy is one of the basic human rights whose respect is required by the civilization standards of modern times. Imperative norms that prescribe as unacceptable "arbitrary and unlawful" interference with the private life of people and their families, as well as the violation of the inviolability of home and personal integrity are

contained in the Universal Declaration of Human Rights (art. 12). The International Pact on Civil and Political Rights provides that no one may be subject to arbitrary or unlawful interference with his private life, his family, home and correspondence (Art. 17). The privacy of citizens is also protected by the provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8).

By implementing the provisions of these international acts they have become an integral part of our positive law. The concrete expression of this provisions of international documents was also found in the Constitution of the Republic of Serbia. Specifically, generally accepted rules of international law and ratified international treaties are an integral part of the legal order of the Republic of Serbia and are directly applicable. However, in order to confirm an international treaty, it must be in accordance with the Constitution (Article 16, paragraph 2).

The Constitution of Serbia proclaims basic human rights, including those related to the freedom of communication. The secrecy of communication by letters and other means is guaranteed (Article 41, paragraph 1 of the Constitution of Serbia). Deviations from privacy protection (even for a limited time) have a constitutional justification. However, the constitutional norm allows a departure from the inviolability of secrecy of letters and other means of communication, based on a court decision, and if this is necessary for the conduct of the criminal procedure or protection of the security of the country, and in the manner provided by the law (Article 42, paragraph 2).

Citizens' privacy is also protected by *criminal law*. Criminal legislation of the Republic of Serbia criminalizes behavior which constitutes an unauthorized insight into the private life of citizens. Specific crimes, which incriminate inadmissible conduct in the sphere of freedom of communication, are the result of the legislator's efforts to protect the privacy of citizens. These are crimes: violation of the confidentiality of letters and other consignments (Article 142 of the Criminal Code of Serbia); unauthorized eavesdropping and tone recording (Article 143 of the CC of Serbia), unauthorized photographing (Article 144 of the CC of Serbia), unauthorized publication and display of another's writing, portrait and footage (Article 145). The accomplishment of this goal also is provided by the criminalization of the unauthorized violation of the inviolability of the apartment (Article 139 of the CC of Serbia) and illegal search (Article 140 of the CC of Serbia).

1. Violation of privacy by limitation of the suspect's communication

The international legal and constitutional legal rank of the right to free correspondence and communication is not a guarantee at all for its inviolability. In this sense, international legal documents also provide *exceptions from the inviolability of private life*. The European Convention allows the possibility of "inteference by public authorities with the exercise of the right to privacy" in accordance with the law and in the interests of national security, public security or the economic well-being of the country, in order to prevent disorder or crime, the protection of health, morals and the rights and freedoms of others. The limits of a legitimate restriction on the freedom of communication are also determined by the practice of the European Court of Human Rights. From the practice of the European Court in the case of *Klass and Others v. Germany*, follows the right of the state to protect itself against immediate threats against "free democratic constitutional order" from riots and crimes, as well as from

threats to national security.[1] However, it would be contrary to the principle of the rule of law if the discretionary freedom of the executive was unlimited. Although States have tried to dispute that the observation of the suspect's communication outside the scope of the right to privacy, justifying this with the protection of the public interest, the Court has made it clear that recording the conversation constitutes an interference with the right to private life.

Starting from the aforementioned case *Klass v. Germany*, the Court later dealt with the assessment of the quality of the law relating to the secret observation of the communication of the suspect. The court found in *The Sunday Times v. The United Kingdom* found that the "*quality of law*" criterion implies that national law must be available and predictable, and the law is predictable if it is clear and precise.[2] In these cases, the court applies the concept of "*potential victim*". It is not necessary that the law, which regulates the interception of the suspect's communication, be applied in a specific case. The existence of a law in itself constitutes a threat to all people it can be applied to.[3] It is enough that an individual proves that there is a "reasonable probability" that the law can be applied to him.[4]

Based on the Court's practice, it can be concluded that adequate procedural guarantees, in the event of a secret observation of communication, can be provided by prescribing the nature of the offenses for which it is possible to apply this measure,[5] the categories of persons to which these measures may be applied, the duration limitation, the procedure for storing and using the obtained data, the prevention measures when delivering materials to third parties and the circumstances under which the collected material must be destroyed.[6]

The Court found a violation of the right to a private and family life under Article 8 of the Convention by failing to fulfill the criteria "in accordance with the law" and "the necessity of interference in a democratic society" in the event of an inadequate reasoning for determining the secret observation of the communication of the suspect. In the cases *Dragojević v. Croatia* and *Bašić v. Croatia*, the Court pointed out that the absence of an explanation of specific reasons justifying the application of the measures of secret surveillance, in particular, which explains the legal requirement that the investigation could not be carried out otherwise or would have disproportionate difficulties, does not provide the necessary protection against misuse. Necessary guarantees of legality can not be justified by the retroactive justification of the application of secret surveillance.[7]

In addition to fulfilling the criteria of "predictability of the law", in the case of the application of the secret observation of communication, the Court examines the fulfillment of the conditions for the necessity of interference in a democratic society, in order to achieve a legitimate aim. There must be adequate guarantees against misuse. Assessment of the

[1] Klass and Others v. Germany, *App. no. 5029/71, § 46*,

[2] The Sunday Times v. The United Kingdom, *App. no. 6538/74 (26/04/1979) § 49;*

[3]Klass and Others v. Germany, *App. no. 5029/71, § 34*, Liberty and Others v. the United Kingdom, *App. no. 58243/00, §§ 56, 57*

[4] Kennedy v. UK, *App. no. 26839/05, § 122.*

[5] *The condition of predictability does not require the determination of a list of the named crimes, but it is sufficient that it be determined by nature (certain groups of offenses). For example, in the United Kingdom, interception of the suspect's communications can be ordered when necessary in the interests of national security, with a view to preventing or detecting serious crimes or for the protection of the economic well-being of the United Kingdom.* Kennedy v. UK, op. cit*., § 159.*

[6] Huvig v. France, *App. no. 11105/84, § 34;* Amann v. Switzerland, *App. no. 27798/95, § 76;* Valenzuela Contreras v. Spain, *App. no. 27671/95, § 46;* Prado Bugallo v. Spain, *App. no. 58496/00, § 30.*

[7] Dragojević v. Croatia, *App. no. 68955/11, § 98,* Bašić v. Croatia, *App. no. 22251/13, § 33, 34.*

fulfillment of this criterion depends on the nature, scope and duration of the measures, the reasons for determining, the authorities responsible for implementation and supervision, as well as the type of remedy, which is envisaged at the national level.[8]

On the other hand, from the practice of the European Court of Human Rights, it follows that the right to privacy was not violated if the state used the "*products*" of wiretapping telephone conversations to deny the access of an eavesdropped person to the civil service.[9] In contrast, privacy is also violated in the event that the police are eavesdropping their employees in their own premises without a warrant.[10]

Likewise, it is unacceptable not only to illegally wiretap phone conversations, but also to provide the police with data obtained by registering phone calls without a legal basis, or without the consent of the person whose conversations are registered. Considering the nature of these measures, it is clear that there is no obligation for the state to inform the person to whom these measures apply.[11] However, the existence of legal remedies for persons whose communication is intercepted is of great importance. They must be accessible, regardless of whether a person has information on whether or not these measures have been applied to him.[12]

3. Secret surveillance of telephone and other communications of the suspect

It is indisputable that the state can not completely renounce the control over the communications of the defendant (or suspect). If this were the case, the success of the criminal justice protection of the society would be called into question. However, consistency in the realization of the defendant's human rights requires precise conditions under which the principle of the inviolability of the secrecy of letters and other forms of communication can be departed from.

3.1. Conditions for the implementation of this measure

International standards for the *protection of privacy* require that surveillance and recording of telephone and other communications of the suspect can be ordered only under conditions prescribed by the law. From the requirements of a substantive nature, it is necessary to foresee that the decision on deviation from the principle of inviolability of the secrecy of letters and other forms of communication can be made only in case of endangering the highest social values by organized commission of explicitly stated crimes. In addition, the decision on the supervision and eavesdropping of telephone and other communications (fax, mobile phones, e-mail, etc.) must be essentially court-based, with the obligation to explain the decision, but also time-limited. Data obtained by applying this measure may be used as evidence in criminal proceedings only if this measure is applied in accordance with the normative framework for its application and can not be used for other, non-process purposes.

3.1.1. Criminal offenses for which this measure is applied

The Code of Criminal Procedure stipulates that secret surveillance of communications can be initiated if there is a *suspicion* that a person has participated in the

[8] Klass and Others v. Germany, *op. cit, §§ 49, 50,* Weber and Saravia v. Germany, *App. no. 54934/00, § 106*
[9] Leander v. Sweden, *App. no. 9428/81*
[10] Halford v. UK, *App. no. 20605/92*
[11] Kennedy v. UK, *App. no. 26839/05, § 167*
[12] Roman Zakharov v. Russia, *App. no. 47143/06, § 233,234*

commission of the most serious crimes prescribed by the provision of Art. 162 of the CCP of Serbia. An additional requirement for the application of this and other special means of proof is that the evidence for the prosecution could not be collected without the application of these measures, or their collection would be significantly more difficult (Article 161 of the CCP of Serbia). Therefore, subsidiarity in the application is normatively determined, as a result of the possibility of over - interference in the area of human rights protection of the suspect.

The legislator also allows the possibility of application of secret surveillance of the suspects' communications in case there is a suspicion that a person is *preparing* the execution of any of the crimes that constitute a material condition for the application of this measure. The confirmed subsidiarity of the application of the measure in this case, is a logical result of the effort to limit its excessive scope. The regulated obligation of the prosecuting authorities to act in a manner that is less threatening for the human rights of the suspect is also on that course (Article 161, paragraph 3).

The application of secret surveillance of communications, as well as most other special means of proof, is foreseen for criminal offenses under the jurisdiction of specialized prosecuting authorities, as well as for the listed criminal offenses (Article 162 of the CCP). These are crimes for which prosecution jurisdiction have public prosecutors for organized and war crimes.

These specialized public prosecutors are prosecuting the perpetrators of criminal offenses committed in the form of organized crime, suspects for war crimes, as well as the perpetrators of certain enumerated criminal offenses, envisaged by the Law on the organization and competence of state authorities in combating organized crime (Article 2).

Organized crime involves the commission of criminal offenses under the following conditions: a) the existence of a group of three or more persons; b) that the group exists for a certain amount of time; c) action of the group based on the agreement, with the aim of committing criminal offenses; d) execution of a criminal offense, for which a sentence of imprisonment of four years is prescribed, or a more severe punishment; e) the goal of committing criminal offenses is to obtain, directly or indirectly, financial or other benefits (Article 3).

The war crimes prosecutor's office has jurisdiction: a) for crimes against humanity and other goods protected by international criminal law (genocide, war crimes against humanity, war crimes against civilians); b) serious violations of international humanitarian law committed in the territory of the former Yugoslavia, starting from January 1, 1991; c) for the criminal act Assistance to the perpetrator after one of these criminal offenses.

The secret surveillance of the suspect's communications may be determined, except for criminal offenses within the jurisdiction of the specialized public prosecutor's offices, and for certain criminal offenses listed in the provision of Art. 162. Code of Criminal Procedure of Serbia. Among other, these are the following crimes: severe murder, kidnapping, forgery of money, espionage, attack on constitutional order and other criminal offenses (Article 162, paragraph 1, item 2 of the CCP).

The criminal procedural legislation of Serbia, obviously, belongs to those legal systems in which criminal acts are defined on the basis of the enumeration principle (the so-called catalog of criminal offenses), which are the basis for the application of the measure Secret surveillance of telephone and other communications of the suspect. To this group of legislation also belongs *German law* (§ 100. The StPo foresees the application of this measure to the perpetrators of criminal acts defined on the basis of the enumeration principle, mainly

those directed against the constitutional order and security of the country, the most serious violations of international law, forgery of money, robbery, etc.), as well as the *Italian* criminal procedural legislation (Article 266. *Codice di procedura penale*).

To this group of legislation also belongs *American law*, which allows the application of surveillance measures and recording of telephone and other communications when illuminating crimes with the element of violence, related to drugs and organized crime.

The Code of Criminal Procedure of Montenegro, however, accepts the so - called *combined system*. According to the provision of Art. 158 of the CCP of Montenegro, this measure can be applied to perpetrators of criminal offenses for which a sentence of imprisonment of ten years or more is envisaged, as well as for criminal offenses with elements of organized crime, against the security of computer data, but also for some listed crimes. *Croatian legislation* also belongs to this group of legislation. Namely, the Croatian CCP allows the use of surveillance and technical recording of telephone and other communications for criminal offenses against the Republic of Croatia and the armed forces of Croatia, for which there is a sentence of imprisonment of five years or more years or long-term imprisonment foreseen, but also for a number of enumerated criminal offenses, as well as for organized forms of commission of criminal offenses (Article 334 of the CCP of Croatia). The CCP of the *Republic of Srpska* (Article 235) offers a similar solution. According to this Code, the application of this measure is possible, if criminal offenses against the constitutional order and security of the RS, against humanity and values protected by international law, terrorism, and crimes for which the punishment foreseen is over five years, have been committed or are being prepared.

Comparatively observed, in addition to these two systems, there are legal solutions according to which surveillance and recording of telephone and other communications can be ordered depending on *the severeness of the prescribed sentence* (de facto, depending on the gravity of the offense). *French* legislation falls into this group (art. of the CPP 100 foresees that this measure can be taken for crimes or offenses for which a punishment of two years or more is envisaged, and also *Swiss law* (arts. 66 al. 1 a, b, c, the LPP envisages the possibility of monitoring and recording communications of suspects for crimes and offenses "whose weight or peculiarities justify this measure" for punishable acts done by the telephone, if certain facts cast doubt on the person to whom the control should be determined and if the illumination of the criminal offense without the application of this the measures would be difficult). [13]

Similar legal solutions exist in the *British*, i.e. the right of England and Wales (Scotland has autonomous legislation). However, according to the 1985 Law on the regulation of telephone eavesdropping, the Secretary of State may issue an interrogation warrant if this is necessary for the interests of State security or the prevention of *serious criminal offenses* or for the preservation of the economic well-being of the United Kingdom.[14] British law, therefore, does not provide for even the lower limit of the penalty required for the application of this measure.

[13] Banović, B, Korišćenje specijalnih sredstava za nadzor komunikacija u pretkrivičnom i krivičnom postupku i ljudska prava (Use of special means for monitoring communications in pre-criminal and criminal proceedings and human rights), Pravni život, 2001, no. 9, p. 320.

[14]Krapac, D, PhD, Engleski kazneni postupak (English Criminal Procedure), Zagreb, 1995, p. 126.

In the end, there are also legislations that do not specify the scope of criminal offenses for which the measure of surveillance and recording of telephone and other communications can be used, so this is regulated by general linguistic formulation (reasonable reasons for the application of this measure, the need for evidence collection, etc.), in, for example, *Spanish and Belgian law*.[15]

During the surveillance and recording of the telephone and other communications of the suspect, data may be recorded indicating the execution of another criminal offense, not the one for which this measure was taken. That is the so-called *accidental finding*. In the criminal procedural legislation of Serbia, until the adoption of the enforceable Criminal Procedure Code, there was a legal vacuum in regulating this issue, which negatively reflected the legitimacy of privacy restrictions by applying this measure.

However, Serbia's positive legislation (Article 164) permits the use of data on criminal offenses obtained through the use of special means of proof, although the collected material on the criminal offense and the perpetrator was not included in the warrant for the implementation of these measures. It is necessary that the data collected relates to some of the offenses for which the application of these measures can be determined (to be included in the legal catalog).

The Code of Criminal Procedure of Montenegro also regulates the treatment of an "*accidental* finding", only in the case of finding out information about one of the crimes from the list provided for by law (Article 159, paragraph 10). In this situation, the part of the footage will be copied and forwarded to the state prosecutor, with no restriction to the recording being treated as the original recording of a conversation pointing to that other criminal offense.[16] However, neither the Montenegro CCP does not provide a solution for the conduct of investigative authorities in the case of registering data on a criminal offense that is not a part of the list of criminal offenses for whose detection it can be ordered monitoring and recording communications of the suspect.

Such a video could have a so-called. cognitive significance, that is, it can serve the state prosecutor for further conduct within his/her rights and duties, and, by himself, could not be used as evidence in criminal proceedings.[17]

The approach of Macedonian legislation is also interesting. Provision of Art. 263. of the CCP of the *Republic of Northern Macedonia* allows the use of data obtained through the use of special means of proof, which relate to a criminal offense not covered by an order, provided that it is possible for this measure to be applied for such a criminal offense. However, this provision does not explicitly permit the use of personally identifiable information about a person, which is not covered by an order for the implementation of these measures. It seems

[15]See: Škulić, M, Organizovani kriminalitet-Pojam i krivičnoprocesni aspekti (Organized Crime - Concept and criminal procedural aspects), Belgrade, 2003, p. 265,266.

[16]Radulović, D, Specijalne istražne radnje i valjanost dokaza pribavljenih preduzimanjem tih radnji u krivičnom procesnom zakonodavstvu Srbije i Crne Gore i opšteprihvaćeni pravni standardi (Special investigative actions and validity of evidence obtained in the criminal procedural legislation of Serbia and Montenegro and generally accepted legal standards), a report from XLI regular annual consultations of the Association for Criminal Law and Criminology of Serbia and Montenegro, Zlatibor, September 2004, p. 469.

[17]Ibid

that this was not the intent of the legislator, and that therefore this provision should be clearly re-formulated and specified.[18]

3.1.2. Persons whose privacy can be restricted by observation and recording of telephone and other communications

It is clear from the provisions of the Criminal Procedure Code of Serbia that this measure can be applied to persons for whom there is a *suspicion* that they have committed or are preparing to commit some of the crimes in the field of organized crime, war crimes, as well as certain criminal acts enumerably determined by law. The condition is also that the evidence of this criminal offense and the perpetrator can not be revealed by other means of proof. Therefore, the telephone and other communications of the *suspect* in the pre-trial procedure can be observed.

Communication by phone, fax, e-mail and other modern technical means is, so to speak, two-way. This means that the surveillance and recording of the suspect's communications necessarily involve the technical observation of the person on the other side of the phone call, who does not necessarily have to be involved in criminal activities. If this were the case, the privacy of a "non - delinquent " interlocutor who is not involved in the criminal activity of the suspect will be protected by the obligation to use the information obtained only for process purposes. However, the question arises as to whether surveillance and recording of communications can be applied to persons who are in some way involved in the criminal activity of the suspect.

The Code of Criminal Procedure of Serbia does not provide a decisive answer to this issue, while the Montenegrin CCP foresees the application of secret surveillance and technical recording of communications, and to persons for whom there are grounds for suspicion that they *transfer the messages related to criminal acts* to the perpetrators or that the *perpetrator is using their connections* for the telephone or another telecommunication device, for criminal acts in the catalog of the criminal acts relevant for the application of this measure. (Article 157, paragraph 3 of the CCP of Montenegro). The same legal solutions exist in *German* (§ 100th StPo) and *Croatian* law (Article 332, paragraph 7 of the CCP). Croatian positive law allows for the application of this measure, except to the persons who transmit messages and use the connections for the technical means of the suspect, and for persons who conceal the perpetrator or conceal the means by which the crime was committed, destroy or hide the traces or objects created by the criminal offense, and help the perpetrator in other way not to be discovered. Croatian case-law has confirmed this view, even before the legislature regulated this situation. The Supreme Court of Croatia took the view that an "accidental finding" could be used as evidence in criminal proceedings if that other person was in the "criminal sphere" of the person to whom the measure was ordered (for example, using his phone connections).

The question arises as to whether the results obtained by applying this measure can be used against a person who, later in the criminal procedure, may have the position of the so-called privileged witnesses. It may be considered that the use of the secret surveillance of communications of these persons would deny the essence of the process position of this

[18] Kalajdziev, G. Lazetic et al., Komentar Zakonot na krivičnata postapka (Commentary on the Law on Criminal Procedure), Skopje, 2018, p. 590.

category of witnesses. However, if these persons also had the capacity of a suspect because they are preparing or have already committed one of the criminal offenses for which the use of specific evidence could be determined, then the secret supervisor of their communications would be legal. Canadian law, however, allows monitoring of communications of *unknown persons*, whereby this measure can not be applied to persons known at the time of filing the application, while French law determines the monitoring of communications carried out from the Bar Association by the prior notification of the president of the bar association.[19] Problems can also arise in terms of monitoring individuals protected by criminal process immunity.[20]

3.2. Making a decision on the secret observation of the suspect's communication

The application of the measure of surveillance and recording of telephone and other communications of the suspect restricts one of the fundamental human rights - the right to privacy. It is a crucial question, how to shape the tendency to use technical achievements in the evidentiary process, without, however, exceeding the threshold of an authorized breach into the *intimacy*. The need for evidence must not violate the minimum of the *moral dignity of the suspect*. Therefore, a decision on deviation from the principle of inviolability of secrecy of letters and other forms of communication should be made only under the conditions and in the manner strictly provided for by the law and only for the purposes of the criminal procedure.

From the nature of this measure, which delineates the *horizons of freedom of intimate life of people*, derive the exceptional nature of its application. Therefore, the application of this measure of secret surveillance of the suspect's communications must have a *subsidiary character*, i.e. this measure should be applied only when evidence is not provided in another way. Unlike the previous legislation, the current Criminal Procedure Code of Serbia prescribes the subsidiary character of this special mean of proof, as well as for other special means of proof. *Montenegrin* and *Croatian* legislation have the same approach, because they condition the application of the measure of surveillance and recording of telephone and other communications of the suspect with the previous use of "classical" means of proof. Thus, the secret observation of the suspect's communication is possible "if in some other way the evidence could not be collected or their collection would require a disproportionate risk and endanger lives of people" (Article 157, paragraph 1 of the CCP of Montenegro), or if the investigation of criminal offenses could not have been carried out otherwise or would have been incompatible with disproportionate difficulties (Article 332, paragraph 1, of the CCP of Croatia). The subsidiary character of this measure is also present in *American law*, according to which the application of this measure is possible if a regular investigation procedure has been tried and failed, or is unlikely to succeed or is excessively dangerous to use (18 USC (§2518 11) (a) and (b) (i)). [21]

The *public prosecutor* has the initiative for applying the measure of supervision and recording the communication of the suspect, which should provide the reasoned proposal with

[19] See: Ilić, G, Odstupanje od nepovredivosti tajne pisma i drugih sredstava opštenja, (Deviation from the inviolability of secrecy of letters and other means of communication), Revija za kriminologiju i krivično pravo, 2003, no.1, p.29.
[20] See: Radulović, D, op. cit. p. 470.
[21] Banović, B, op. cit. p. 324.

the facts from which the necessity of applying this measure can be seen (Article 166, paragraph 1 of the CCP of Serbia). The role of the initiator for the application of this measure the public prosecutor has also in *Montenegrin* (Article 159 § 1 of the CCP), *Croatian* (Article 332, paragraph 1) and *Canadian law* (Article 185 (1) C cr), while in *US law* a request for supervision of communication is submitted by a police officer with the consent of the state prosecutor.

International *privacy protection* standards require that a decision directly affecting the suspect's intimate life sphere must be *strictly formal*. A legitimate insight into the communication of the suspect is possible only on the basis of a written and reasoned order of the investigating judge that contains information about the person to whom this measure is being applied, the basis of suspicion, the manner of implementation, the scope and duration of this measure. communication of the suspect is possible only on the basis of a written and reasoned order of the investigative a judge containing information about the person to whom this measure is applied, the basis of the suspicion, the manner of implementation, the scope and duration of this measure. Also, the decision on supervision and recording of telephone and other communications deeply affects the *intimate sphere* of the suspect, protected by international and constitutional norms. The logical consequence of this fact is that this decision can only be brought by the *court*.

According to the Serbian legislation, the secret supervision of the communication of the suspect is determined by the preliminary procedure judge, by issuing a reasoned order (Article 167, paragraph 1 of the Code of Criminal Procedure of Serbia). The order should contain: available information on the suspect, the legal name of the criminal offense, the marking of the known telephone number and the address of the suspect, or the telephone number or address for which there are grounds for suspecting that the suspect is using them, the reasons for the suspicion, the manner of implementation, the scope and duration of this special mean of proof (Article 167, paragraph 2, of the CCP of Serbia).

The decision on the implementation of secret surveillance of communications in Montenegrin law is brought by a judge for investigation (Article 159, paragraph 1, of the CCP of Montenegro). The judicial authority acting at the stage of the investigation is responsible for the making of this decision, in the law of *France* (art. 100 al. 2, CPP) and *Croatia* (Article 332, paragraph 1 of the CPC), *Germany* (§ 100.b. Abs. 2 StPO of Germany) and *Italy* (art. 267 CPP).

The judicial character of the decision on the supervision and recording of telephone and other communications of the suspect is somewhat relativized by the legal solutions of *Italian* and *German* law. In these legal systems, the decision to monitor the communications of the suspect is primarily brought by the investigating judge, but if there is a danger of delay, the decision is passed by the state prosecutor who immediately informs the investigating judge (art 267 CPP of Italy) and the investigating judge must confirm the decision of the state prosecutor within three days (§ 109.d of the StPO of Germany).

The legal basis for the decision on monitoring and recording of the suspects' communications is also contained in the *Law on the Security Information Agency of Serbia*. This law stipulates that "the director of the Agency may, if necessary for the sake of security of the Republic of Serbia, by its decision, on the basis of a *previous decision of the court*, determine certain measures to be taken to certain individuals and legal entities, which are deviating from the principle of inviolability of secrecy of letters and other means of communication, in the procedure established by this Law "(Article 13).

This, as well as the provisions of Art. 14 and 15 of the original text of this law passed in 2002 were the subject of establishing constitutionality. Namely, in its decision from 2013 (No. 3-252 / 2002 and 66/2014), the Constitutional Court of Serbia stated that the provisions of the Law on the Security Information Agency are overly general in character and allow broader grounds for restricting the right to privacy. It is therefore said that the provisions of this law should clearly specify the circle of persons to which special means of proof are applied, as well as the procedure for their implementation.

By amendments to the Law on the Security Information Agency done after the Constitutional Court's decision (the last one from 2018), the view of the Constitutional Court was respected. First of all, the Director of Security Information Agency is no longer competent to make a decision on the implementation of the measures of secret surveillance of communications. He is authorized to initiate it, to the Higher Court in Belgrade, which can make this decision. It is a novelty that the Director of Security Information Agency can file a complaint to the Appellate Court if a proposal for the application of these measures has been rejected. Measures to monitor and record telephone and other communications are also envisaged by the so-called police law of other countries. In Germany, these issues are regulated by the Law on combating illegal drugs commerce and other forms of organized crime, the Law on the Federal criminal office, the Law on Federal border protection service and other laws.

In Italy, the Act on the Protection of confidential and classified information, even amended certain provisions of the Code of Criminal Procedure.[22] The possibility of undertaking the secret observation of communication of the suspect on the basis of the police powers envisaged by regulations regulating the activities of the police may adversely affect the protection of the privacy of the suspect.

An important component of the privacy protection of the suspect is the *time dimension* of this measure. Since this is a measure that greatly narrows the horizons of freedom and the rights of the person to whom it is applied, it is necessary to restrict the duration of this measure. According to the CCP of Serbia, this measure can last for a maximum of six months (three plus three months), and exceptionally, not more than three months times two (Article 167, paragraph 3).

The *Montenegrian* Code of Criminal Procedure provides for the duration of this measure to a maximum of 18 months from the day of issuing an order of implementation of this measure (Article 159, paragraph 5). The duration of the observer's observation of communications in *Croatian* law amounts to a maximum of eighteen months (Article 335, paragraph 3 of the CCP), eight months in *French* (art 100 al., CPP 2), six months in *German* (§ 100. b. Abs. 2 StPO of Germany), and forty-five days in the *Italian* law (art. 267 CPP).

3.3. The implementation of this measure

The protection of the privacy of the suspect presupposes, not only the strict form in the issuance of an order to control and record communications of the suspect, but also clearly precise conditions for the *implementation* of this measure. Since it is a conspiratorial measure, in its implementation, by the nature of the matter, a minimum number of subjects participates.

The surveillance and recording of telephone and other communications is conducted by the *police*, the Security Information Agency or the Military Security Agency, and the

[22] Ibid, p. 321.

creation of technical conditions for the implementation of this measure falls within the scope of work of postal, telegraph and other companies, companies or persons registered for the transmission of information (Article 168 paragraph 1 and 2 of the CCP of Serbia). The collected data, obtained by executing this measure, are being submitted to the preliminary procedure judge and to the public prosecutor upon their request.

The Code of Criminal Procedure of Montenegro regulates the implementation of this measure in more detail. Specifically, the provisions of the CCP of Serbia do not specify the obligations of the police authorities towards the public prosecutor and the preliminary procedure judge when implementing the measure. In contrast, a police officer who performs surveillance and recording of the suspects' communications has the obligation to keep records of the conducted operation and to submit *periodic reports* on the execution of the measure to the investigative judge and the state prosecutor (Article 160, paragraph 5 of the CCP of Montenegro).

A more logical is the solution of the Montenegrin legislation that the final report and other materials obtained by this measure are submitted to the *state prosecutor* (Article 160, paragraph 6 of the CCP), rather than the preliminary procedure judge (as derived from Article 170, paragraph 1 Of the CCP of Serbia).[23] The higher level of involvement of the state prosecutor and the investigative judge during the implementation of this measure is also envisaged by Croatian legislation (Article 337, paragraph 1 of the CCP). Namely, reports and materials are submitted to the state prosecutor, while the investigating judge has the right to request from the state prosecutor the results of the applied measures at any time.

Police authorities are, except in our country, authorized to execute surveillance and recording of telephone and other communications of the suspect, in *American*, *Canadian* and *Croatian* law. The implementation of this measure in *German* law is entrusted to a judge, a state prosecutor or his assistant police officer, while *French* legislation entrusts the monitoring of communications of the suspect to investigating judge or judicial police officer. The obligations of the post office and other providers registered for the transmission of information in the execution of the measure of supervision and recording of the suspects' communications are explicitly foreseen, in our and also in the German legislation (§ 100.b. Abs. 3 StPO).[24]

3.4. Use of evidence obtained through the supervision and recording of telephone and other communications of the suspect

In order to achieve the optimum protection of the human rights of the defendant, it is necessary to provide that only the information obtained in accordance with the conditions required for the decision on limiting the freedom of communication may be used as evidence in criminal proceedings. If a measure of supervision and recording of telephone and other communications was applied contrary to the legal requirements for the implementation of this measure or if it was done in disagreement with the order of the preliminary procedure judge, the court decision can not be based on such evidence (Article 163, 3. CCP of Serbia). Therefore, it is the court's obligation to *extract* the evidence obtained in an unlawful manner from the *case file*. If the verdict was based on these, *unlawful*, evidence, it would be a

[23] This view is represented also by Radulovic, D, op. cit. p. 471.
[24] See: Ilić, G, op. cit. p. 33.

substantial violation of the provisions of the criminal procedure (Article 438, paragraph 1 of the CCP of Serbia). By positive legal solutions, this violation has received the character of a relatively serious violation of the provisions of the criminal procedure, although until the adoption of the positive CCP it had the character of an absolutely essential violation of the provisions of the criminal procedure. The evidence whose existence was revealed from the data collected by surveillance and the recording of telephone and other communications by the suspect (so-called "*fruit of the poisonous tree*") is also illegal.

However, the question arises as to how it can be ascertained that the "*fruit of the poisonous tree*" is used in criminal proceedings. The fact that there is legally invalid evidence in the case files or that the court did not comment in the reasoning of the verdict to legally invalid evidence does not in itself mean that they do not represent the factual support of the judgment. However, if the court, in the reasoning of the judgment, gives great importance to distant indications and there are evidence in the files that can not be the basis of a judgment, the judgment was rendered under the influence of the invalid evidence. In that case, there would have been odds, albeit small, of success in denouncing the verdict by Article 438. paragraph 1. point. 11 of the Code of Criminal Procedure of Serbia (these are formal defects of a written judgment).[25]

It is interesting to note that the practice of the European Court of Human Rights does not exclude the possibility of using evidence obtained through the unlawful observation of the defendant's communications. In a decision on the case of *Khan v. The United Kingdom* (dated 12 May 2000), it was noted that the use of recorded material obtained in an unlawful manner is not in conflict with the requirements of righteousness (Article 6, paragraph 1 of the European Convention), although condemnation is based *exclusively on this evidence*![26]

Disrespect of the conditions for monitoring the communications of the suspect envisaged by law is sanctioned by the inability to use this evidence also in the criminal procedure in the *Montenegrin* Criminal Procedure Code (Article 161), as well as the *Croatian* Criminal Code (Article 339, paragraph 8).

3.5. Prohibition of the use of received data for non-processing purposes

From the standpoint of the protection of human rights of the suspect, it is necessary to prohibit the use of data obtained by wiretapping and tone recording of the suspects' conversation for other *non-procedural purposes*. The established irrelevance of the knowledge obtained for the purposes of the criminal proceedings must result in the *destruction of the data and information* from which they were obtained, under the supervision of the preliminary procedure judge. This way of handling data unnecessary for the conduct of criminal proceedings is provided by Art. 163. paragraph 1. of the Code of Criminal Procedure of Serbia and Art. 160, paragraph 7. CCP of Montenegro. This prevents the creation of a file or the so-called *data banks* on the defendant, which could be used to achieve non-procedural purposes.

[25] See:Vasiljević, T, Grubač, M, Komentar Zakona o krivičnom postupku (Commentary on the Criminal Procedure Code), Belgrade, 1987, p. 624

[26] Ljudska prava u Evropi (Human Rights in Europe), Pravni bilten, Zemun, no. 6, 2000, p. 13-15.

The question arises as to whether the data obtained by observation of the conversation of the defendant with the defense can be used in the criminal proceedings. The Criminal Procedure Code of Serbia does not regulate this issue. This suggests that it is possible to monitor and record the communications of the defendant with the defense counsel or the suspect with a lawyer under the general conditions for the application of this measure (Article 161 of the CCP).

Final remarks

The right to privacy is one of the fundamental human rights. However, the revelation of modern types of crime (especially organized crime) requires the use of technical achievements that necessarily limit the privacy of the persons to whom these measures have been applied.

The normative expression of the special means of proof from Art. 161. Of the Code of Criminal Procedure is basically harmonized with the United Nations Convention against transnational organized crime. However, this does not mean that the "*legal coordinates*" in which this investigation can be carried out constitute an optimal institutional environment for increasing the effectiveness of criminal prosecutions or for protecting the privacy of the suspect. On the contrary, the forthcoming changes to the CCP need to regulate some issues that do not represent part of the positive regulation of this mean of proof, and the importance of regulating these issues is indicated by doctrine, case law and comparative law.

The legal solutions must reinforce the *subsidiary character* of the special means of proof, ie. the implementation of these measures should be approached only if the absence of these measures would result in disproportionate difficulties or a serious danger or other evidence would not determine the facts necessary for the revelation of serious forms of crime. This attitude was also taken up by the International Criminal Law Association at its 16th Congress[27] and it corresponds with advocating for a greater degree of protection of the privacy of the suspect.

The legality of privacy restriction by surveillance and recording of telephone and other communications will be taken into consideration if the forthcoming legislative changes through the explicit legal provision allowing the use of data about persons *involved in the criminal activity* of the suspect, obtained by supervision and recording of the suspect's communications. The person whose connections to the phone the suspect used, as well as persons who are transferring messages related to criminal acts from the "catalog", to or from suspect, must not stay out of reach of this measure. Theoretical criminal procedural law, as well as the legislation, should give clear answers to the possibility of using the results of special means of proof against persons protected by immunity, privileged witnesses and lawyers of the suspects.

The logic of the criminal procedure indicates that the final report on the conducted observer's communication of the suspect should be submitted to the *public prosecutor* because he is authorized to initiate a criminal proceeding (of course, if this arises from the results of this and other actions in the pre-trial procedure) rather than the preliminary procedure judge.

[27] See the text of the Resolution for the Third Section of the Congress, International Review of the Penal Law, 199, no. 3-4, p. 923.

A person who has been the subject of secret surveillance of communications, against whom criminal proceedings are not initiated within the legal deadline, must be informed that this special mean of proof has been taken against him. This must be the legal obligation of the prosecuting authorities, not just the legal possibility.

BIBLIOGRAPHY

Amann v. Switzerland, App. no. 27798/95

Banović, B, Korišćenje specijalnih sredstava za nadzor komunikacija u pretkrivičnom i krivičnom postupku i ljudska prava (Use of special means for monitoring communications in pre-criminal and criminal proceedings and human rights), Pravni život, 2001, no. 9

Bašić v. Croatia, App. no. 22251/13

Dragojević v. Croatia, App. no. 68955/11

Halford v. UK, App. no. 20605/92

Huvig v. France, App. no. 11105/84

Ilić, G, Odstupanje od nepovredivosti tajne pisma i drugih sredstava opštenja, (Deviation from the inviolability of secrecy of letters and other means of communication), Revija za kriminologiju i krivično pravo, 2003, no.1

Kalajdziev, G. Lazetic et al., Komentar Zakonot na krivičnata postapka (Commentary on the Law on Criminal Procedure), Skopje, 2018

Kennedy v. UK, App. no. 26839/05

Kennedy v. UK, App. no. 26839/05

Klass and Others v. Germany, App. no. 5029/71

Krapac, D, PhD, Engleski kazneni postupak (English Criminal Procedure), Zagreb, 1995

Leander v. Sweden, App. no. 9428/81

Liberty and Others v. the United Kingdom, App. no. 58243/00

Ljudska prava u Evropi (Human Rights in Europe), Pravni bilten, Zemun, no. 6, 2000

Prado Bugallo v. Spain, App. no. 58496/00

Radulović, D, Specijalne istražne radnje i valjanost dokaza pribavljenih preduzimanjem tih radnji u krivičnom procesnom zakonodavstvu Srbije i Crne Gore i opšteprihvaćeni pravni standardi (Special investigative actions and validity of evidence obtained in the criminal procedural legislation of Serbia and Montenegro and generally accepted legal standards), a report from XLI regular annual consultations of the Association for Criminal Law and Criminology of Serbia and Montenegro, Zlatibor, September 2004

Roman Zakharov v. Russia, App. no. 47143/06

Škulić, M, Organizovani kriminalitet-Pojam i krivičnoprocesni aspekti (Organized Crime - Concept and criminal procedural aspects), Belgrade, 2003

The Sunday Times v. The United Kingdom, App. no. 6538/74

Valenzuela Contreras v. Spain, App. no. 27671/95

Vasiljević, T, Grubač, M, Komentar Zakona o krivičnom postupku (Commentary on the Criminal Procedure Code), Belgrade, 1987

Weber and Saravia v. Germany, App. no. 54934/00