Protection of Personal Data in the Criminal Legislation in Macedonia

Lazar NANEV

e-mail: lazar.nanev@ugd.edu.mk

Olga KOSHEVALISKA

e-mail: olga.gurkova@ugd.edu.mk

Abstract

This paper aims to illustrate the protection of personal data in the criminal legislation in Macedonia. Given the fact that their use throughout the criminal proceedings is constant, delicate and complex, this paper will contribute to the reflection of the actual situation in respecting the right of personal data by the competent authorities. Particular importance will be given to the protection of this right when applying special investigative measures because of the numerous derogation of the right.

Key words*: personal data, criminal procedure, special investigative measures, EU.*

Introduction to Data Protection in Macedonia. The obligation for the protection of personal data originates from the same fundamental right under Article 8 of the European Convention on Human Rights (hereinafter ECHR).[1] Apart from this international instrument, the protection of personal data is regulated by the Convention on the protection of personal data of Council of Europe (hereinafter COE) from 1981, the Additional Protocol and the Recommendation no. (87) 15 of the COE. The latter two instruments are the basis for the creation of our national legislation in this area.[2] Given the fact that our country is pro-European oriented, the process of the ongoing harmonization of the national legislation with the EU legislation is necessary. For Macedonia, a particularly important challenge was and still is, the building of the legal framework in this field, while implementing as many as possible international instruments. Throughout this process the only limiting condition can be national sovereignty and national security.

---

[1] European Convention on Human Rights and Fundamental Freedoms from 1950. The translation of the Convention and its Protocols in Macedonian language are available in "Official Gazette" no. 11/1997, 30/2004 and 30/2005;

[2] The Convention 108 is ratified by the Assembly of Republic of Macedonia and came into force on 1st of July 2006 and its Additional Protocol was signed on 4th of January 2008.

The definitions for personal data, in our national legislation are identical to the definitions that are part of the EU legislation. In this respect, in our national legislation the term "Personal data" stands for: any information relating to identified natural person or legal entity that can be identified, and a person which can be identified is a person whose identity can be determined directly or indirectly, in particular based on the identification number of the citizen or based on one or more features specific to their physical, physiological, mental, economic, cultural or social identity.

The right to protection of personal data in our country is raised to the level of constitutional right guaranteed in Article 18 of the Constitution of the Republic of Macedonia.[3]

Every abuse of this constitutionally guaranteed right is incriminated as a separate offense in the art.149 of the Criminal Code of Macedonia.[4]

The mere criminalization of this right shows its value in the national legislation which is a big step in the process of harmonization with EU law.

The Macedonian Code on protection of personal data. The Macedonian Code on protection of personal data[5] regulates general rules for personal data that are valid on the territory of Macedonia. Given the fact that protection of personal data in criminal cases is not regulated by this law, its elaboration in this paper will be just general and focused on general provisions on which the criminal code invokes.

[3] Article 18 of the Constitution of Republic of Macedonia: The safety and confidentiality of personal data is guaranteed.

Protection against the violation of personal integrity arising from the registration of information through information processing is guaranteed. Constitution of the Republic of Macedonia, adopted on 17 November 1991, Official Gazette no.52 of 11.22.1991, and changes in the Official Gazette no. 1/1992, 31/1998, 91/2001 84/2003, 107/2005, 3/2009, 13/2009 49/2011;

[4] Art.149 of the Macedonian Criminal Code: (1) A person who, contrary to the conditions laid down by law, without the consent of the citizen, collects, processes or uses his personal data, shall be punished by a fine or imprisonment up to one year.

(2) The punishment from paragraph 1 also stands for the one who enters in computer information systems of personal data with the intention of using them for himself or for others, with the purpose to realize some benefit or to inflict some damage.

(3) If the crime from paragraph 1 and 2 are done by an official in performing his duty, he shall be punished with imprisonment of three months up to three years.

(4) The attempt is punishable.

(5) If the crime is done by legal entity, it will be punished by a fine. Kambovski, V., "Criminal Law - Integral text Preface, brief explanations of terms and registry, Skopje 2011, (published in Macedonian language);

[5] Law of protection of personal data (Official Gazette no.7/2005, 103/2008; 124/2008; 124/2010 and 135/2011), hereafter CPPD;

Hence, in Article 7 of Data Protection Code it is proposed that the processing of personal data relating to criminal offenses, sentences, alternative measures and security measures on criminal charges may be made in accordance with law.[6] The same applies to the processing of personal data contained in judicial decisions.[7]

This Code guarantees protection of personal data of every individual without discrimination on the basis of nationality, race, color, religious beliefs, ethnicity, gender, language, political or other beliefs, property, birth, education, social origin, citizenship, place or type of residence or any other personal characteristic.

Entitled body for the supervision over the legality of the processing of personal data and their protection on the territory of Republic of Macedonia is the Directorate for Personal Data Protection. The Directorate is an independent state authority with status of legal entity.[8]

Data protection in criminal law. Moving along the trend of the EU legislation in which such rights are raised to the level of fundamental rights, our criminal legislation provides multiple protections of personal data. This is particularly important given the fact that the use of personal data throughout the criminal proceedings is constant.

Initial processing of personal data starts within the jurisdiction of the police. Thus, the police collects, processes, analyzes, evaluates, assesses, uses, transmits, stores and deletes data, processes personal data under the terms and conditions set out within the Police Code[9] and special law. The police also keep track of personal and other data in order to prevent and detect crimes and misdemeanors, as well as finding and arresting the offenders.[10]

Police processes personal data when there are grounds for suspicion that the person has committed, is or has been involved in planning, organizing, financing or execution of a crime.

In accordance with Article 67 of the Police Code, Personal Information includes: first and last name, data of birth (day, month, year and place), residence or domicile, personal identification number and address, citizenship, and other data that can directly or indirectly identify a person.

Personal data relating exclusively to racial origin, religious belief, sexual behavior or political opinion, membership of a specific movement or organization

[6] Article 7, CPPD;
[7] Article 7-a CPPD;
[8] Article 37 CPPD, the official web site of the Directorate is www.dzlp.com.mk ;
[9] Police Code (Official Gazette no. 114/2006; 6/2009 and 145/2012), hereinafter PC;
[10] Article 66 PC. According article 14 from PC, the Bureau of Public Security, which is a body within the Ministry of Interior affairs is in charge for the personal data on the territory of the whole Republic, and on local level, in accordance with Article 21 of the same Code, the Department of interior affairs is in charge;

established by law, and other special categories of personal data identified by a special law, cannot be collected by the police. Notwithstanding, police can collect these data under the terms and conditions set forth by this Code or a special law, but only when this is extremely necessary for the purposes of a specific investigation.

When the police are collecting personal and other data for using them as evidence of crimes or offenses with the purpose to identify the perpetrators, police officers may use technical resources to capture and record video and audio in a manner and under conditions determined by law.

When the police officers are collecting personal and other data from other persons or from existing data sets if the informing of the person to whom these data refers is obstructing or hindering the performance of the police work, the police officers are not always required to inform them. For the collected data the operating officer prepares a report, which is submitted to the immediate superior performing officer who makes a valuation and submits it to the competent organizational unit for further action.

Within the criminal proceedings, the court, the prosecution and other agencies with special powers, collect, process and store personal data for the purposes of criminal proceedings, taking into account the nature and scope of the data relevant to the needs in the relevant case. The latter is in accordance with the international principles of proportionality, necessity and relevance of the processing of personal data. The data stored in the proceedings must be correct. Personal data that is not accurate or is collected contrary to law, must immediately be changed or deleted. The accuracy of personal data in the data sets is checked every five years, as is determined by the law that establishes the data sets. Deadlines for storage and deletion of personal data from the data sets are determined by the law that established the data sets.[11]

The first, initial taking of personal data in the criminal proceedings is when the accused is first asked for his first and last name, his nickname if any, the name and surname of the parents, the maiden name of mother, place of birth, place of residence, date, month and year of birth, personal identification number, ethnical belonging, citizenship, occupation, family situation, education, property; whether, when and why the person had been earlier convicted; if and when the person has served a sentence, whether there are other proceedings against him/her for another crime, and if he/she is a minor who is his legal representative.[12]

The personal data subjects have the right to be informed of the use or collecting and storing of their personal data. If the law does not provide otherwise, the public prosecutor or the court shall inform the data subjects, upon request, about whether their personal data have been collected, processed or held for the purposes of criminal proceedings. But the public prosecutor or the court cannot inform the

[11] Article 140 of Law of Criminal Procedure, Official Gazette no. 150 from 18.11.2010, hereinafter CPC;

[12] Article 205 of CPC;

data subjects prior to the expiration of one year from the date of issuance of the order for conducting the investigation.[13]

Data subjects have the right to access and correct their personal information held by the police. This may be limited if the restriction is necessary for performing the statutory powers of the police to prevent, detect and prosecute perpetrators of crimes and misdemeanors, in order to maintain public safety or when it is necessary for the protection of the personal data or the rights and freedoms of others.[14]

Criminal Procedure Code also provides provision of personal data for users. Users, in term of this code, are public authorities and other legal entities and natural persons. The latter ones are conditioned with giving a legal basis for the access to others' personal data. The personal data that is provided to users, can be used in accordance with the law, in other criminal proceedings, in proceedings of international cooperation in criminal matters and international police cooperation. In other litigations, personal data may be used only if the subject is directly related to the subject of criminal proceedings.

Personal data that is collected solely on the basis for determining the identity, physical examination or molecular-genetic analysis, after completing the determination of the criminal proceedings may only be used in accordance with the law, only to detect or prevent crime.[15]

Supervision of the processing of personal data and their protection within the police work and during the criminal proceedings is performed by the Directorate for Personal Data Protection. Regulations concerning the protection of personal data will apply on the collection, processing and storage of personal data for the purposes of criminal proceedings.

Data protection is extremely important in cases when there is use of special investigative measures because of the substantial intrusion into the sphere of privacy.

The protection of personal data in the use of special investigative measures. The Council of Europe defines special investigative measures with the following meaning: "special investigation techniques" means techniques applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target persons.[16]

[13] Article 142 of CPC;
[14] Article 76 of PC;
[15] Article 141 CPC;
[16] Rec(2005)10, Council of Europe, Committee of Ministers, Recommendation Rec(2005)10 of the Committee of Ministers to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism (20 April 2005), Rec(2005)10, available at https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=CM last access 06.03.2013;

The special investigative measures, which essentially interfere into privacy, can be applied only when it is likely to provide information and evidence necessary for successful criminal procedure, which otherwise cannot be collected.[17]

On the one hand, it is recognized that the methods of secret monitoring, recording and taping are a threat to democracy and human rights and on the other hand, there is recognition that democratic societies today are threatened by sophisticated forms of crime, espionage and terrorism, and therefore States must have a means by which they can effectively confront these threats. Hence, only a reasonable compromise between the requirements for protection of democratic society and individual rights can be accepted. The main idea is to find a model that serves both.

After the adoption of the constitution in 1991, until the constitutional amendments to the provisions on privacy, the law and practice in our country were extremely unsatisfactory precisely because, on the one hand, we had an unrealistic ultraliberal constitutional solution that prohibited every taping, and on the other hand real, intolerable legal uncontrolled practice of eavesdropping. In this sense, certain constitutional and legislative changes were necessary.[18]

In Macedonia, the first investigative measures were introduced with the novel of the CPC in 2004. Given the fact that the old code is still a current one, we have had a long period of their application which allows us to assess objectively how these special investigative measures were applied in practice, which legislative changes that have caused an impact on and their impact on the right to privacy and protection on personal data. All of this is in the threshold of the entry into force on the new Criminal Procedure Code which provides new and more numerous special investigative measures that affect privacy a lot more.

The former and current CPC[19] provides the following special investigative measures: 1) the interception of communications and entering homes and other premises or vehicles to create the conditions for interception under conditions and procedures specified by law, 2) review and search in computer system, seizing of computer system, a part of it or a database for storing computer data, 3) secret surveillance, monitoring and audio-visual recording of persons and subjects with technical means, 4) virtual (simulated) purchase of items and seeming (simulated) giving bribery and seeming (simulated) accepting bribery, 5) controlled delivery and transportation of persons and objects, 6) use of undercover agents to monitor and collect information or data; 7) opening apparent (simulated) bank account for

[17] Lazetic – Buzarovska, G., Kalajdziev, G.,: Investigation – Manual for practitioners, Skopje, OSCE, 2010, p.31, (published in Macedonian language);

[18] Matovski, N., Lazetic – Buzarovska, G., Kalajdziev, G.,: Criminal Procedure Law, Second and amended issue, Academic LTD, Skopje, p.263, (published in Macedonian language);

[19] Criminal Procedure Code, Official Gazette no. 15/1997; 44/2002; 74/2004; 83/2008; 67/2009 и 51/2011, hereinafter former and current CPC;

the purpose of transfer of funds derived from crime and 8) registration of seeming (simulated) entities or using existing entities for data collection.

The purpose of the special investigative measures is data, reports, documents and objects obtained by its application, under conditions determined by the CPC, to be used as evidence in criminal proceedings. In case of inadequacies in their application - evidence derived from them cannot be used as evidence.

During the preliminary investigation, special investigative measures are assigned with a decision in the form of an order from the public prosecutor or the investigating judge (upon written proposal of the public prosecutor), and in previous investigation procedure, only with an order of the investigating judge.

Exceptionally, in cases of emergency, where the delay can cause irreparable consequences for the successful conduct of the proceedings, the investigating judge, on a previous proposal of the Public prosecutor, may issue a verbal order that will allow monitoring of communications based solely on verbal command.[20]

The new CPC provided the following special investigative measures: 1) monitoring and recording of telephone and other electronic communications in a procedure established by a special law, 2) monitoring and recording home, indoor or enclosed space that belongs to that home or office space labeled as private or vehicle, and entering in these premises with the purpose of creating conditions for interception, 3) secret monitoring and recording of persons and subjects with technical means outside their home or business premises designated as private, 4) secret insight and search in a computer system and 5) automatic or other, search and comparison of personal data, 6) inspect in generated telephone and other electronic communications; 7) simulated purchase of objects; 8) simulated giving and receiving bribes, 9) controlled delivery and transport of persons and objects; 10) using undercover agents to monitor and collect information or data; 11) simulated opening of a bank account and 12) simulated registering of entities or using existing entities for data collection.[21]

The lawful application of these old and new measures remains to be seen. In advance we can only say that this law has many critical points in terms of privacy. Thus the growing number of special investigative measures implicates of an increased opportunities for infringement of privacy during their use. Here are a few "critical points". In this sense, Article 255, determines who can be the subject of special investigative measures. So, special investigative measures can be appointed not only for a person who has committed a crime under Article 253 of this Law or the person who takes action to commit a crime or preparing to commit a criminal offense under Article 253, but also for a person who receives or forwards shipments from the suspect or when the suspect uses his communication device. This means that the investigation can be expanded in terms of the subject? How long this person

[20] Article 11-a Amending Law on the Code for interception on communications, 2008;
[21] Article 252 from the new CPC;

would be monitored: only when the suspect is present or until the investigation is complete. We don`t have answer on these questions, and we don't expect to have even after the application of the new CPC, because judged by past practice, investigators successfully hide the exceeding of special investigative measures. Our opinion is that there is a risk of over-collection of personal data, which can cause a serious attack on privacy. In these situations, the initial gathering of information cannot be called inappropriate. However, once it is determined that the person is not included, the authorities should not proceed with the collection of information (or, to retain and use the information they have collected).

If this is done there is a risk to gather information on a larger scale - for example, collecting information about people associated with the suspect or civil society which they belong to. This can have a negative effect, and lead people in a state of fear of participation in such civic organizations as legal unions, political parties and etc.[22] Of course, the fact that the using of special investigative measures gives immediate results of the investigation, it is not in favor of the legality of their application because investigators find them as a first resort to facilitate and speed up the investigation, instead of using them in extremely necessary situations.

The law provides a special investigative measure - automatic or other search and comparison of personal data of citizens. This technique consists of automatic or other search and comparison of collections of personal data of personas, or other data directly related to them, and their comparison with certain characteristics of the person which is suspected to be related to the crime, in order to exclude persons not connected to the crime or to determine individuals who possess characteristics that are needed for the investigation. We wonder how many people will be included in this comparison. In addition, this provision is worded with extremely wide range. This practically means that everybody is under suspicion and in any given moment can be held at a police station "in order to exclude them from the list of suspects." The frightening fact is that this will be legitimate, legally based and approved by the court. Also a "Boiling Point" is the provision that gives unnecessary long term[23] for storage of personal data in the event of a use of a special investigative measure with the application of Article 252 paragraph 1 point 5. Hence, deletion of personal data, in cases where the decision is not to initiate a criminal proceeding, is after 15 months. After 15 months, the collected personal data will be deleted or destroyed under the supervision of the preliminary proceedings judge, the prosecutor and the representative of the Directorate for Personal Data Protection for what the Public Prosecutor will make transcript.

Monitoring of communications: A serious threat to the right to privacy. The right to privacy and the right to protection of personal data repeatedly were and still are a target of inappropriate legislation leading to erosion of these two

[22] Haton, L.: Supervision in collecting information, p.109, (published in Macedonian language);

[23] Comparative, this term in the legislation of the EU countries is 6-12 mounts;

fundamental human rights. The serious lack of provisions in the Law on Electronic Communications[24] has resulted in their revoke by the Constitutional Court.[25] So, the alleged "technical" Law on Electronic Communications in fact made invasion of privacy.[26] Specifically, the Law Amending the Law on Electronic Communications was in direct conflict with the general law governing the interception of communications - Law on interception of communications and the Law of criminal procedure, the Constitution, the international instruments ratified by Republic of Macedonia and as such are part of our legal system, as well as Article 5 of the Code on protection of personal data. The Helsinki Committee for Human Rights in Republic of Macedonia[27] filed a motion to the Constitutional Court which corrected the mistake of the legislature. Revoked provisions of the law, derogated the existing legal and constitutional norms, giving the authorities (Ministry of Internal affairs) legal basis for interception of communications and unrestricted power to dispose of the data, bypassing any external control.[28] The given solutions were used to avoid the court, the prosecutor's office and even the operators.

As previously stated, the interception of communications is regulated by a special law - the Law on interception of communications.[29] This Law regulates the procedure for monitoring and recording of telephone and other electronic communications, handling, storage and use of data and evidence obtained through the interception of communications and control of the legality of the interception of communications. For the purposes of this law, the term "communication" refers to

[24] Law for electronic communications (Official Gazette no. 13/2005, 14/2007, 55/2007, 98/2008 и 83/2010);

[25] Decision of the Constitutional Court of the Republic, U.no: 139/2010-0-0 from 20.10.2010 according to which the challenged provisions of the Law for Interception of Communications are revoked because of inaccuracy regarding the conditions and procedures which could result in deviation of the constitutionally guaranteed right to privacy, that according to the Court, represent real threat of arbitrary and arbitrary interference of state bodies in private life and correspondence of citizens which may adversely affect the reputation of citizens without a real basis in the Constitution and laws;

[26] Kalajdziev, G.: Erosion of privacy in Macedonia, Towards the amending of the Code of electronic communications, Helsinki Committee of human rights in Macedonia, June, 2010;

[27] Helsinki Committee for Human Rights in Republic of Macedonia: Successful Initiative to the Constitutional Court, available at http://www.mhc.org.mk/announcements/31?locale=mk#.UTSU_FddCno last access on 06.03.2013;

[28] Privacy under scrutiny: A brief analysis of the draft amendments to the Law on Electronic Communications - Helsinki Committee for Human Rights in Macedonia Article 112 paragraph 7 and art.114 paragraph 7 of the amended Act;

[29] Law of interception of communications (Official Gazette no.121/2006, 110/2008 and 116/2012), hereinafter LIC;

all types of telephone and other electronic communications, such as internet protocol, voice over internet protocol, web site and e-mail, and "interception" refers to secretly learning the content of communication and creating a technical record of the content of the communication, for the purpose of reproduce. The Public Prosecutor, the Ministry of Interior, the Financial Police, Customs and the Ministry of Defense are liable authorities for monitoring communications.[30] Giving the affirmation to the importance of interception of communication by regulating it with special law is of great importance. This also refers to the public responsibility of the state authorities that will monitor the communications. But all of this intrudes in the sphere of privacy. With this kind of measures, neither the police nor the prosecution and the court need other investigative measures. All they need is time for interception and recording the things they want to prove.

Request for the approval of order for interception of communications is submitted to the competent judge by the competent public prosecutor on his/her own initiative or by previous suggestion of the police officer at the Ministry of Interior or a member of the Financial Police, or the person authorized by law from Customs if they are leading the case. Any possible disputes between the prosecutor and the judge will be resolved in accordance with the CPP. The monitoring period is limited up to 4 months, but this period may be extended several times, to the total of 14 months, including the time determined by the first order issued for the interception of communications. This term is a bit longer – up to 6 months for interception of communications in cases when the interests and security of the state is affected. This period may be extended to a total of two years. Our opinion is that these periods for interception are disproportionately long, given the fact that the investigation is immediate and usually lasts much shorter than the total duration of these periods.

The positive reviews of this law can be addressed to the right to a legal protection of the person whose communication had been intercepted contrary to the provisions of this law. This person has the right to compensation before the competent court in an immediate procedure, which cannot last longer than three months. Also, this person has the right to appeal to a higher court within eight days of the reception of the verdict. The appellate court will decide for the appeal within eight days of its submission.

The law provides that the court may order the interception of communications when there are grounds to suspect that someone is preparing to commit a crime against the state, against the armed forces or against humanity and international law or prepares, promotes, organizes or participates in an armed attack against Macedonia or is disabling its security system. This is only when the authorities are unable otherwise to provide data on such activity or their provision

[30] The Ministry of Defense is authorized authority to monitor communications only in terms of the frequency spectrum of radio waves on high, very high and ultra-high frequency (HF, VHF and UHF) that are designated for the needs of the defense;

would be linked to greater difficulties to prevent the crime, armed attack or disability to the security system.[31] Our opinion is that if there are indeed any of the above threats to national security, privacy and protection of personal data should be sacrificed. But this sacrifice must be really necessary, on reasonable legal grounds and justified.

The request for approval of order for interception of communications may be submitted by the Minister of Interior and Minister of Defense or persons authorized by them. In this case the request for interception of communications will be submitted to the Public Prosecutor of the Republic of Macedonia, after which the Prosecutor will submit it to the Supreme Court of the Republic of Macedonia. The Judge of the Supreme Court will issue an order for interception on the facts and circumstances of the applicant if he/she considers that this is based on law. The data collected with the order for interception of communications will be stored at the Ministry of Interior or/and the Ministry of Defense under a special regime, at the longest period of five years after the time specified in the issued order.[32] The importance of national security is seen through the involved authorities for proposing, conducting, and making the interception of communications, which are from the highest level.

Supervision of the implementation of the special investigative measure - interception of communications by the Ministry of Interior, the Financial Police, Customs and the Ministry of Defense, is done by the Assembly of the Republic of Macedonia.[33]

Monitoring the use of special investigative measures. The court is liable to control or supervision the application of special investigative measures. We think that in general, the judiciary control is desirable, especially in the area where the abuse is potentially so easy in individual cases, and can have very harmful consequences for a democratic society.[34] But the low level of criticality in our judiciary has proved many times that this is not our most appropriate solution, although another real solution won't be adequate for our legal system. Courts give the impression that they are a partner of the police and the prosecution in law enforcement, rather than as their controller.[35]

The legislature has also provided control and supervision over the implementation of special investigative measures by the public prosecutor, which is not a functional solution, given that the public prosecutor has major responsibilities in the process of proposing and extension of the measure, so there is a reasonable

[31] Article 29 of LIC;
[32] Article 34 LIC;
[33] Article 35 of LIC;
[34] Matovski, N., Lazetic – Buzarovska, G., Kalajdziev, G.,: Criminal Procedure Law, Second and amended issue, Academic LTD, Skopje, p.263, (published in Macedonian language);
[35] Ibid, p. 267;

doubt for a kind of conflict of interest among the public prosecutor, which in this situation is not impartial entity exercising control and supervision over the practical implementation of the measure. We give the same remark which we gave to the court. We think that the Public Prosecutor has also developed servile attitude towards the Ministry of internal affairs and doesn't show great enthusiasm for some control over the police.[36] Even you can observe that in practice it is contrary to what the law provides. Instead the police to be in service of the prosecutors, prosecutors are placed in the police service.

There is also, another type of supervision - supervision by the Parliamentary Commission for Supervision of the interception. This Commission is not responsible for overseeing the execution of all special investigative measures but only for the interception of communications. The composition of the Commission[37] gives too much political context of something that in democratic countries would be monitored by an independent court. Given the current position of the judiciary in our country, the Commission is not redundant but desirable. A serious disadvantage is that its position is formal and as such is prescribed in the Law to intercept communications. Apart from the annual report that is submitted to the Parliament and the meetings on the Commission we do not see any activity that would give a positive result. Our opinion is that this must change. It is desirable to have more Commissions that would monitor legality of all the special investigative measures, but only if these Commissions have greater authority than the jurisdiction of Commission for supervision of the interception. But it seems that there is some purpose for the inexistence of a clear normative framework or practice to achieve the control and supervision of specific mechanisms and procedures. Thus, the Ministry of Internal Affairs opens its way to monitor citizens in a very easy way. We can even say that the Ministry of Internal Affairs is "playing around" with the parliamentary committee and its task to supervise the legality of the interception of communications. In any normal democratic state based on the separation of powers and the rule of law, this would be considered as a scandal, but in our country it is almost treated as just another inter-party dispute.[38]

Hence, we can conclude that there is no system for effective, external and constant control over the special investigative measures in terms that these measures are really applied on lawful grounds and in legal proceedings with all guarantees against arbitrariness and abuse.

[36] As in: Control over wiretapping, Helsinki Committee for Human Rights of the Republic Macedonia;

[37] Two members from the opposition, two members of the ruling coalition and a president from the opposition;

[38] As in Quarterly Report December 2011 - February 2012, the Helsinki Committee for Human Rights of the Republic, available on the site http://www.mhc.org.mk/reports/50?locale=mk#.UTiT7lckQcE last seen 07.03.2013;

Our opinion is that a cautious approach is required in the application of special investigative measures, in their compliance with the principles of domestic law, so they do not come into collision with the fundamental human rights and freedoms.[39]

At the end we only applaud the new solutions in the new CPC where for the application of special investigative measures, the Attorney General is obliged to submit an annual report to the Parliament. Unlike the current CPC, where the supervision over all investigative measures is in hand of the court, except for the interception of communications, with the new CPC the Prosecutor is obliged to report to Parliament. It remains to see how this responsibility in practice would be really useful. In today's surroundings of highly strained relations between the ruling party and the opposition, it remains to be seen how this responsibility will avoid political context and threatening. We are more certain are that over time this responsibility will be reduced to a mere formality.

Recommendations for successful balance between privacy and special investigative measures. The conduct of criminal proceedings and the protection of national security are legitimate aims for limiting human rights such as the right to privacy but all restrictions must be in accordance with national legislation, which must include safeguards against abuse and remedies in case of abuse.

At the end, it is necessary to provide some brief references to domestic law in favor of the lawful use of special investigative measures that violate privacy and limit the fundamental right to protection of personal data.

As previously stated, the state is often able to justify the use of the special investigative measures, but has difficulty is in proving that the interference in private life was necessary in this case. Hence, our recommendation for each application of special investigative measures is to fulfill cumulatively two conditions: first, the use of such measure to be necessary in that case, and second, and its use to be in accordance with law. "Necessary" means that the interference in the private life of the individual is to address the "urgent social need"[40]. In other words the interference is not to be only reasonable but also proportional to the aim pursued. The term "proportionality"[41] involves two moments: the proportionality in applying special investigative measures and means used for the purpose of the proceeding, and proportionality and fair balance between the general interests of the community and the protection of individual rights. At the same time, the state authorities must show that the interference in the private life of the individual was

[39] Kambovski, V.: International legal framework in fight against corruption, Fredrick Ebert Foundation, Skopje, p.16, (published in Macedonian language);

[40] See Sunday Times vs. United Kingdom, 1980, 2 EHRR 245;

[41] For more on proportionality see Haton – Supervising collecting of personal data, p.109;

not greater than necessary. Also the interference should be strongly argued and elaborated with reasonable arguments.[42]

Second, when using any of the special investigative measures, the authorities need to know how, and to accept the fact that the result of the investigation on the suspect can be negative. They should not seek for a way to extend the use of the special investigative measures or to make persistent, unjustified invasion of privacy which in these cases can never be justified.

Third, the authorities should always apply less intrusive and more appropriate measures which are effective as well as the more intrusive ones. This is because in some cases the less intrusive measures give the same result with a minimal invasion of privacy and without derogation abuse of human rights. This reference is of particular importance because our authorities are not taking into account the extent which leads to minimal violation of human rights. Instead they seek for a measure that will promptly give the expected result with minimal effort.

Fourth, it is necessary to establish a strong, uncontradictive and undisputable legal framework, as an appropriate basis for the use of special investigative measures for collection of data, guaranteeing that they should be used only when they are proportionate to the aim. The legal framework should be adapted to the level of intrusion. This means the greater is the level of intrusion, the higher should be the level of authority that decides for the intrusion. According to this, there should always be a judicial authorization for the use of measures in order to prevent arbitrariness and abuse.

Fifth, the supervision of the special investigative measures should be continuous, uninterrupted, real, with no political context, and especially not to be formal with quarterly or monthly reports that will neither reach the public eye, nor will have some legal force that would prevent further abuse.

Sixth, there must be sanctions for those who would overstep their authority or unlawfully apply special investigative measures, without an order of the court and out of any legal procedure.

Seventh, all of the reasons that justify the use of special investigative measures must be clearly defined and elaborated. The use of generic terms like "imminent danger of execution ..." or "endangering national security" which are too general and not specified in practice should be forbidden. These terms, in practice, give extensive opportunities for violating the rights of citizens.[43] The terminological confusion and uncertainties in this field is absolutely impermissible.

[42] So as Matovski, N., Lazetic – Buzarovska, G., Kalajdziev, G. (2012): Criminal procedure Law, p.264-5, (published in Macedonian language);

[43] See in Kalajdziev, G., Jovcevski, J.: The Right to respect privacy in Macedonia, Macedonian review for Criminal law and Criminology, no.1, 2009, 2 August – S, Stip, p.267-285, (published in Macedonian language);

Eighth, disabling the light marginalization of privacy in the use of special investigative measures and disabling any arbitrariness and abuses in the proceedings.

Ninth, amending the law regarding the categories of persons who may be subjected to the use of special investigative measures, thus providing clear determination. Also, determining whether the number of people that are being monitored can be extended, and if so which cases precisely. Provisions of the law that currently regulate these issues are unacceptably too generic.

Tenth, specifying rules for storage, collection and destruction of data collected in criminal proceedings.

Finally, the area of national security, public safety and defense must have stricter safeguards and principles that will be used by courts in order to justify the use of special investigative measures that are in continuous conflict with the rights and freedoms of the individual. Security services must first prove that there is a direct, immediate, concrete and serious treat, not just vague or possible threat.

Bibliography (In Order of Appearance)

European Convention on Human Rights and Fundamental Freedoms from 1950. The translation of the Convention and its Protocols in Macedonian language are available in “Official Gazette" no. 11/1997, 30/2004 and 30/2005;

The Convention 108 is ratified by the Assembly of Republic of Macedonia and came into force on 1st of July 2006 and its Additional Protocol was signed on 4th of January 2008.

Constitution of the Republic of Macedonia, adopted on 17 November 1991, Official Gazette no.52 of 11.22.1991, and changes in the Official Gazette no. 1/1992, 31/1998, 91/2001 84/2003, 107/2005, 3/2009, 13/2009 49/2011;

Kambovski, V., "Criminal Code - Integral text Preface, brief explanations of terms and registry, Skopje 2011, (published in Macedonian language);

Law for protection of personal data (Official Gazette no.7/2005, 103/2008; 124/2008; 124/2010 and 135/2011), hereafter CPPD;

Official web site of the Directorate for protection on personal data is www.dzlp.com.mk ;

Police Code (Official Gazette no. 114/2006; 6/2009 and 145/2012), hereinafter PC;

Law of Criminal Procedure, Official Gazette no. 150 from 18.11.2010;

Rec(2005)10, Council of Europe, Committee of Ministers, Recommendation Rec(2005)10 of the Committee of Ministers to member states on “special investigation techniques” in relation to serious crimes including acts of terrorism (20 April 2005), Rec(2005)10, available at

https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=CM last access 06.03.2013;
Lazetic – Buzarovska, G., Kalajdziev, G.,: Investigation – Manual for practitioners, Skopje, OSCE, 2010, p.31, (published in Macedonian language);
Matovski, N., Lazetic – Buzarovska, G., Kalajdziev, G.,: Criminal Procedure Law, Second and amended issue, Academic LTD, Skopje, p.263, (published in Macedonian language);
Law of Criminal Procedure, Official Gazette no. 15/1997; 44/2002; 74/2004; 83/2008; 67/2009 и 51/2011, hereinafter former and current CPC;
Amending Law on the Code for interception on communications, 2008;
Haton, L.: Supervision in collecting information, p.109;
Law for electronic communications (Official Gazette no. 13/2005, 14/2007, 55/2007, 98/2008 и 83/2010);
Decision of the Constitutional Court of the Republic, U.no: 139/2010-0-0 from 20.10.2010
Kalajdziev, G.: Erosion of privacy in Macedonia, Towards the amending of the Code of electronic communications, Helsinki Committee of human rights in Macedonia, June, 2010, (published in Macedonian language);
Helsinki Committee for Human Rights in Republic of Macedonia: Successful Initiative to the Constitutional Court, available at http://www.mhc.org.mk/announcements/31?locale=mk#.UTSU_FddCno last access on 06.03.2013;
Privacy under scrutiny: A brief analysis of the draft amendments to the Law on Electronic Communications - Helsinki Committee for Human Rights in Macedonia Article 112 paragraph 7 and art.114 paragraph 7 of the amended Act;
Law of interception of communications (Official Gazette no.121/2006, 110/2008 and 116/2012), hereinafter LIC;
Control over wiretapping, Helsinki Committee for Human Rights of the Republic Macedonia;
Quarterly Report December 2011 - February 2012, the Helsinki Committee for Human Rights of the Republic, available on the site http://www.mhc.org.mk/reports/50?locale=mk#.UTiT7lckQcE last seen 07.03.2013;
Kambovski, V.: International legal framework in fight against corruption, Fredrick Ebert Foundation, Skopje, p.16, (published in Macedonian language);
Sunday Times vs. United Kingdom, 1980, 2 EHRR 245;
Kalajdziev, G., Jovcevski, J.: The Right to respect privacy in Macedonia, Macedonian review for Criminal law and Criminology, no.1, 2009, 2 August – S, Stip, p.267-285, (published in Macedonian language);