NBP 2021, Vol. 26, Issue 2, pp. 43–52
https://doi.org/10.5937/nabepo26-33542
Original scientific paper

Control and Supervision of the Implementation of Measures for Interception of Communications: The Macedonian Case

[1]Ice Ilijevski[1], [2]Katerina Krstevska Savovska[2]

[1]St. Kliment Ohridski University, Bitola, Faculty of Law – Kicevo, Republic of North Macedonia

[2]St. Kliment Ohridski University, Bitola, Faculty of Security – Skopje, Republic of North Macedonia

Submitted: 2021-08-13; Accepted: 2021-11-08; Published: 2021-11-23

Abstract: The implementation of the measures for interception of communications is a useful tool in fighting organized crime and endangering public and national security. However, if they are not in accordance with the law, their implementation can seriously jeopardize the privacy of individuals. In the past, there had been several Macedonian affairs related to the illegal surveillance of communication that caused reformation of the system for interception of communications. Therefore, if certain inconsistencies are timely detected and signalized by the representatives of the control and supervising bodies, then there should be an adequate reaction for protection of the general values of the democratic society. Having in mind the above, the paper will give an overview of the current Macedonian situation regarding the system of control and supervision of the measures for interception of communications, or to be more precise - it will analyse the institutions and bodies that have authority to control and supervise. A special emphasis will be given to the deficiencies and weaknesses of this system, as well as the necessity for its upgrading and improving in order to prevent possible abuses in the future.

Keywords: control, supervision, interception, communications, special investigative measures.

Graphical abstract

1 https://orcid.org/0000-0002-8515-2032
2 Corresponding author: katerina.krstevska@gmail.com

Citation: Ilijevski, I., & Krstevska, K. (2021). Control and supervision of the implementation of measures for interception of communications: The Macedonian case. *NBP. Nauka, bezbednost, policija*, *26*(2), 43–52. https://doi.org/10.5937/nabepo26-33542

ISSN 2620-0406

INTRODUCTION

Having in mind the threats and risks of the internal security, the countries have provided a significant authority to the security-intelligence and counterintelligence agencies and services in order to fight against terrorism, espionage, organized crime or other illegal acts that have an aim to threaten or undermine the democratic society. Such authorities usually have a high degree of secrecy that can be misused and can lead to illegal and unauthorized actions, inefficiency, abuse of power, but they can also be used for political goals. In order the given authorities not to be abused and not to intrude into the human rights and freedoms, it is necessary to conduct an appropriate control and supervision of them. Moreover, the security-intelligence services, as a part of the state executive governance, must be within the system of control and supervision and must strictly obey the rule of law principle.

The seriousness of the global threats through all forms of modern crime has imposed the need for the communications to be intercepted. This produces an overlap between the security as a public interest and the privacy as a personal right, i.e. the privacy can be restricted in order for the national and public security to be protected. However, this should be done in cases where the usage of such measures is the only way to protect the national and public interest. In addition, the establishment of an efficient system of control and supervision of the implementation of the measures of interception of communications must be in accordance with the principles of democracy, transparency and accountability, and finally - in accordance with the principle of privacy.

The purpose of controlling the security system (as part of the state administration bodies) is twofold. On the one hand, it provides legality and expediency in the work and realization of the public interest within the framework of the legal order. This can be achieved by removing certain illegal activities that can occur within the security system, correcting and directing certain phases in the legal procedure and throughout efficient process of building and upgrading the security system. On the other hand, the control over the security system provides the protection of citizens and their organizations from illegal actions of certain segments of the same security system (Bakreski, 2014).

In essence, the control and supervision over the implementation of measures for interception of communications is performed by different entities with a help of various mechanisms. Since their adjustment and position within the system do not usually offer sufficient efficiency and effectiveness during the realization, a constant promotion and improvement is required.

Given the fact that the public is always interested in the work of the security and intelligence services, there is a need for broader transparency of the entities that perform control/supervision, in order for the public suspicion in these organizations to be reduced and the public confidence in them to be increased (Geneva Centre for Security Sector Governance [DCAF], 2021).

The independence of oversight bodies should be enshrined in law and applied in practice (European Union Agency for Fundamental Rights, 2018). Although quite exploited, an emphasis should be given to the Report and Recommendations of the Senior Experts' Group, that was leaded by Reinhard Priebe, on systemic Rule of Law issues relating to the communications interception revealed in Spring 2015 (European Commission, 2015). These documents clearly noted the shortcomings of the control and supervision over the security system and the guidelines that should be followed. Additionally, detailed recommendations were given in the document titled Urgent Reform Priorities (European Union, 2015).

As a result of the reforms of the system for interception of communications, in 2018 a new Law on Interception of Communications (LIC) was adopted by the Macedonian Assembly (Law on Interception of Communications [LIC], 2018) allowing communications to be intercepted in order to detect and prosecute perpetrators of criminal acts, as well as to protect the interests of security and defence of the state. LIC also introduced specific safeguards, such as a control and supervision of the interception of communications. Furthermore, the Law on Operational-Technical Agency was adopted (Law on Operational-Technical Agency, 2018, 2019), establishing a new body known as OTA (Operational-Technical Agency) with a task to act as an intermediary between the authorized authorities for interception of communications and telecommunication operators in order to avoid concentration of power in one authority, and to ensure that the interception of communications will be based solely on law and appropriate court decisions. OTA was designed as a buffer zone between the authorized authorities that are using the interceptions and the operators, and by doing so – the function of expert supervision over the system for interception of communications is performed. This Law also regulates the OTA's competencies, management, professional supervision as well as its financing.

Having in mind the above, by introducing such reform into the Macedonian security-intelligence system, instead of the Security and Counterintelligence Directorate a new independent body of the state administration and outside of the Ministry of Internal Affairs was established - known as a National Security Agency (Law on National Security Agency, 2019). The Agency, that has a status of a legal entity, can secretly collect data and information by intercepting the communications, it can monitor and record telephone and other electronic communications with a special technical devices and equipment without the intermediation of OTA and the operators; it can use secret collaborators, as well as persons with concealed identities; it can supervise postal and other shipments, etc.

Finally, the interception of communications is also prescribed as a special investigative measure in the Law on Criminal Procedure – LCP (Law on Criminal Procedure [LCP], 2010, 2012, 2018). The Law dedicates a separate chapter to these measures, i.e. the Chapter XIX, where it is stipulated that special investigative measures can be used – including the monitoring and recording of the telephone and other electronic communications – when it is necessary to obtain data and evidence for successful conduct of criminal procedure, which cannot be obtained by other means. In essence, one of the most commonly used explanations for the necessity to prescribe special investigative measures, given by the Macedonian relevant authorities, is to respond to the new challenges in the fight against

organized crime and its forms, by introducing a new procedural solutions, particularly by introducing special investigative measures (Krstevska & Todorovski, 2012).

Consequently, these reforms in the legal system have increased the number of authorities, beside the Macedonian Assembly, that can supervise the interception of communications. Their spheres of supervision are given in the Table 1 (Nikolov, 2019).

Table 1. *Supervisory authorities over the implementation of the measures for interception of communications*

Supervisory authorities	Legality	Effectiveness	Efficiency
Assembly	☑	☑	
Civic Oversight Council	☑		
Directorate for Security of Classified Information	☑		
Personal Data Protection Agency	☑		
Ombudsman	☑		

JUDICIAL AND PROSECUTORIAL CONTROL

The judicial and prosecutorial control is carried out when it is needed and without a prior notice, as well as there are no restrictions on the scope, width and type of activities and data that can be controlled towards the competent authorities for implementation of the special investigative measures, the operators and OTA. Namely, the control over the legality of the implementation of the measures for interception of communications for the purposes of the criminal procedure by the authorized enforcement authorities, the operators and OTA is conducted by the public prosecutor in charge of the investigative procedure and the judge of the pre-trial procedure who had issued the order for the special investigative measure. In addition, when it comes to the measures for interception of communications for the interests of security and defence of the state, then the control is conducted by the Chief Public Prosecutor and the judge of the Supreme Court who had issued the order for interception of communications.

Based on the legal provisions, the control is restricted to the legality of the measures' implementation (Articles 57-61 of the LIC) and is, as a rule, *ex post*, but considering that both institutions are directly involved in the procedure from the very approval of the measures until the final use of the obtained data as evidence in the criminal procedure, the control is always *ex ante* (principle of prior judicial approval of measures) but also continual (reports on continual implementation, extension and expansion of the measures). Besides the direct form of (field) control, which is recommended, there is also an indirect control that is achieved by way of analyses of the obtained reports from the implemented measures for the interception of communications and other official documents related to the use of the measures by the competent authorities, OTA and operators (DCAF, 2019).

For the purpose of conducting successful control (Articles 58 and 59 of the LIC), the law incorporates the option of hiring technical experts from the order of registered experts, who can employ their expertise to support the court or the public prosecutor's office in conducting technical control of the intermediary devices and equipment for the interception of communications in the work stations of the competent authorities for the implementation of the measures, i.e. OTA, the operators, the Basic Public Prosecutor's Office for Organized Crime and Corruption and the National Security Agency. The technical control is the only objective control that proves without a doubt the existence of unlawful interception of communications. This is carried out by comparing the similarity of the electronic logs (that are automatically generated) in intermediary devices at the work stations of the competent authorities, OTA and the operators, and special technical devices and equipment on the premises of the Basic Prosecutor's Office for Organized Crime and Corruption (DCAF, 2019).

Even though in theory these are solid provisions, still they are a novelty in terms of the work of these institutions since there has been a complete lack of judicial control over the measures for interception of communications related to the national security. Therefore, major efforts will have to be exerted for capacity building – both at the level of technical possibilities, support and understanding of the matter and on the level of building an awareness regarding the importance of a consistent performance of this important task (Lembovska, 2020).

In accordance with the LCP's Article 271, the Macedonian Chief Public Prosecutor is obliged once a year to submit a report to the Assembly regarding the implementation of the special investigative measures requested during the previous calendar year. The annual reports so far contain only statistical data on the number and type of special investigative measures implied, the criminal acts for which the measures were imposed, the number of persons, etc. From these reports it can be concluded that the most applied special investigative measure was the monitoring and recording of the telephone and other electronic communications within a procedure stipulated with a separate law, compared to other measures determined by the LCP (Public Prosecutor's Office, 2014–2019).

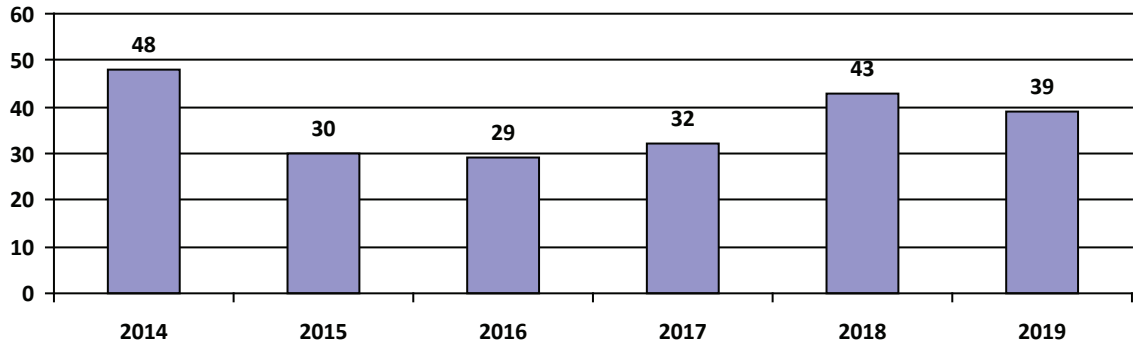

Figure 1. *Number of cases in which the measure of monitoring and recording of the telephone and other electronic communications was applied within a procedure stipulated with a separate law*

ASSEMBLY

The Macedonian Assembly has an obligation to ensure that the executive authorities work for the benefit of the citizens, and this is usually done throughout its working bodies, i.e. commissions. They are necessary since they allow security issues to be discussed on a multi-party basis, and among them the most important is the work of the Commission for supervision of the implementation of measures for interception of communications (the Commission). The Commission is composed of the President, four members, a deputy President and four deputy members, where the President and the deputy President are from the largest political party in the opposition, and also the opposition has a majority. This ensures balance and empowers the opposition to oversee special investigative measures. In essence, the Commission reviews issues related to (Assembly of the Republic of North Macedonia, 2018):

- Supervising the implementation of measures for interception of communications;
- Determining the legality of the implementation of the measures for interception of communications by the authorized bodies (OTA);
- Determining the effectiveness of the implementation of special investigative measures;
- Drafting report on the performed supervision;
- Establishing international cooperation on issues related to such supervision;
- Other issues related to the Authorized Authorities (OTAs) for the implementation of measures for the interception of communications.

In order for the supervision to be performed effectively, based on the LIC's Article 39, the Commission may engage national and international technical experts in possession of the appropriate expert knowledge, who can actively participate in the supervision upon their accreditation as part of the Commission.

The supervision performed by this Commission towards OTA and the operators, according to Articles 41–43 of LIC, is limited only to insight of the anonymized court order and the check on the logs - automatically created and processed electronic data in the mediation technical devices in the operators and in OTA regarding the time of initiation and termination of the measures, the number of anonymized court orders and the total number of implemented measures in a certain period of time, while in the authorized bodies, the supervision is limited only to the insight in the anonymized court order and the documents referring to the initiation and termination of the implementation of the measure. Moreover, the Commission does not have the availability to obtain data on the content of the communication and the true identity of the person whose communication is monitored.

If the current composition of this Commission is taken into consideration from the aspect of expertise and education (period 2020–2024), there is a good basis for conducting a supervision because most of its members are in the field of law and IT sciences. However, having in mind the specificity and sensitivity of the issue, the Assembly should provide them with an additional technical assistance, i.e. professional and permanent technical staff.

CITIZEN SUPERVISION COUNCIL

Citizen Supervision Council (the Council) is a new supervisory body from the civil sector that is set up for the first time by the LIC, with the aim of exercising citizen supervision over the legality of the implementation of the measures for interception of communications. The Council, as an independent and autonomous body within the exercise of its competence, is composed of the President and six members elected by the Assembly. The Council, in accordance to the LIC's Article 51, has adopted the Rules of Procedure for its work regulating issues on the procedure and the manner of its work. In terms of action, the Council is authorized to perform supervision in two ways, upon its own initiative or upon a complaint submitted by a citizen.

The Council, upon its own initiative, can supervise the work of OTA and authorized bodies, with a previous announcement to them. This supervision is performed in order to compare the data from the anonymized copies of the orders for the needs of supervision and control for the period of the last three months. It should be noted that anonymization is a process in which all identifying elements listed in the order, including personal and other data, are removed in a way that ensures that the subject of the personal data can no longer be identified directly or indirectly. Hence, from such supervision, the Council's work is limited and boils down only to determining the number of orders for interception of communications, the duration of the measure and the identification number.

Concerning the Council's acting upon a filed complaint by a citizen, it comes down to submitting a request to the competent Assembly's Commission to perform a supervision in accordance to the LIC with the purpose of ascertaining whether the telephone number provided by the citizen is being or has been unlawfully intercepted in the last three months. The Commission's notification provided to the Council, for the purpose of preserving confidentiality of the interception of communication measures, shall only state whether in the specific case an infringement has been found or not. Also, after receiving a complaint, the Council is obliged to perform supervision in OTA and authorized bodies. Such LIC's provision, on the one hand, duplicates the work with the Assembly's Commission to which the complaint is submitted, but on the other hand leaves the opportunity for an independent supervision of the Council.

In the last period, i.e. since the election until today, the Council has faced several challenges in its work. The first obstacle in the work of the Council was its incomplete election, i.e. in January 2019 four members were elected, and the other three members were elected in May 2019. Regarding the provision of working conditions, the Council was only given the premises in the Assembly, while other material and technical conditions have not been provided yet. In June 2020, the President and two members resigned due to its non-functioning. The last country reports of the European Commission (European Commission, 2020) and the US Department of State (Bureau of Democracy, Human Rights, and Labor, 2020) note serious remarks about the non-functionality of the Council and the need to provide resources for its performance.

OTHER SUPERVISORY BODIES

a) Personal Data Protection Agency

The Personal Data Protection Agency plays an important role in ensuring the protection of the fundamental rights and freedoms of individuals in relation to the processing of their personal data. According to the LIP, it is one of the competent bodies for supervision of the implementation of the measures for interception of communications in order to determine the legitimacy of the undertaken activities during the personal data procession and the measures taken for their protection.

One of the most important instruments for ensuring the protection of personal data is the supervision, as stipulated by Article 102 of the Law on Personal Data Protection – LPDP (Law on Personal Data Protection, 2020), which is a systematic and independent control over the legality of the undertaken activities in processing personal data and their protection. It includes research, verification, guidance and prevention of personal data protection. Based on the annual programme, a regular supervision can be performed. In addition, an extraordinary supervision can also be performed, based on the proposal/initiative of a state body, legal or natural entity, *ex officio* or if the supervisor suspects that there has been a violation of the LPDP. Furthermore, as noted by LPDP's Article 104, control supervision can be performed in order to eliminate the ascertained violations. The conducted supervisions are followed with a report, containing the findings of the current situation and possible violations of the regulations related to personal data protection.

b) Directorate for Security of Classified Information

The Directorate for Security of Classified Information, established by the Law on Classified Information (Law on Classified Information, 2019), has a task to implement the policy for protection of classified information. The Directorate's oversight function is carried out by performing inspections in order to determine whether OTA and authorized bodies fulfil the conditions for handling classified information. The inspection, that can be regular, extraordinary or controlling, is performed by the inspectors for security of the classified information, who are authorized to (Article 83 and 85) supervise the implementation of the law and other regulations in the field of security of classified information, propose measures for elimination of the identified irregularities and shortcomings within a certain deadline and take other actions in accordance to the law.

c) Ombudsman

The Ombudsman has a significant role in supervising the implementation of measures for interception of communications, given that it protects the constitutional and legal rights of citizens when they have been violated by state administration bodies and other bodies and organizations that have public authority. According to the law (Law on the Ombudsman, 2003, 2009, 2016, 2018), the Ombudsman has a solid investigative authorities and can initiate investigations on its own authority based on the probable cause or on the assessment that abuses may occur. Furthermore, the Ombudsman has the authority to compel public institutions to provide information and detailed explanations regarding any complaint in a timely manner, as well as the right to enter into institutions' premises in order to access their documentation.

When the Ombudsman concludes that the constitutional and legal rights of the complainant have been violated or other irregularities have been made, he/she may: give recommendations, proposals, opinions and indications on the manner of eliminating the established violations; propose a certain procedure to be conducted again in accordance to the law; initiate a disciplinary procedure against an official, i.e. responsible person and submit a request to the competent public prosecutor for initiating a procedure for determining criminal liability.

CONCLUSION

Analysing the Macedonian situation, it can be concluded that there is solid ground for implementation of control and supervision over the implementation of measures for interception of communications, but there are also a number of shortcomings, omissions and weaknesses in the practical application of control and surveillance mechanisms.

Therefore, the inefficiency in the work of institutions and bodies conducting control and supervision so far can be overcome by introducing a new body, i.e. an Agency as a higher instance mechanism of control and supervision, as well as a body that shall perform parallel control and supervision, and by doing so - shall not allow violation of the human freedoms and rights of citizens guaranteed by the Constitution, laws and ratified international agreements (Ilijevski, 2016). By establishing such Agency, the principle of rule of law shall be obeyed and the professional capacity and public confidence shall be strengthened towards the organs and bodies of the security system and their employees.

REFERENCES

Assembly of the Republic of North Macedonia. (2018). *Commission for supervision of the implementation of measures for interception of communications.* https://www.sobranie.mk/rabotni-tela-2020-2024-ns_article-komisija-za-nadzor-nad-sproveduvanje-na-merkite-za-sledenje-na-komunikaciite-2020.nspx

Bureau of Democracy, Human Rights, and Labor. (2020). *Macedonia 2020 Human Rights Report.* https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/north-macedonia/

European Commission. (2015). *Recommendations of the Senior Experts' Group on systemic Rule of Law issues relating to the communications interception revealed in Spring 2015.* https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/news_corner/news/news-files/20150619_recommendations_of_the_senior_experts_group.pdf

European Commission. (2020). *Macedonia 2020 Report.* https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/north_macedonia_report_2020.pdf

European Union Agency for Fundamental Rights (FRA). (2018). *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the European Union (Vol. II).* https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu

European Union. (2015). *Urgent reform priorities for the Former Yugoslav Republic of Macedonia (June 2015)*. https://eeas.europa.eu/sites/default/files/urgent_reform_priorities_en.pdf

Geneva Centre for Security Sector Governance (DCAF). (2019). *Benchbook on the implementation of measures for interception of communications*. https://www.dcaf.ch/benchbook-implementation-measures-interception-communications.

Geneva Centre for Security Sector Governance (DCAF). (2021). *Common minimum standards for conducting control and surveillance visits to security and intelligence institutions in the Republic of Macedonia*. http://www.dcaf.ch/sites/default/files/publications/CommonMinimumStandardsOversightsVisits_ MKD_A4.pdf

Ilijevski, I. (2016). A proposed mechanism for enhancing the control and oversight of the security system of the Republic of Macedonia. *Contemporary trends in social control of crime*. St. Kliment Ohridski University, Faculty of Security – Skopje.

Krstevska, K., & Todorovski, Lj. (2012). The special investigative measures in the new Macedonian Law on Criminal Procedure. In M. Šikman (Ed.), *Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal* (pp. 409–421). Visoka škola unutrašnjih poslova.

Law on Classified Information, *Official Gazette of the Republic of Macedonia*, 275/2019.

Law on Criminal Procedure (LCP), *Official Gazette of the Republic of Macedonia*, 150/2010, 100/2012, 198/2018.

Law on Interception of Communications (LIC), *Official Gazette of the Republic of Macedonia*, 71/2018.

Law on National Security Agency, *Official Gazette of the Republic of Macedonia*, 108/2019.

Law on Operational-Technical Agency, *Official Gazette of the Republic of Macedonia*, 71/2018, 98/2019.

Law on Personal Data Protection (LPDP), *Official Gazette of the Republic of Macedonia*, 42/2020.

Law on the Ombudsman, *Official Gazette of the Republic of Macedonia*, 60/2003, 114/2009, 181/2016, 189/2016, 35/2018.

Lembovska, M. (2020). *More than (de)politicization: The role of security-intelligence services in (de)capturing the state.* EUROTHINK: Center for European Strategies. http://eurothink.mk/2020/09/19/the-role-of-security-intelligence-services-in-decapturing-the-state-2/

Nikolov, A. (2019). *Analysis of the legal framework for interception of communications and implementation thereof.* Foundation for Internet and Society – Metamorphosis. https://metamorphosis.org.mk/en/izdanija_arhiva/analysis-of-the-legal-framework-for-interception-of-communications-and-implementation-thereof/

Public Prosecutor's Office. (2014–2019). *Annual reports on the work of the public prosecutor's offices.* https://jorm.gov.mk/category/dokumenti/izvestai/

Bakreski, O. (2014). *Kontrola na bezbednosniot sektor*. Ss. Cyril and Methodius University in Skopje, Faculty of Philosophy.