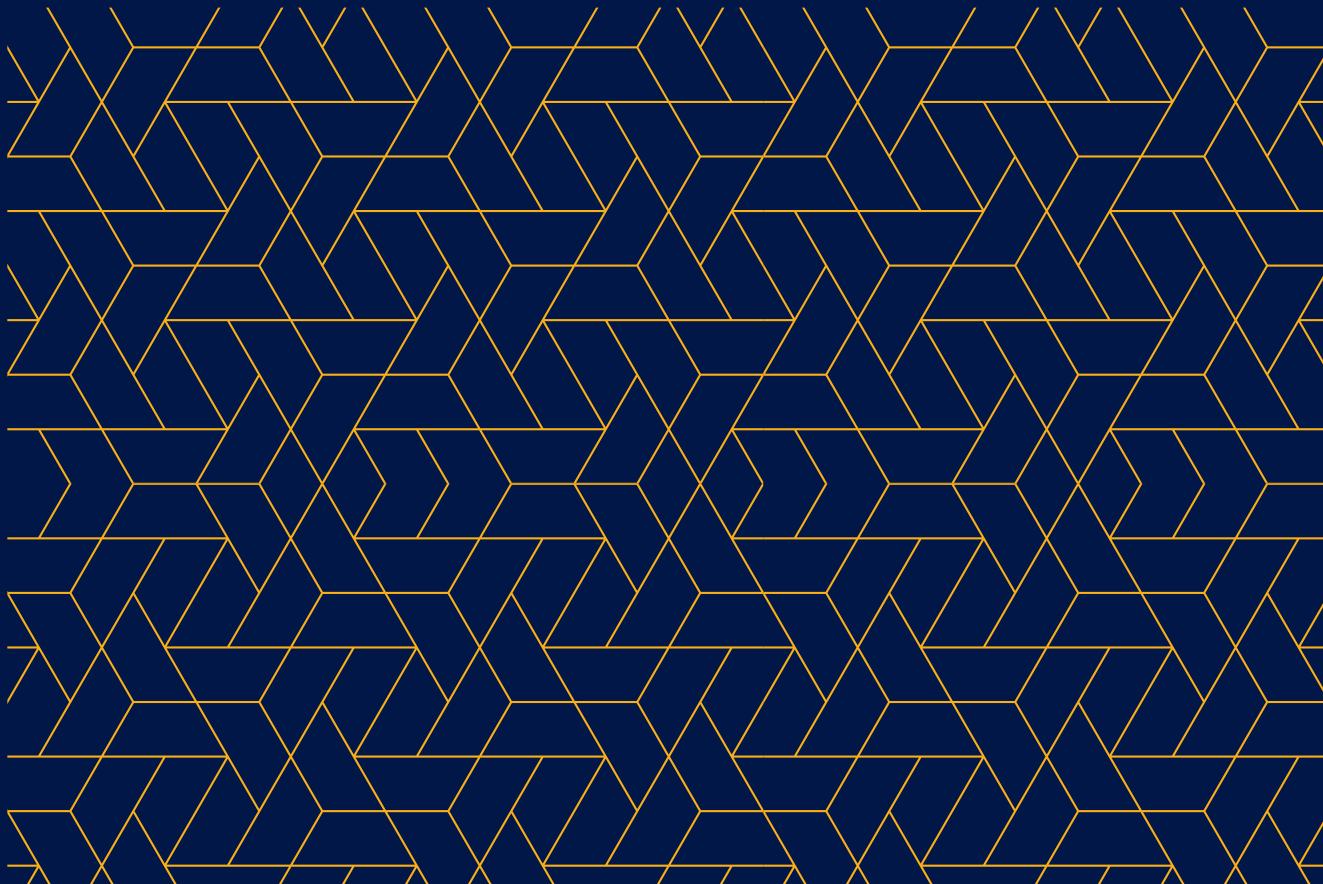
DCAF Geneva Centre for Security Sector Governance

ANALYSIS OF THE CONTENT AND PRACTICAL IMPLEMENTATION OF THE LAW ON OPERATIONAL TECHNICAL AGENCY AND THE LAW ON INTERCEPTION OF COMMUNICATIONS

Author

Prof. Dr. Biljana Karovska - Andonovska

Skopje, February 2021



About this analysis

This analysis was produced as part of DCAF implemented Intelligence Sector Reform Programme in North Macedonia.

The views expressed are those of the author and do not reflect the views of the institutions referred to or represented within this publication.

Note

About DCAF

DCAF – Geneva Centre for Security Sector Governance is an international foundation whose mission is to assist the international community in pursuing good governance and reform of the security sector. DCAF develops and promotes norms and standards, conducts tailored policy research, identifies good practices and recommendations to promote democratic security sector governance, and provides in-country advisory support and practical assis-tance programmes.

EXECUTIVE SUMMARY

The analysis of the Law on Operational Technical Agency and the Law on Interception of Communications reflects he current state from the viewpoint of legal solutions, but also from the viewpoint of real problems seen in practice, which come in part as the result of inconsistent and insufficiently precise legal provisions. Thus, a special emphasis was put on the provisions that do not fully serve the reform priorities and the segments that do not correspond to international documents and the practice of European courts.

The analysis offers alternative solutions and concrete recommendations to overcome the evident weaknesses in some of the existing legal provisions. This is especially true for several segments underlined in the text (provisions on interception of communications without the mediation of OTA; provisions on metadata; certain aspect in the interception of communications in the interest of security and defense; security of data; as well as the provisions on oversight and control over the interception of communications).

The structure of the document is comprised of an introduction, approach to the reforms, analysis of the legal framework, opportunities and challenges, and conclusions.

The introduction presents the detected shortcomings in the previous system for interception of communications and the determined reform priority contained in the Report of the Senior Experts' Group on Systemic Rule of Law Issues led by Mr. Reinhard Priebe, on the basis of which the reform actions were created.

The part dedicated to the approach to reforms provides an overview of the process of creation of legal solutions and the selection of a new model for interception of communications, largely copied from the legislation of R. Croatia. This part contains an overview of all the laws comprising the reform package for interception of communications or which are related to the wider reform of the security-intelligence sector.

A central and essential part is the analysis of the legal framework, which has conceptually been divided into two parts: analysis of the Law on OTA and analysis of the Law on Interception of Communications, with the remark that the provisions of these laws are necessarily intertwined in certain segments. That is why, examination of both laws is necessary in both parts.

The analysis of the legal framework is still more concentrated on the Law on Interception of Communications, because the Law on OTA mainly regulates issues related to OTA's competences as mediator in the process of interception of communications, the management of OTA and the rights and obligations arising from the working relationships therein. Bearing in mind the role of OTA in the entire concept, the analysis suggests technological upgrading with adequate digitalization of the overall process for establishing the technical crossover between the operator and competent bodies for interception of communications, in order to eliminate unwanted side effects and occurrences, mostly caused by the human factor për përgjimin e komunikimeve.

The part analyzing the Law on Interception of Communications is divided into three equal subsections in order to provide better visibility of the text. The provisions from this law are analyzed in the order in which they are contained in the legal text.

First, a review is given of the chapter relating to interception of communications as a special investigative measure, then the interception of communications in the interest of security and defense, and the last issue analyzed is the chapter on oversight and control of the interception of communications.

The part regarding interception of communications without the mediation of OTA and the operators, with special technical equipment and devices that enable that, is especially problematic. These provisions in essence do not correspond to the concept in which OTA has a mediation role between the operators and the competent bodies for interception of communications. Thus, a suggestion is given on redefining them with the aim of authorizing OTA to manipulate the records for usage of the equipment (as an administrator) and to perform control over the records. In this same direction, the active role of OTA should also be enabled in the control over the process of online interception of communications.

Essential shortcomings have also been noticed in the provisions for interception of communications in the interest of security and defense. Namely, regarding the provisions on metadata, it has been concluded that they do not correspond to the case law of the European Court of Justice and the opinion of the Venice Commission on the use of metadata. The inconsistent provisions on metadata from the Law on Criminal Procedure were are also pointed out, and an alternative solution for regulating this issue is offered.

The new measures for interception of communications in the interest of security and defense are also disputable. They should be redefined because they do not fit completely the definition of interception of communications in the sense of the Law on Interception of Communications, and at the same time they infringe the domain of certain police competences provided in the Law on Police. Additionally, their preventive usage should be regulated more precisely, because they prescribe the implementation of invasive measures only on the basis of indications, without even the existence of reasonable doubt.

Last on this list is the unselective introduction of all criminal acts against armed forces in the framework for interception of communications, which does not correspond to international principles that prescribe the implementation of special investigative measures only in regard to the most severe forms of crime.

In line with the determined reform priorities, a suggestion is given to mores seriously treat the issue of the safety of data collected through interception of communications, by applying specific technical and organizational measures in all stages of processing, keeping and destruction of data.

Regarding oversight, positive steps have been taken by introducing certain novelties, such as the engagement of technical experts, shortened procedure for issuing security certificates, ad-hoc oversight, etc. However, opposed to this, it has been established that the Committee has limited competences that do not provide for quality and efficient oversight over the legality of interception of communications. Thus, it is recommended that the Committee is given a wide array of actions and access to OTA's devices and court orders that have not been anonymized. This is the only way for the Committee to determine whether a certain person, telephone number or email address were illegally intercepted. In addition to this, the status of the Civilian Control Council must urgently be regulated, because currently it is undefined, which renders this body non-

functional. In this regard, it is necessary to redefine the competences of the Civilian Control Council, which are currently limited and do not enable it to directly act upon receiving a complaint by a citizen.

Regarding control, special attention must again be given to the interception of communications with special devices and equipment and without the mediation of OTA, where the competences for control by the competent public prosecutor, the Public Prosecutor of R. N. Macedonia and the judge of the preliminary procedure are probably not realized in practice, because of the necessary technical knowledge on the functioning of these devices and equipment, and it is unrealistic to expect that these persons have such technical knowledge.

The part dedicated to the opportunities and challenges is focused on the evident legal weaknesses and unrealized legal obligations in the almost two years of application of the new model for interception of communications (the lack of technical and staffing capacities in the Customs Administration and the Directorate of the Financial Police for independent interception of communications; the incomplete realization of the legal obligation for selection of technical experts in the parliamentary oversight Committee; non-functioning of the Civilian Control Council). Additionally, all of this is accompanied by the allegations for lack of implementation of the essential part of the reform – separation of the interception of communications as SIM from the interceptions in the interest of security and defense, because of the allegedly still present possibilities (optic cable) to find out the content of all intercepted communications by the new ANB, which is located on the premises of the former UBK.

The conclusions of the analysis represent a summary of the concrete recommendations for legal corrections on the one hand, and the need to look at the problem in a wider context, on the other hand. In this sense, amongst other things, a recommendation is given to clearly delineate the competences of the security services, creation of a clear concept for overcoming the political influences over security services and judiciary bodies, as well as the creation of legal solutions that correspond to the capacities of the institutions.

CONTENTS

1. INTRODUCTION

This article analyzes the laws that represent a part of the reform package used to reform the system for interception of communications in 2018, in the frames of the wider security-intelligence services reform. With this aim, the analysis is focused on the Law on Interception of Communications and the Law on the Operational Technical Agency, as key laws in this field. However, due to the close connection of the subject matter, the text also includes a necessary review of certain provisions from other laws and an appropriate comparative analysis to certain segments of the Security and Intelligence System Act of the Republic of Croatia, which were used as a model in creating the reformed system for interception of communications in R. N. Macedonia.

The purpose of the analysis is to point out the shortcomings in certain legal provisions and the weaknesses in their implementation. The ultimate goal of the analysis is to determine whether the set reform priorities have been fulfilled, through an almost two year application of the new concept for interception of communications.

The communication interception system reform in R. N. Macedonia was made necessary by the massive illegal wiretapping that the public became aware of in 2015. As a result of this, a Senior Experts' Group on Systemic Rule of Law Issues, established by the European Commission and led by Reinhard Priebe, prepared a Report (the "Priebe Report") establishing the factual situation and recommending appropriate solutions in the areas were shortcomings were detected. The document, entitled Urgent Reform Priorities,[1] established systemic flaws, concentration of power and abuse of the surveillance mechanism by the then Administration for Safety and Counter-intelligence (UBK), as well as an exclusive power by the UBK to intercept communications. The second Priebe Report from 2017 includes an assessment of the reforms thus far and recommendations for further steps in the reform process.[2]

Regarding parliamentary oversight over competent authorities for interception of communications, the experts have concluded that it has been established in theory, through parliamentary committees, which still do not conduct oversight over the UBK, nor do they gather statistical data on interception of communications. Lack of technical knowledge and a long procedure for issuing security certificates for committee members, as well as the continuous boycott of the committees caused by the boycott of the work of the Parliament by the then opposition, have been pointed out, amongst other things, as reasons for the inefficient oversight.

[1] Available at: http://ec.europa.eu/enlargement/news_corner/news/news-files/20150619_urgent_reform_priorities.pdf

[2] Available at: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/2017.09.14_seg_report_on_systemic_rol_issues_for_publication.pdf

2. APPROACH TO THE REFORMS

Based on their analysis, the Expert Group led by R. Priebe, recommended in their first report, amongst other things, the removal of UBKS's intermediary function and its capacity to directly access the technical equipment enabling communication signal mirroring, and relocation of the mediation devices to the premises of telecommunication operators that will activate and divert signals to the competent agencies for interception of communications only upon prior receipt of a relevant court order. It was also recommended to reinforce data security and their storage under a special regime, selection and employment in the services on the basis of strict criteria, merit and integrity, their regular training, provision of well trained staff to control intelligence services' operations and including technical experts as support to parliamentary committees for security services oversight and oversight over the application of measures for interception of communications.

A legal framework for interception of communications was created on the basis of the determined weaknesses and provided recommendations and it was expected to provide the legislative basis for a balanced system, which would make illegal wiretappings impossible. The process for creation of the basic setup of the system for interception of communications was conducted without a wider debate based on reliable scientific and expert opinions. Contrary to the recommendations and expectations for better transparency, the model for interception of communications was selected without prior public debate. The model includes a separate entity - the Operational-Technical Agency (OTA), as the intermediary between competent authorities for interception of communications and operators, which should only relay the signal, without the possibility of knowing the content of intercepted communications.

The new model for interception of communications does not correspond to the recommendations made by the Expert Group led by R. Priebe, especially regarding the recommendations to relocate the mediation devices to the premises of the telecommunications operators.

Several public debates and meetings came after the non-transparent choice of the communications interception model, including with representatives from the non-governmental sector, and some of the comments were accepted, but the proposers of these laws were not ready to accept others, although they were aimed at improving the proposed legal solutions.

The reform package in the field of interception of communications actually contains two new laws, the Law on Interception of Communications[3] and the Law on Operational-Technical Agency.[4] In order to harmonize certain provisions from these laws, amendments and supplements were also adopted during this period to the Law on Electronic Communications[5] and the Law on Criminal Procedure[6], as well as amendments to the Law on Classified Information[7]. The Law on National Security Agency[8] and the Law for Coordination of the Security

[3] Law on Interception of Communications, Official Gazette, no. 71/18, 108/19

[4] Law on Operational-Technical Agency, Official Gazette, no. 71/18

[5] Law on Amendment and Supplement of the Law on Electronic Communications, Official Gazette, no. 11/18, 98/19

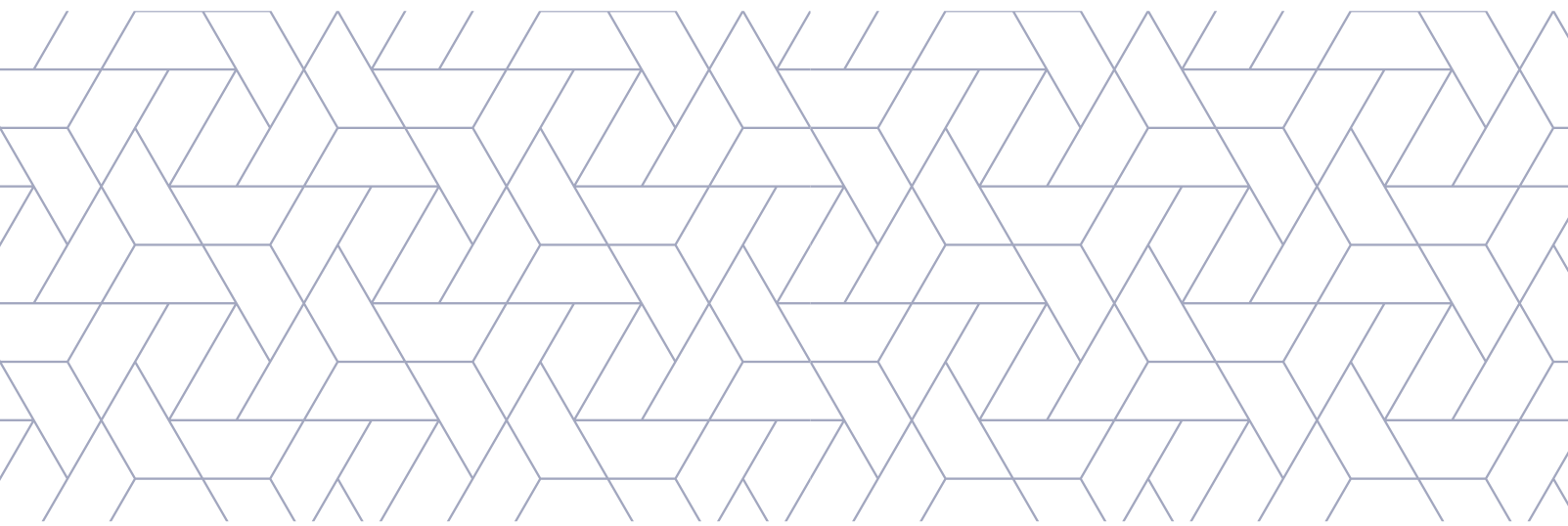
[6] Law on Amendment and Supplement of the Law on Criminal Procedure, Official Gazette, no. 198/18

[7] Law on Supplement of the Law on Classified Information, Official Gazette, no. 21/18

[8] Law on National Security Agency, Official Gazette, no. 108/19

Intelligence Community[9] were adopted some time later. The reform legislative framework should be completed with a new Law on the Intelligence Agency.[10]

The impression exists that partial legal solutions were created, without a clear vision of the entire security-intelligence system. This is confirmed by the fact that the first set of laws adopted in 2018 were subjected to amendments and supplements after a short time, in order to harmonize them with the new laws adopted in the meantime, i.e. in 2019.



[9] Law for Coordination of the Security Intelligence Community, Official Gazette, no. 108/19

[10] Law on Intelligence Agency, Official Gazette, no. 21/21

3. ANALYSIS OF THE LEGAL FRAMEWORK FOR INTERCEPTION OF COMMUNICATIONS

The following analysis of the legal framework includes the provisions from the Law on Operational Technical Agency (LOTA) and the Law on Interception of Communications (LIC). In this, due to the close connection between those two laws and several other legal acts, as was pointed out in the introduction, the part relating to LOTA includes an overview of certain LIC provisions directly related to OTA, whereas the part relating to LIC also inevitably considers the related provisions from other legal acts.

3.1. Law on Operational Technical Agency

The logic behind one of the recommendations contained in the "Priebe Report" was that mediation devices should be relocated to the premises of telecommunications operators that will activate and divert signals to competent authorities for interception of communications only after receiving a court order. In opposition to this, according to the selected model and with a special law, adopted simultaneously with the new LIC from 2018, an independent state body was established providing technical connectivity between operators and authorized bodies (Article 2 of LOTA). The model has been taken from Croatian legislation and to a great extent mirrors the provisions of the Act on the Security Intelligence System of the Republic of Croatia.[11] The Ministry of Interior (MoI), as proposer, justified the advantages of this model, amongst other things, with avoiding the concentration of power in a single body and the possibility for double control. Although the model is in essence identical to the Croatian one, we can still detect certain differences, which have been emphasized in this analysis below.

At the very onset of the reform process, the model providing OTA with the roll of intermediary and coordinator in the interception of communications imposed certain questions, amongst others the fact that OTA is taking over the same equipment used by the UBK for this purpose. Although Article 2 paragraph 2 of the Law on OTA contains a provision stating that OTA does not have technical capabilities to access the content of intercepted communications, Article 35 paragraph 1 of LIC provides that in order to avoid obstacles in the founding and establishment of OTA, the Government shall ensure that the technical devices for interception of communications LEIMD[12] and LEMF[13], as well as the technical documents, are transferred from UBK to OTA.

Pursuant to Article 35 paragraphs 3 and 4 of the Law on OTA, a maximum of seven persons who have experience in working with technical devices for interception of communications may be transferred from UBK to OTA. The integrity of the persons transferred from the former UBK to OTA was exceptionally important in returning the lost trust with the wider public regarding the operations of the security services. Although the OTA staffing process was not sufficiently transparent and the public was not appropriately informed of the criteria for

[11] Act on the Security Intelligence System of the Republic of Croatia, available at:https://www.uvns.hr/UserDocsImages/dokumenti/nacionalna-sigurnost/ZAKON-O-SIGURNOSNO-OBAVJESTAJNOM-SUSTAVU-RH-NN-79-2006.pdf

[12] Mediation technical equipment and appropriate software support that enables the activation of the measure for interception of communications.

[13] Equipment for interception of communications comprised of the means use to transfer the content of the intercepted communication and the information related with the intercepted communication.

transferring UBK employees to OTA, OTA was still effectively and efficiently established as a separate service. The reservations expressed that a newly established and insufficiently staffed service is being given relatively easy access to sensitive data came as a consequence of the previously lost trust in the services involved in the process of intercepting communications, and the fact that the state was faced with major illicit wiretapping scandals on several occasions.

The Law on OTA mainly regulates issues related to OTA's competences as mediator in the process of interception of communications, the management of OTA and the rights and obligations arising from the working relationships therein.

Looking back from today, and less than two years from the beginning of the application of LIC and LOTA, which is still a relatively short time, it can only be presumed that the selected model for interception of communications with the mediation of OTA is probably burdening the procedure with a series of actions that must be taken before the start of implementation of the court order for interception of communications (introduction of an identification number as an anonymization tool, anonymizing the court order for forwarding to OTA, delivery of the anonymized order to OTA, activation of the system in OTA, etc.). On the other hand, the positive effect of the new model is the existence of an additional layer of oversight, i.e. the possibility for a better quality oversight over the interception of communications in the sense that there are more points for collection of data that can be further compared. The overall process for establishing the technical crossover between the operator and competent bodies should be technologically upgraded, which would eliminate unwanted side effects and occurrences, mostly caused by the human factor.

PROCESS OF INTERCEPTION OF COMMUNICATIONS

OTA activates and creates technical conditions for interception of communications in criminal investigations and for protecting the security and defense interests of the state (Article 3 paragraph 1 of LOTA). The process for interception of communications, regulated in the provisions of LIC, is performed in the manner that after a court order has for interception of communications has been issued, an anonymized copy of that order is submitted to OTA. Pursuant to Article 64 of LIC, the authorized person in OTA is obliged to immediately activate and make available the communication for which the order was issued, as well as to stop the interception of communications in case of expiry of the time provided in the order, or when an order was issued to terminate the measure. During this process, OTA also performs expert supervision over the operations of the operators.

CONDITIONS FOR APPOINTMENT OF THE DIRECTOR OF OTA

The Director of OTA is appointed and dismissed by the Parliament with a two thirds majority vote for a mandate period of five years, without the possibility for reelection. These are correct legal solutions, in particular the two thirds majority, which practically confirms the legitimacy of the appointed director and the achieved consensus between the political parties in the Parliament regarding the person in question. It is also good that one of the bases for dismissal of the OTA Director is established interference in the control and oversight by competent bodies by the OTA director, pursuant to Article 9 paragraph 2 line 2 of LOTA. This sends a message on the importance that the legislators give to oversight and control, as very important segments in the system for interception of communications.

However, it is unclear why Article 5 from the Law on OTA only provides for citizenship, degree of education and relevant working experience as conditions for appointment of a director. The lack of conflict of interest and lack of security risk for appointment of a specific person as director are not prescribed as conditions (and they are prescribed for the director of ANB (National Security Agency), and the authorized officials of both OTA and ANB).

RECOMMENDATION

The conditions provided in Article 10 of the Law on National Security Agency can be copied regarding the appointment of the OTA Director as well.

REPORT ON THE WORK OF OTA

Pursuant to Article 7 of the Law on OTA, the Director submits for review to the Parliament of R. N. Macedonia an annual report on the work of OTA in the previous calendar year that, amongst other things, should contain a number of activated communications for each body individually. This number does not contain the number of activated communications for security and defense, which as a legal solution can only be justified from the point that it is sufficient for the wider public to be informed only about the total number of activated measures. However, the oversight parliamentary committees in this sector should have information indicating the situation regarding national security, and also to which extent are the competent institutions handling them. Parliamentary committees and the Parliament should assess, control and approve the budgets of security services, on the basis of relevant indicators. For these reasons, the needs for oversight of the number of activated communications in the interest of security and defense, this information must be submitted to the parliamentary committees.

RECOMMENDATION

In this regard, the provisions on the content of the annual report on OTA's work need to be amended and these are some of the possible alternatives:

- Delete in Article 7 paragraph 2 line 2 the second sentence according to which in the number of activated communications for each competent body individually "there shall be no number of activated communications stated for security and defense";
- Article 7 paragraph 2 should be supplemented with a new line according to which, in a separate report for the purposes of oversight or in a different written form, the total number of activated communications will also include the number of activated communications in the interest of security and defense.

According to the 2018 annual report,[14] OTA mediated in the activation of measures in a total of 153 communications, 5 communications of which were for the needs of the Department for Fight against Organized and Serious Crime in the Public Security Bureau (PSB) in the MoI, and 8 communications for the needs of the Special Public Prosecution Office. There is no information on the remaining 142 communications, but it is unrealistic to presume that they were in the communications whose numbers do not need to be provided in this report.

Because of the current situation and the implications from the declared state

[14] https://ota.mk/adocs/scan-izvestaj-ota-2018.pdf

of emergency, the report on OTA's work for 2019 was reviewed at a session of the Government on 22.04.2020,[15] but it has still not been published on the OTA web page. According to the minutes of the session of Government, amongst other things, the Report contains information that in 2019 OTA diverted 269 communications for the needs of the Public Security Bureau of the MoI. However, after the technical counting in the tracking system and after performed insight of submitted court orders, counting of active targets, telephone numbers and e-mail addresses, it was concluded that the *numbers on the OTA Report do not coincide with the numbers in the MoI records.* OTA answered that the difference in the part of technically diverted communications comes as a result of *differences between the methodology of OTA and the methodology of the MoI*.

RECOMMENDATION

OTA and MoI, as well as other entities included in the process of diverting and interception of communications, as well as oversight and control, should establish a single methodology for counting and insight into all relevant data related to this process.

EXPERT SUPERVISION OVER OPERATORS

OTA is authorized to perform expert supervision over operators, comprising supervision over the utilization of technical equipment and electronic communication lines connecting OTA to the operator (Article 32 of LOTA). For this purpose, in November 2018 the Director of OTA established a Committee for expert supervision that, according to the 2018 report, had several meetings with the operators where they presented the proposal Guidelines on the manner of acting of service operators. Supervision of the operators was not performed in 2018, because of the short time that had passed since the establishment of OTA. As stated previously, a Report on the work of OTA for 2019 is still not fully publicly available.

3.2. Law on Interception of Communications

The Law on Interception of Communications as *lex specialis* regarding the application of the measures for interception of communications regulates the procedure for interception of communications in criminal investigations; the conditions and procedure for interception of communications in the interest of security and defense; the issues regarding oversight and control in this filed; as well as the obligations of OTA and the operators in the process of interception of communications.

This is the order in which the analysis of the LIC provisions was made, with a special emphasis primarily on provisions that legally and technically contain insufficiently clear and precise formulations, and the provisions that need to be seriously reassessed and reformulated.

3.2.1. Interception of Communications for the Purposes of Criminal Investigations

Competent bodies for interception of communications in criminal investigations are the public prosecutor and the justice police (police officers from the MoI and representatives of the Financial Police, authorized persons in the Customs Administration and authorized officials in the Ministry of Defense who working on detection and reporting of criminal acts). The order for interception of

communications is adopted by the competent judge in the preliminary procedure, on the basis of a request by the competent public prosecutor.

The LIC chapter on interception of communications is entitled "Procedure for Implementation of a Special Investigative Measure". Formulated in such a way, the title may indicate all (12 in total) special investigative measures (SIM measures) provided in the Law on Criminal Procedure (LCP), instead of the SIM measure from Article 252 paragraph 1 point 1 of the LCP that this chapter actually refers to. It is not enough that in Article 4 paragraph 1 point 4 of LIC explains the term "special investigative measure" as "monitoring and recording of telephone and other electronic communications", because special investigative measures in the sense of LCP are all measures in Article 252 paragraph 1. Thus, the chapter title should be reformulated as: "Procedure for Implementation of Special Investigative Measure Interception and Recording of Telephone and other Electronic Communications".

PROCEDURE IN CASES OF URGENCY

Article 10 of LIC replaces the oral order for interception of communications that existed thus far with a temporary written order issued in cases of urgency, both for criminal investigations and in the interest of security and defense. The conditions for issuing a temporary written order are reduced to the following formulation "when there is reasonable doubt that the delay can adversely affect the implementation of the procedure" (Article 10), or "when there is danger of postponement" (Article 30).

RECOMMENDATION

- Due to the possible implications from the issuing of temporary written orders, it is necessary to more precisely define the conditions under which such an order may be issued, and the conditions contained in the basic text of LIC from 2006 (in 2012 they were amended to a formulation similar to the one given above) could be returned, which provided that the then oral order was issued in case of danger of death or serious bodily harm, the escape of a perpetrator of a criminal act with a prescribed prison sentence for life or large scale material damages.

STORAGE AND DESTRUCTION OF DATA COLLECTED THROUGH INTERCEPTION OF COMMUNICATIONS

Pursuant to Article 16 of LIC, after the adoption of the decision by the public prosecutor the data from interception of communications will be submitted to the court and will be kept within deadlines depending on whether a judgment of release, abandonment or conviction was adopted, and after the expiry of the deadlines the data will be destroyed upon which a report will be prepared.

The legislator should pay more attention to the safety of the data collected through interception of communications in these provisions, in the direction of the recommendations from the "Priebe Report" for strengthening data security in order to avoid any risk from their uncontrolled or illicit usage.

RECOMMENDATION

- Concrete technical and organizational measures for safety during processing and during storage of data from intercepted communications should be determined, in accordance with the Law on Personal Data Protection (LPDP)16 and Directive 2016/680 for protection of personal data in criminal investigations.[17]
- The deletion of special categories of personal data should be predicted, along with the statements given in relation to this category of data collected during interception of communications.
- Liability should be predicted in case of failure to comply with the legal deadlines for destruction of data collected during interception of communications.

INTERCEPTION OF COMMUNICATIONS WITH SPECIAL TECHNICAL DEVICES AND EQUIPMENT

Pursuant to Article 17 of LIC, communications may be intercepted with special technical devices and equipment that enable the interception of communications without involvement of OTA and the operators. These technical devices and equipment are kept in the Basic Public Prosecution Office for Organized Crime and Corruption and, on the basis of an issued court order, an authorized person from the justice police takes the technical devices and equipment, conducts the interception of communications and then returns the devices and equipment. LIC does not regulate in which cases and under which conditions communications will be intercepted without the involvement of OTA and the operators. There is also the issue of whether and in which manner will oversight be performed over these interceptions, because the control over this type of interception of communications is specially regulated in Article 60 of LIC. Interception of communications special devices and equipment and without involvement of OTA and the operators has also been predicted in the interest of security and defense "in a procedure and under conditions stipulated by law" (Article 34 of LIC).

Article 26 of the Law on the National Security Agency (ANB) regulates this issue almost identically as in Article 17 of LIC, but it contains two important limitations that are not included in Article 17 of LIC. Namely, the limitations stipulate that interceptions will be performed without the mediation of OTA *only when it is technically impossible to intercept and record the communication without using the special devices and equipment*; and that *authorized ANB officials may not have technical or any other possibility to change or delete the data from the special technical devices and equipment*.

Article 17, paragraph 7 of LIC provides a possibility, but not an obligation, for the competent public prosecutor to at any time, request **from the authorized person from the justice police to listen or re-listen to a conversation that is subject of interest and perform an examination of the records on the use of the devices and equipment. From the viewpoint of control over the process, this is a correct legal solution, but at the same time it is highly probable that the prosecutor has no**

[16] Law on Personal Data Protection, Official Gazette, no. 42/20

[17] Directive (EU) 2016/680 of The European Parliament and of The Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data

technical knowledge of the special devices and equipment the usage of which is regulated in this part of LIC. Thus, in practice, the public prosecutor probably cannot conduct an appropriate expert examination of the records on the use of the special devices and equipment, especially if the justice police are able to manipulate the records on the use of the equipment. This is why, excluding OTA from the process of intercepting communications in cases when it cannot be expected from the public prosecutors to have knowledge of the functioning of complex and sophisticated technologies, leaves serious possibilities for possible cover-ups by the justice police and disabling of ex-post control. The situation is similar with online interception of communications, where OTA is excluded from the control system without justification. Bearing in mind that almost all electronic communications strive towards online platforms, this can be a serious problem and bring the existence of OTA into question after a certain time.

The provisions from Article 60 of LIC determine that the control over the manner of using the special technical devices and equipment is performed by the Public Prosecutor of R. N. Macedonia and the preliminary procedure judge who issued the interception order. Although this legal solution seems to strengthen the system of control, its purposefulness is disputable. It is disputable how much time the Public Prosecutor of R. N. Macedonia has to dedicate to this type of control in each individual case. It is also very possible in this case as well that the Public Prosecutor of R. N. Macedonia does not have the technical knowledge on the special devices and equipment, which is why LIC provides for the possibility of engaging technical experts.

RECOMMENDATION

- Because the interception of communications with special technical devices and equipment deviates from the OTA system that serves as an intermediary between the competent bodies and operators, it is necessary to more precisely define all aspects relevant to the process of interception without the mediation of OTA and the operators, as well as to determine mechanisms for oversight when interception is performed in this manner.
- One of the possible solutions is to authorize OTA to manipulate the records for use of the equipment (as administrator) and to perform controls over the records, independently and on request of the public prosecutor. This will achieve multi-layer control and the justice police will only be able to use the device, but not manipulate the records, which will indubitably reduce the suspicion of risk from possible misuses. In this direction, OTA should also have an active role in the control over the process for online interception of communications.
- The provisions related to the interception of communications in the interest of security and defense without mediation by OTA and the operators should still be contained in one law, instead of having one part in LIC and another part in the Law on ANB. Primarily, the possibility of incorporating these provisions in the Law on Interception of Communications, as lex specialis on this issue, should be investigated.

3.2.2. Interception of Communications in the Interest of Security and Defense

Authorized bodies for interception of communications in the interest of security and defense are ANB and the Ministry of Defense - Military Service for Security and Intelligence, as well as the Center for Electronic Reconnaissance of ARM used for the needs of defense (in the frequency range of high, very high and ultra-high frequencies). The order for interception of communications is adopted by a Supreme Court judge determined under the internal allocation of the court, on the basis of a request by the Director of ANB, i.e. on proposal by the Minister of Defense or a person authorized by the Minister.

MEASURES FOR INTERCEPTION OF COMMUNICATIONS IN THE INTEREST OF SECURITY AND DEFENSE

The chapter on interception of communications in the interest of security and defense, the legislator has prescribed four new measures for interception of communications, as follows:

- interception and recording of telephone and other electronic communications;
- monitoring and recording of the interior of facilities, closed premises and objects and the entrance to those facilities, closed premises and objects, for the purpose of creating conditions for the implementation of the measure;
- following and recording persons in an open and public space with lighting;
- interception and audio recording of the contents of the communications of persons in an open and public space.

Part of the newly established measures inherently do not completely fit the definition of interception of communications in the sense of LIC and go into the domain of the police competences regulated in Article 28 paragraph 1 of the Law on Police.[18] Such regulation leaves the possibility of overlaps in practice between entrusted police competences and ordered measures for interception of communications.

RECOMMENDATION

The measures provided in Article 18 of LIC should be redefined, in order to distance them from the actions that come under police competences regulated in the Law on Police.

[18] Law on Police, Official Gazette, no. 114/06, 114/06, 6/09,145/12, 41/14, 33/15, 31/16, 106/16, 120/16, 21/18, 64/18

CONDITIONS FOR INTERCEPTION OF COMMUNICATIONS IN THE INTEREST OF SECURITY AND DEFENSE

Article 19 paragraph 1 of LIC provides that the measures for interception of communications referred in the interest of security and defense will be applied when there are grounds for suspicion that the preparation of a crime is underway against the state, against the armed forces or against humanity and the international law. The non-selective introduction of all criminal acts in this framework does not correspond to the international principles that dictate the use of special investigative techniques only in relation to the most severe forms of crime.[19] Namely, the Criminal Code predicts a prison sentence of up to five years for only a small part of the criminal acts against the armed forces, and for most of them the penalty is one to three years with the possibility of disciplinary sanctions if the offense was light and if it is in the interest of the service.

RECOMMENDATION

- The criminal acts that are not included in the definition of severe criminal acts provided in the United Nations Convention against Transnational Organized Crime,20 and in the Council of Europe Recommendation of the Committee of Ministers concerning guiding principles of the fight against organized crime.[21]

PREVENTIVE ACTIONS

Paragraph 2 of Article 19 of LIC predicts for applying measures for interception of communications for the purpose of preventive action, in the event of preparing, inciting, organizing or participating in an armed attack against the state or disabling its defense system; as well as activities related to the criminal acts terrorist organization, terrorism and financing of terrorism, if the information cannot be provided in another way or this would be related to greater difficulties.

RECOMMENDATION

- The preventive application, or application before the crime, of measures for interception of communications deserves a more serious approach and this issue must be regulated much more precisely because it means the application of most invasive measures only on the basis of doubt, which leave room for suspicion regarding the possibility for violating the personal rights of individuals.

[19] Council of Europe Recommendation (2005) 10 of the Committee of Ministers to member states on "special investigative techniques" in relation to serious crimes including acts of terrorism

[20] The United Nations Convention Against Transnational Organized Crime (2000)

[21] Council of Europe Recommendation (2001) 11 of the Committee of Ministers to member states concerning guiding principles of the fight against organized crime

METADATA

In the special chapter entitled "Metadata" the legislator has provided an obligation of the operators to submit metadata on request by authorized bodies, for the needs of security and defense. The Public Prosecutor of R. N. Macedonia should be informed about this request, and if they do not confirm the justification for the data, the authorized body is obliged to immediately stop using the data and destroy them.

This is data that the operators keep according to the Law on Electronic Communications (LEC).[22] However, these formulations, in these provisions of LIC and in the provisions of LEC, enable all bodies for interception of communications to inspect metadata unselectively for all citizens, without a court order or decision of a public prosecutor.

In the meantime, Directive 2006/24/EC that was transposed to our legislation in this way, was annulled by the European Court of Justice,[23] with the rationale that governments may not force telecommunication companies to keep all data on their clients and that unselective and massive retention of metadata is in opposition to the EU Charter of Fundamental Rights.

Another disputable issue regarding metadata is that: "Insight into realized telephone and other electronic communications" that indubitably represent metadata, is a SIM measure that pursuant to Article 252 paragraph 1 point 6 of LCP is applied on an order from a prosecutor. Opposed to this SIM measure, Article 287 paragraph 8 of LCP unnecessarily prescribes an obligation for the operator to submit the metadata they retain upon request from a public prosecutor. The prescription of this obligation, in a situation where it already exists as a SIM measure in the same law, creates the possibility for circumspection of the protective mechanisms predicted for SIM measures and at the same time, just like the case with the aforementioned SIM measure, it creates a possibility to achieve insight into metadata without a court order.

RECOMMENDATION

The provisions regulating metadata in several laws (LIC, LEC, LCP) should be completely redefined, bearing in mind the case law of the European Court of Justice and the opinion of the Venice Commission on metadata, contained in the Rule of Law Checklist.[24] One of the alternative solutions to regulating this issue can be the following:

- To include insight into metadata in the definition for interception of communications and to practice it on the basis of a previously issued court order, under conditions and procedures that are valid for all other measures for interception of communications

[22] In the sense of Articles 176, 177 and 178 of LEC, this is data that operators are obliged to keep for 12 months from the date the communication was performed, in the form of an electronic record for every access of the citizens to every form of electronic communication, and they contain data on the name, telephone number or IP address, the location of the persons communicating, the time of communication, etc.

[23] Judgment of the Court (Grand Chamber) of 8 April 2014 Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and The Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12)

[24] European Commission for Democracy through Law (Venice Commission) Rule of Law Checklist, March 2016, available at: https://www.venice.coe.int/images/SITE%20IMAGES/Publications/Rule_of_Law_Check_List.pdf

(in criminal investigations and for security and defense). The redefinition would surely dictate changes in Article 252 paragraph 1 of LCP, so that the SIM measure from point 6 is issued with a court order, and changes in Articles 32 and 33 of LEC. In this sense, Article 287 paragraph 8 of LCP will need to be abolished.

STORING AND DESTROYING DATA

The period for keeping the data collected from interception of communications in the interest of security and defense was reduced from the previous five years, which was assessed as too long by the Expert Group led by Priebe, to three years (Article 29 paragraph 1 of LIC). However, pursuant to Article 29 paragraph 2 of LIC this period can be reinitiated in the event of obtaining new information that is directly related to the specific data for which the storage period has not expired yet. Additionally, Article 29 paragraph 5 states that "all data in the court register on the person to whom the order referred shall be kept for 10 years and they shall be destroyed after the expiry of this deadline".

RECOMMENDATION

- An additional reasonable period can be determined in Article 29 paragraph 1 and after the expiration of this period the data can be appropriately destroyed, in order to disable keeping them indefinitely and leaving room for possible misuse.
- The period of 10 years contained in the previously quoted Article 29 paragraph 5 of LIC and Article 67 paragraph 2 of LIC should be revised.
- Article 29 should be supplemented with provisions listing the security measures provided in the aforementioned LPDP and Directive 2016/680, which fully corresponds to the recommendation from the "Priebe Report" on strengthening data security and their keeping under a special regime.
- An obligation should also be determined to destroy the original recording and all copies in all institutions and subjects involved in diverting and interception of communications.

3.2.3. Oversight and Control over Interception of Communications

OVERSIGHT OVER THE MEASURES FOR INTERCEPTION OF COMMUNICATIONS

Oversight over interception of communications is a complex process in which the oversight bodies are expected to act as true correctors of the security services. In opposition to this, interception of communications can bring into question the respect for fundamental human rights and create an environment of uncertainty. Oversight should be conducted in continuity through an established practice and by supervisory bodies free from partisan and political influences. In this, supervision should not be reduced to submitting annual reports to the Parliament, although the previous Law on Interception of Communications had not predicted any additional mechanisms for the function of efficient supervision.

The LIC from 2018 overcomes certain disputable elements that, although seemingly of a technical nature, have thus far made more difficult, and at certain times completely paralyzed oversight over interception of communications. This primarily relates to the engagement of national and international technical experts with appropriate expert knowledge, who would participate in oversight as part of the parliamentary Committee for oversight over communication interception measures. The same applies for the issuing of security certificates in a procedure no longer than 30 days (Article 37 paragraph 2 of LIC),[25] for the purposes of which the Law on Classified Information was amended in 2018. It is important that the parliamentary Committee conducts oversight without any prior announcement, if necessary, and at least once in three months, even in the event of a lack of a majority of votes (Article 44 paragraph 1 of LIC). During oversight, the Committee can request expert assistance by any state institution and body that is not the subject of oversight, including the Agency for Electronic Communications, the Directorate for Security of Classified Information and the Directorate for Personal Data Protection, on issues in their field of competence.

Opposed to these elements, the introduction of which in the law seemed necessary, there is still the impression that the competent parliamentary Committee has limited competences, which can bring into question the quality and comprehensiveness of supervision. Namely, the Committee, but also the accredited technical experts, during oversight can compare the logs for the time and date of start and end of the interception of communications, which is data that can be received from the operators, OTA and the competent bodies. OTA and the competent bodies can also make available the anonymized court order (regular and temporary court order), and from OTA also the logs on the total number of implemented measures for interception of communications in a given time period. By accessing this data, the Committee and technical experts still do not have insight into the data on the identity of the person, telephone number, e-mail address, etc. For these reasons, during oversight the Committee and technical experts cannot compare the data from the issued court order with the actually activated interception of communications regarding the specific person, telephone number or e-mail address. Lacking this possibility for comparison, the Committee as an oversight body cannot determine whether a certain person or communication means was illegally intercepted.

Compared with the legislation in R. Croatia, which was used as the model for our legislation, the National Security Council, as one of the bodies used by the Croatian Parliament to perform oversight over security-intelligence agencies, including over the covert collection of data, has significantly wider competences. In addition to the insight into the activities and measures undertaken by the security agencies, the Council can request the Supreme Court of Croatia and security-intelligence agencies a report on the implemented measures for covert collection of data and measures undertaken against persons, can interview directors and employees of security agencies regarding the legality of specific measures that were implemented, and discuss the legality of the financial and material work of the security-intelligence agencies. This body also performs direct oversight security-intelligence agencies in accordance with the same provisions of the Security and Intelligence System Act of the Republic of Croatia that are provided for the expert oversight performed by the Office of the National Security Council. From the viewpoint of Croatian legislation, direct oversight means oversight

[25] Although Article 37 paragraph 2 of LIC is not appropriately formulated. The 30 day period only concerns the duration of the procedure, whereas the security certificate may not be issued at all, if the security assessment dictates that.

of the legality of work over security-intelligence agencies, of the realization of the prescribed goals and scope of work, of the implementation of measures for covert collection of data, of financial means, as well as the coordination and cooperation between security-intelligence agencies and appropriate services in other countries. In addition to this, pursuant to Article 108 of the Security and Intelligence System Act of the Republic of Croatia, in the frames of expert oversight provides a competence for oversight bodies to request from security agencies data on the identity of the agency's sources when it is necessary for the oversight goals in a specific case, and in case of disagreement of the agencies with such a request a decision is made by the National Security Council.

Although this system for interception of communications was the model used to establish the bases of the system in R. N. Macedonia, LIC is still restrictive when prescribing the competences of the parliamentary oversight Committee and many legal solutions from the Croatian system are not contained in our legislation. It is disturbing that these are mechanisms that can contribute to efficient oversight and increasing the trust of citizens in the work of both the parliamentary Committee and security services.

RECOMMENDATION

- The possibility for supplementing Article 42 of LIC should be considered, by providing an authorization for the Committee and technical experts, or only of the technical experts, to have access to OTA devices during oversight, with the possibility to access court orders that have not been anonymized.
- In the strict listing of data in Articles 41, 42 and 43 of LIC, the possibility for insight into other documents and data needed during oversight, which cannot be predicted at the time of creation of the legal provisions, needs to be established.
- Article 40 of LIC should be supplemented with provisions enabling the Committee for oversight over the measures for interception of communications a wider array of competences and actions that it can take, especially regarding invitations to interviews of the management staff and other employees from the competent bodies and in OTA, in cases when additional information is needed regarding the legality of application of specific measures (which is actually predicted for the competent working body of the Parliament for oversight of ANB, pursuant to Article 60 paragraph 5 of the Law on ANB), and the possibility to invite the management staff and other employees from the competent bodies and in OTA to meetings of the Committee where they can answer questions posed by the Committee members, including technical experts.
- Article 40 of LIC should also include oversight over the efficient implementation of measures for interception of communications in the sense of purposeful utilization of financial and human resources, and the effectiveness of oversight should be also be a goal regarding the measures for interception of communications in the interest of security and defense.

In addition to the aforementioned, it is necessary to create appropriate by-laws regulating the methodology for realization of field visits and providing for the consequences if the committees fail to submit or are late in submitting reports to the Parliament, the deadlines in which competent bodies must submit the requested information, as well as the consequences of the late submission thereof. Additionally, mechanisms need to be created to raise awareness of committee members on the importance of parliamentary oversight over interception of communications and appropriate mechanisms to free the members from partisan and political influence during oversight.

COUNCIL FOR CIVILIAN CONTROL

The Council for Civilian Control is promoted in Article 35 of LIC as a new body performing oversight of the legality of the measures for interception of communications and OTA, on own initiative or on a complaint submitted by a citizen. LIC does not specifically provide for the status and conditions for work of this body, except that the work premises of the Council are provide by the Parliament, and the financial means are provided by the state's budget. Because of the unregulated status, the Council for Civilian Control cannot dispose of its approved budget funds. This is certainly one of the reasons why, more than one year after its establishment, the Civilian Control Council has not started properly functioning, and basic work conditions have not been created in the sense of the necessary technical means, archive, security safe, registration of an e-mail address, fees for the members and security certificates for some of the members. Amendments to LIC were proposed in the Parliament regarding certain norms related to the Council, but they still have not been adopted. In the meantime, because of all these reasons, one member of the Council tendered their resignation in October 2019, which was followed by resignations of the president and vice-president of the Civilian Control Council in June 2020.

Regarding the competences of the Civilian Control Council, LIC provides certain limitations that need to be reexamined, because the manner in which its competences are regulated now does not guarantee efficient civilian oversight and turn the Council into an inefficient body. Namely, after receiving a complaint by a citizen, the Civilian Control Council does not have the possibility of acting independently to determine if the complaint is grounded, i.e. whether the communications of a certain person or telephone number were illegally intercepted. Regarding the complaint, the Council must submit a request to the Committee for oversight over interception of communications for it to conduct oversight and inform the Council regarding that in 15 days' time. Set up like this, the relation between the Civilian Control Council – oversight Committee is disputable, and not only places the Council in a marginalized position, but also brings into question the justification for its existence.

On the other hand, the position of the Civilian Control Council is additionally marginalized by the fact that even the oversight that the Council can perform pursuant to Article 51 paragraph 2 line 2 of LIC, should be announced in advance and only related to comparing anonymized orders in the last 3 months. Such limitations of oversight are not provided in LIC regarding the Committee or other oversight bodies.

Comparatively, the competences of the oversight body titled the Council for the Civilian Oversight of Security and Intelligence Agencies in R. Croatia are not limited only on the oversight of the legality of measures for interception

of communications. This body also performs oversight of the work of security-intelligence agencies, monitors and supervises the measures for covert collection of data, collects information and data related to its competences, etc. Additionally, this body can have insight into reports and other documents of the security-intelligence agencies, interview the management staff and other officials of the agencies and, in addition to its own initiative and complaints of citizens, it acts on requests by state bodies and other legal entities.

RECOMMENDATION

- The status if the Civilian Control Council should be appropriately regulated in order to create all necessary preconditions for its efficient technical and material functioning. One of the possible solutions is for the Council to receive the status of a working or expert body in the Parliament.
- In parallel to regulating the status of the Council, a review must be made of all the limitations regarding the competences of the Civilian Control Council in the current LIC. In this, because the legal solutions from R. Croatia were copied as a model during the reform of the security-intelligence sector, they should be taken into account as the starting basis for redefining the legal competences of the Civilian Control Council. In this direction, the Council should be given the right to act directly on received complaints from citizens, as well as unannounced supervision, without the existing time limitation regarding the comparing of court orders. Additionally, the Council should have the right to inspect all the data available to the Committee, as well as insight into the devices of OTA and court orders that have not been anonymized. For this purpose and if the Council has a need for this, it should be provided expert support from the accredited technical experts, regardless of the fact that the Council can comprise persons with formal education in technical sciences, who still do not have to be experts in the field of telecommunications.
- In perspective, in a wider context of the security-intelligence sector, and based on the example of the Council for Civilian Oversight of the Work of the Security and Intelligence Agencies in R. Croatia, the possibility should be reviewed to also expand the competences of the Civilian Control Council over the work of security-intelligence services, in parallel to the parliamentary Committee for oversight of the work of ANB and the Intelligence Agency.

CONTROL OVER INTERCEPTION OF COMMUNICATIONS

Unlike oversight, control over the interception of communications is conducted within judicial bodies. Control over the legality of implementation of measures for interception of communications is performed by the public prosecutor conducting the investigation and the judge of the preliminary procedure who has previously issued the order for interception of communications as a SIM measure, i.e. the Public Prosecutor of R. N. Macedonia and the Supreme Court judge who

issued the order for interception of communications in the interest of security and defense. Control over the manner of usage of the special technical devices and equipment from Article 17 of LIC is performed by the Public Prosecutor of R. N. Macedonia and the preliminary procedure judge who issued the order for interception of communications.

Identical to supervision, control is also determined by a set of factors, the most important of which is the independence of control bodies.

With the aim of efficient control, control bodies, same as oversight bodies, can engage technical experts and perform control as needed and without prior announcement. Article 59 of LIC prescribes the activities that control bodies can perform in the frames of their competences, such as inspecting the location of the work stations used by the authorized authorities, the rooms of OTA where the Law communication interception equipment and the mediation devices are located and also the location where the operators keep the devices for diverting the signal to OTA. Additionally, they may request or directly access the electronic registry system; request an insight or obtain a copy of the registry and the anonymized interception order in a written form; read all logs created, recorded or saved by the systems used by OTA and the operators, etc.

Additionally, the provisions from Article 258 of LCP are also in the context of control by the public prosecutor according to which, during the implementation of SIM measures, the justice police prepares a report that it submits to the public prosecutor at their request and in any event within 30 days, and after the implementation of the measures it drafts a final report with attached complete documents on the technical recording and submits it to the public prosecutor. In turn, the public prosecutor submits the report and complete documents to the court in eight days after adopting the prosecutorial decision.

Related to SIM measures in general, including the measure for interception of communications, Article 271 of LCP obliges the Public Prosecutor of R. N. Macedonia to submit an annual report to the Parliament detailing all the data according to the 8 points contained in Article 271 of LCP.

In practice, the annual reports on application of SIM measures are usually submitted by the Public Prosecutor to the Parliament in seven to nine months after the end of the year they refer to, which is rather inadequate. In addition to this, these reports are not published on the web-site of the Public Prosecution Office and frequently do not contain all of the elements provided in Article 271 of LCP. Data is lacking on the number of proposals for interception of communications submitted to the public prosecutor, how many were approved by the prosecutor, how many own initiatives they had for interception of communications and for how many of the submitted requests a court order was issued. Additionally, the reports do not list the reasons for failure when the interception of communications did not provide relevant results for the procedure, and they do not contain data on the costs generated by the application of SIM measures, including the measure for interception of communications.

RECOMMENDATION

- In the interest of transparency, it would be useful to determine a reasonable timeframe in which the Public Prosecutor of R. N. Macedonia would be obliged to submit the annual report on the application of SIM measures to the Parliament with all necessary elements, and publish the same on the web-page of the Public Prosecution Office.

On the other hand, regarding the legality of implementation of measures for interception of communications, for control purposes the judge must take an extremely diligent approach when issuing orders for interception of communications and objectively assess whether in the specific case these measures are requested as the final alternative, *ultima ratio*, and not as an option applied in the earliest stages of criminal persecution, without exhaustion of other means.

The judiciary in R. N. Macedonia is generally attributed with a low level of criticism and that it almost regularly fails in its role as controller of the work of the police and the public prosecution. The critical points emphasized for this situation are the election, dismissal and reassignment of judges. In support of this statement stands the fact that since the beginning of the application of SIM measures in our country, there has not been a single case of an adopted court decision refusing the request by the public prosecutor for implementation of such a measure.

The experiences in judicial and prosecutorial control thus far, impose the need for establishing certain mechanisms aimed at raising awareness on the proactive role of judges and public prosecutors in the interception of communications, and not only control over the legality of the implementation of the measures and current insight into the reports on the implementation thereof, but also control over the submission of requests for approval, i.e. adoption of the orders for interception of communications. Judges and public prosecutors must delve into essence of the case, bearing in mind all international principles when submitting a request or adopting an order for interception of communications, in particular the principles of proportionality and subsidiarity, and the with them related principle of *ultio ratio*, which means the awarding of invasive measures as the final alternative and ultimate means.

4. OPPORTUNITIES AND CHALLENGES

Reforms in the field of interception of communications, as part of the wider reform of the security-intelligence sector, are indubitably a complex process full of challenges and more or less expected risks that can determine the success of the reform actions.

In the reformed system for interception of communications in R. N. Macedonia there are evident overlaps in competences and insufficiently clear delineation of competences between individual services. The system retained its former complex structure of several bodies authorized to intercept communications for purposes of criminal investigations and in the interest of security and defense. However, equipping the Customs Administration and the Directorate of the Financial Police with the necessary material and human resources for the legal interception of communications is going slowly. Even two years after the start of application of LIC the interception for the needs of these bodies is still realized through the Ministry of Interior, which is the same as prior to the reforms.

Experience thus far has showed that partisan and political influences over the security services sometimes determine their work. This brings into question the professionalism of the services and undermines the citizens' trust. The vetting process during the transformation of certain services (UBK-ANB) was a major challenge and it should have depoliticized them. However, there were certain remarks, especially by the opposition in the Parliament, joined with accusations that this selection of staff is compromised and is based on subjective and political, instead of objective and clear criteria determined in advance.

Regarding oversight and control, the positive legislative step is too slowly being realized in practice. The Committee on oversight of the implementation of measures for interception of communications is still not staffed with technical experts, in spite of the legal obligation to do so immediately after its establishment, and no later than 50 days (Article 39 paragraph 2 of LIC). One of the candidates who applied was selected in a public competition, and the competition was repeated for the selection of the second expert. In the lack of publicly available information on the outcome of this procedure, unofficial information claim that the second expert has not been selected yet.

On the other hand, the Civilian Control Council was expected to be an important corrector of the entities involved in the process of interception of communications, especially due to the fact that this oversight body is comprised of experts and representatives of the non-governmental sector. However, after its establishment, besides the realization of a few protocol activities, the Council did not initiate any other essential activities, which certainly comes as a result of the obstacles in its functioning. These conditions are an indicator that the efforts for acting in accordance with the reform laws did not create any major developments from what was the practice thus far.

These situations lead to the conclusions that oversight, as a powerful tool that should provide accountability of the security services, cannot be efficient if there is lack of political will, political culture and level of awareness on the need for oversight of security services. The fact that the parliamentary Committee for oversight over interception of communications has a mixed composition (representatives from the opposition and the government) and especially that the President of the Committee comes from the opposition party, should

represent an additional mechanism that should provide oversight efficiency. However, one cannot see any significant proactivity in this sense. In order to face the challenge of oversight of security services, members of Parliament, as members of oversight committees, must set aside the narrow partisan and daily political interests.

During the regular control by the Committee for oversight of the implementation of the measures for interception of communications in July 2019 in OTA's premises, it was concluded at the joint press conference by the President of the Committee and the Director of OTA that interception of communications is maximally secure and without possibilities for misuse.[26] However, recently, the current (technical) minister of interior informed the public that the optical cable that enables the discovering of the content of intercepted communications in the criminal investigations still physically passes through the headquarters of the former UBK, which is the location of the new ANB. The conclusion of the minister was that an essential part of the reform was not realized – separation of the interception of communications for purposes of criminal investigations from interceptions for security and defense. OTA and ANB disputed these claims, but the wider public remains uninformed of the outcome from the submitted criminal complaint from the minister of interior to the public prosecution office regarding the allegations. Regarding the other allegations in 2018, on detected devices for recording of communications on fixed devices in the Public Prosecution Office and the Criminal Court in Skopje, the wider public is also not informed on the course of the preliminary procedure that was initiated, nor whether the Committee for oversight of the implementation of the measures for interception of communications has taken actions in relation to this case.

[26] https://ota.mk/mk/190719-pretstavnici-sobranie-poseta-ota

5. CONCLUSIONS AND RECOMMENDATIONS

The process of creating new legislation for interception of communications was approached with great enthusiasm and the belief that success will be achieved in creating a balanced system, which will be efficient in the function it exists for, and will at the same time secure the respect of fundamental human rights. The general conclusion is that legal solutions from other systems were copied without adapting them to the current situations in the country and the existing capacities of the institutions.

There is no doubt that unwritten rules have been incorporated in the everyday work of the security services and the tendency to practice them in the future can result in hidden obstructions in the application of the new laws. Habits are hard to change with legal and administrative means.

The reform laws offered several quality legal solutions, but the functioning of the system as a whole remains disputable. The “Priebe Report” itself stated that only a few recommendations relate to changes in the legislation and that most of the recommendations can be implemented in the existing constitutional and legal framework. Thus, appropriate implementation of the laws in practice is something the institutions should strive for. This is why we cannot consider the reform process as completed, especially bearing in mind the weakness already seen in the practical implementation of certain legal solutions.

Specifically, several disputable questions are left in the reformed legislation, although they were discussed in the debates prior to the adoption of the Law on Interception of Communications. This especially concerns the interception of communications without the mediation of OTA, which practically annuls the sense of existence of this Agency and undermines the trust in the system for legal interception of communications. Additionally, the provisions regarding metadata must be redefined and precisely prescribed, without the contrary provisions that are currently contained in several different laws. Problematic, especially in the technical-legal sense, is the new set of measures for interception of communications in the interest of security and defense, the legal possibility for their preventive implementation and the expansions of the range of criminal acts for which communications may be intercepted.

All of these individual disputable elements can be overcome with a serious and truly honest approach in the creation of legal norms. However, the comprehensive regulation of the field of interception of communications, as well as the control and oversight over security services, still requires planning and undertaking of appropriate measures in the long term, and not only in the normative sense. Bearing this in mind, it would be purposeful to think in the following direction in a wider context:

- Unifying in a single legal text the segments that are currently unnecessarily contained both in the provisions of the Law on Interception of Communications and the Law on Criminal Procedure, and some in the Law on ANB. This creates confusion and different interpretations of the same issues.
- Clear delineation of the competences of security services in order to avoid overlapping of competences and the possibility for misuse in work. This will help avoid absurd situations in which there is different information on the same event, or when the same case or person as a security threat is the subject of observation or work of several services at the same time.
- Creating a clear concept to overcome the evident problem of political influences over the work of security services and judicial bodies, which sometimes dramatically determines their work and seriously undermines their objectiveness and professionalism.
- Creating mechanisms that will contribute to the elimination of partisan-political influences on the persons involved in the oversight and control of interception of communications, raising the level of security culture and strengthening the integrity and trust between all relevant subjects.
- Creation of reliable legal solutions that correspond not only to the needs and capacities of the institutions, but also with reality in a wider context, taking into account the culture, habits and mentality.

BIBLIOGRAPHY

1. **Law on Interception of Communications**, Official Gazette no. 71/18, 108/19
2. **Law on Operational Technical Agency**, Official Gazette no. 71/18, 98/19
3. **Law on Amendments and Supplements to the Law on Electronic Communications,** Official Gazette no. 11/18, 98/19
4. **Law on Amendments and Supplements to the Law on Criminal Procedure,** Official Gazette no. 198/18
5. **Law on Supplements to the Law on Classified Information**, Official Gazette no. 21/18
6. **Law on the National Security Agency**, Official Gazette no. 108/19
7. **Law on the Coordination of the Security-Intelligence Community**, Official Gazette no. 108/19
8. **Law on Criminal Procedure**, Official Gazette no. 150/10, 09/12, 198/18
9. **Law on Electronic Communications**, Official Gazette no. 39/14, 188/14, 44/15, 193/15, 11/18, 21/18, 98/19
10. **Law on Police**, Official Gazette no. 114/06, 114/06, 6/09,145/12, 41/14, 33/15, 31/16, 106/16, 120/16, 21/18, 64/18
11. **Law on Personal Data Protection**, Official Gazette no. 42/2020
12. **Security and Intelligence System Act of the Republic of Croatia**, available at:https://www.uvns.hr/UserDocsImages/dokumenti/nacionalna-sigurnost/ZAKON-O-SIGURNOSNO-OBAVJESTAJNOM-SUSTAVU-RH-NN-79-2006.pdf
13. **The United Nations Convention Against Transnational Organized Crime (2000)**
14. **Directive (EU) 2016/680 of The European Parliament and of The Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data**
15. **Council of Europe Recommendation (2005) 10 of the Committee of Ministers to member states on "special investigative techniques" in relation to serious crimes including acts of terrorism**
16. **Council of Europe Recommendation (2001) 11 of the Committee of Ministers to member states concerning guiding principles of the fight against organized crime**
17. **EUROPEAN COMMISSION Neighborhood and Enlargement Negotiations Urgent Reform Priorities for the Former Yugoslav Republic of Macedonia** https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/news_corner/news/news-files/20150619_urgent_reform_priorities.pdf

18. **The Former Yugoslav Republic of Macedonia: Assessment and recommendations of the Senior Experts' Group on systemic Rule of Law issues 2017**, Brussels, 14 September 2017 https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/2017.09.14_seg_report_on_systemic_rol_issues_for_publication.pdf

19. **European Commission for Democracy through Law (Venice Commission) Rule of Law Checklist, March 2016**, available at: https://www.venice.coe.int/images/SITE%20IMAGES/Publications/Rule_of_Law_Check_List.pdf

20. **Representatives of the Parliament visiting OTA, 19.07.2019,** available at:https://ota.mk/mk/190719-pretstavnici-sobranie-poseta-ota

21. **Annual Report on the Work of the Operational Technical Agency Skopje, for 2018**, available at:https://ota.mk/adocs/scan-izvestaj-ota-2018.pdf

22. **Government of R. N. Macedonia, 45th session held on 22.04.2020**, available at: https://vlada.mk/vladini-sednici/vladini-sednici

DCAF Geneva Centre for Security Sector Governance

P.O.Box 1360
CH-1211 Geneva 1 Switzerland

info@dcaf.ch

+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva