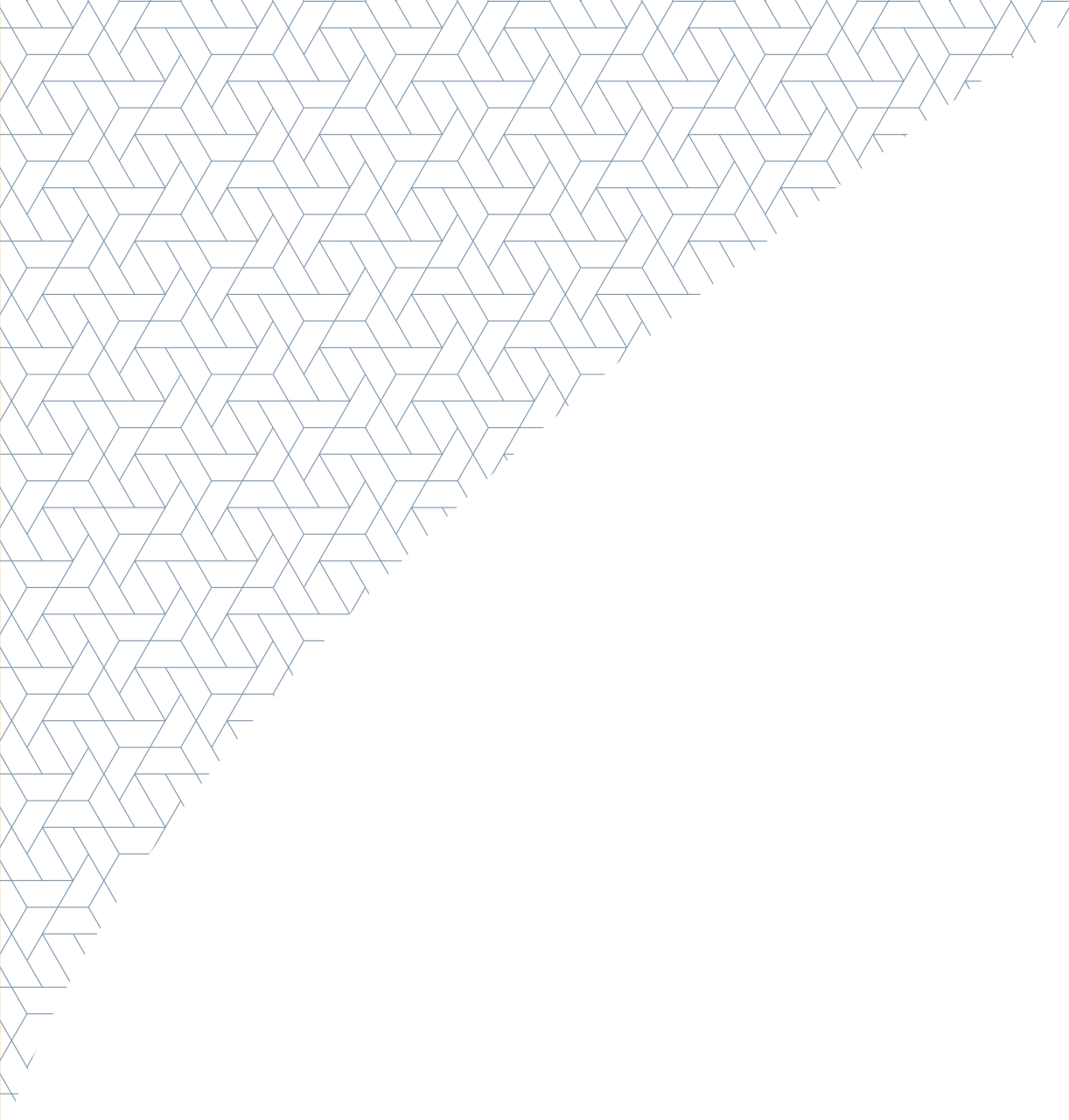


BENCHBOOK

on the implementation of measures
for interception of communications





BENCHBOOK

on the implementation of measures
for interception of communications

DCAF Geneva Centre
for Security Sector
Governance

 Republic of North Macedonia
Academy of Judges and Public Prosecutors
Pavel Shatev

Skopje, December 2019

BENCHBOOK
ON THE IMPLEMENTATION OF MEASURES FOR INTERCEPTION OF COMMUNICATIONS

Authors:

Public prosecutor Spasenska Andonova
Andrej Bozhinovski, M.A.
Judge Daniela Dimovska
Bogdancho Gogov, PhD
Jovan Jovcheski, PhD
Biljana Karovska Andonova, PhD
Judge Sandra Krstikj
Snezana Petrovikj Arsovska
Justice Xhemali Saiti
Public prosecutor Natasha Saramandova

Editors:

Gordan Kalajdjiev, PhD
Penelopa Gjurchilova, PhD

Publisher:

©DCAF, 2019
All rights reserved.
DCAF – Geneva Center for Security Sector Governance
Chemin Eugène-Rigot 2E, CH-1202 Geneva, Switzerland
©DCAF, 2019
All rights reserved.
DCAF – Geneva Center for Security Sector Governance – Skopje Office
Makedonija 11-1/2 Skopje, Republic of North Macedonia

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

343.985:316.77(497.7)(035)
343.985:316.77]:355.45(497.7)(035)
342.738(035)

BENCHBOOK on implementation of measures for interception of communications : Електронски извор / [authors Jovan Jovcheski ... и др.]. - Скопје : Geneva center for security sector governance, Skopje office DCAF, 2019

Начин на пристап (URL): <https://dcaf.ch/resources?type=publications&year=2019&lang=all>. - Текст во PDF формат, содржи 141 стр., илустр. - Наслов преземен од екранот. - Опис на изворот на ден 25.11.2019. - Други автори: Biljana Karovska-Andonovska, Bogdancho Gogov, Andrej Bozhinovski, Xhemali Saiti, Sandra Krstikj, Daniela Dimovska, Natasha Saramandova, Spasenska Andonova, Snezana Petrovikj-Arsovska

ISBN 978-608-66453-5-9

1. Jovcheski, Jovan [автор] 2. Karovska-Andonovska, Biljana [автор] 3. Gogov, Bogdancho [автор] 4. Bozhinovski, Andrej [автор] 5. Saiti, Xhemali [автор] 6. Krstikj, Sandra [автор] 7. Dimovska, Daniela [автор] 8. Saramandova, Natasha [автор] 9. Andonova, Spasenska [автор] 10. Petrovikj Arsovska, Snezana [автор]

а) Посебни истражни мерки - Следење на комуникации - Македонија - Прирачници б) Национална безбедност - Посебни истражни мерки - Следење на комуникации - Македонија - Прирачници в) Право на приватност - Прирачници

COBISS.MK-ID 111715594

PROJECT BACKGROUND AND ACKNOWLEDGEMENTS

European countries, including the Republic of North Macedonia, require their law enforcement and intelligence services to obtain judicial warrants before using Special Investigative Measures (SIM), or other methods for information collection deemed to be particularly intrusive with regards to the right to privacy. Through the authorization of SIM, judges and prosecutors act as guarantors of the rule of law and balance the competing interests of ensuring public safety and safeguarding human rights and liberties. For these reasons, the Programme launched by DCAF in North Macedonia in 2017, to support national authorities in improving security and intelligence sector accountability, had planned from its very beginning to engage (among other actors) with the judicial sector in the country, and help develop capacity and expertise in the judicial authorization of communications interception.

After reviewing existing resources on this topic and holding consultations with representatives of the Macedonian judicial and academic community, the idea to create a new knowledge product tailored to the needs of the Macedonian judiciary emerged as a priority for the DCAF judicial project. The national system for communications interceptions was undergoing significant legislative and institutional changes, while the rapidly growing European jurisprudence on the use of secret surveillance by state authorities was setting high standards as regards the duty of the Courts to scrutinize critically the applications for the use of SIM. The DCAF project proposed to have all these new national regulations and European standards collected and analyzed in a Benchbook that would guide practitioners in the different procedural stages of the judicial control of SIM.

To this end, together with the Academy for Judges and Prosecutors, and enjoying the support of judicial institutions in Skopje, in April 2018 we were able to assemble a working group composed of judges, prosecutors and judicial experts willing to support the development of this knowledge resource. *What* exactly to create and *how*, were questions without easy straightforward responses. It took months of recurring discussions and in-depth analysis of law, procedure, practice, and landmark decisions of relevant European courts before deciding on the detailed outline of the Benchbook. By the end of September 2018, a clear structure of the Benchbook was decided upon, building around three main chapters: (1) a first one reviewing the theoretical and legal foundations of judicial authorization of SIM, (2) a second one providing “a pathway on how to issue an order for the use of SIM in criminal investigations”, as described by one of the judges participating in the project, and, (3) a third one exploring a brand new topic for local judicial literature: the authorization of intrusive methods for national security purposes. The members of the working group, split into three, each team taking the responsibility to draft one chapter, under the leadership and theoretical guidance of a group coordinator. And then, the writing began.

Benchbook development was a genuinely participative process. What is sincerely laudable and somehow surprising, given the professional responsibilities and the hectic agendas of the people involved in this working group, is the fact that they took complete ownership of the writing process. The outline and the content were exclusively *decided on* and *drafted by* them, based on their own knowledge, expertise, research efforts and time. No parts of the Benchbook were outsourced to

external consultants. The ten authors of the Benchbook invested a remarkable individual and collective effort, sustained with patience and professionalism over the course of one year. It is therefore our pleasure to acknowledge and give credit to the ten authors, whose dedication and diligence made this publication possible. We trust that their participation in this project has empowered and inspired them to act as agents of change, who raise the standards of performance to a higher level, influencing the entire judicial system.

Three coordinators, one for each chapter, were selected by their respective drafting teams to provide conceptual guidance, to steer the drafting process and the engagement of different authors. Supreme Court judge Xhemali Saiti, judge Sandra Krstikj and Andrej Bozhinovski, MSc, completed this task admirably, and invested substantial individual efforts and time into this project. Their dedication, direction, and substantive input have been the engines that transformed the Benchbook from an idea to a palpable reality.

The first integrated draft of the Benchbook was completed in January 2019, when a meticulous internal review process started under the coordination and editorial effort of Professor Gordan Kalajdjiev and our colleague dr. Penelopa Gjurchilova. Working with ten different authors, from a range of institutions and perspectives, was not an easy task for the editors. It is with a great debt of gratitude that DCAF wishes to extend a heartfelt thank you to them both. It is their wisdom, hard work, perseverance and leadership that ultimately led to this unique and groundbreaking publication.

The Benchbook was written in a period of profound transformation of the intelligence environment and of the system for communications interception in North Macedonia. Laws, institutions and processes have all changed significantly in the span of just one year. All these changes had to be observed, understood and incorporated into the text, slowing down the writing process and requiring adjustments in the Benchbook structure and content. A fourth chapter was added in spring 2019, to provide an overview of the whole system of democratic safeguards in the use of communications interception. Dr. Jovan Jovcheski has taken the lead in the development of this chapter and we thank him sincerely for his valuable contribution.

Thanks are due also to the legal experts who undertook the external peer-review of the Benchbook. Coming from Croatia and Slovenia, Dr. Sunčana Roksandić and judge Aleš Zalar read the text with eyes well versed in the latest European developments in criminal justice and human rights law. Dr. Marjan Gjurovski and Aleksandar Tumanovski, MSc, brought in the viewpoint of professionals who know well the Macedonian legal system, with its conceptual and practical challenges. The reviewers have all shared perspectives from which a great deal was learned. The Benchbook is better due to their rigorous scrutiny.

It is our pleasure to acknowledge and give credit to the Academy for Judges and Prosecutors for making this project a successful reality. They have been DCAF's partner from the very early stages. They helped us reach out to the right institutions and people and, with every workshop and roundtable we organized together in this project, made sure the Benchbook is a product designed for and tuned to the learning needs of the Macedonian judiciary. In the months following the Benchbook publication, the Academy will take the lead in transforming the Benchbook into a training curriculum for judges and prosecutors, to be introduced into their annual training program. We sincerely hope that this will be a long-term engagement that will generate better awareness and understanding

of the opportunities members of the judiciary have to act with professionalism, integrity, and in the spirit of separation of powers - thus contributing to improved independence of the judiciary.

The Benchbook is available in three languages: English, Macedonian and Albanian. We would like to give special thanks to Ivan Kolekevski, Edona Vinca, Filip Markovikj, Daniela Takeva, MA and Gazmend Qoku who have undertaken the tasks of translation and proof reading and have completed them timely and professionally.

Very special thanks to our colleagues Dr. Kire Babanoski, Vlado Gjerdovski, MSc, and Matilda Todorova for their valuable contribution to the Benchbook completion. They have been responsible for a variety of tasks, from review and editorial support to the management of translation and publication activities; all these were indispensable for the success of this project.

Finally, we would also like to express our gratitude and appreciation to the Programme donors who have made this judicial product possible: Ministry of Foreign Affairs of The Netherlands, Swedish International Development Cooperation Agency (Sida) and the Swiss Agency for Development and Cooperation (SDC).

Dr. Teodora Fuior, project coordinator, DCAF
Marc Remillard, programme manager, DCAF

“The content of this publication does not necessarily reflect the position or the opinions of the donors”



Kingdom of the Netherlands



Sweden
Sverige



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss agency for Development
and cooperation SDC

LETTER
from the
Director of the Academy for Judges and Prosecutors

Dear all,

One of the more significant topics that stir up interest among experts and academia in the Republic of North Macedonia is special investigative measures and their application. The reason for this increased interest is to be found in the actual nature of the special investigative measures, which represent a relative novelty in the Macedonian criminal-legal system (introduced in 2002), as well as in the fact that the use of these measures produces exceptionally important evidence, most often acquired through intrusion and serious invasion and restriction of the fundamental human rights and freedoms of the defendants and other persons. Therefore, it is necessary to eliminate any arbitrariness in the use of these measures by authorized institutions, because of the threat of possible violations or restrictions of the rights that protect the personal integrity and secrecy of personal communications of the persons subjected to these measures. Still, on the other hand, in order to protect the public interest, one has to provide for a successful fight against crime. Therefore, the Criminal Procedure Code provides for a special procedure for enhanced control of institutions that implement these measures. The adopted legal mechanism must be carefully applied by the judicial institutions, because their work in this regard is under permanent scrutiny by the public and the media, but also by concerned citizens.

DCAF's programme for reforms of the security-intelligence services in the Republic of North Macedonia, in cooperation with the Academy as one of the project partners, has implemented the project of "Benchbook on the implementation of measures for interception of communications". The Project's objective is to strengthen the judicial and prosecutorial capacities and expertise in the authorization and oversight of the use of special investigative measures for the purpose of collecting information by security-intelligence services. The result of this one-year collaboration is the publication of this Benchbook, which offers a practical overview of the principles and existing standards that legal practitioners could use in the processes of requesting, authorization and supervision of the interception of communications. Through analysis of the international standards and ECtHR case law, the Benchbook offers clear and practical guidelines for judges and prosecutors on the implementation of these measures, as well as on the various ways of collecting evidence, while being mindful of the proper authorizations.

The adopted the set of laws in the field of interception of communications back in April 2018, has significantly reformed the institutions and processes that constitute the country's system for interception of communications.

I would like to express my gratitude for the DCAF's initiative to launch this project in the Republic of North Macedonia, dealing with a topic that is of current interest and quite sensitive. The organization of numerous working meetings and roundtables was, undoubtedly, of enormous significance during the cooperation thus far and I believe they have been of assistance to the board members (a group of Macedonian judges, prosecutors and legal experts) in drafting the Benchbook.

In conclusion, let me highlight my commitment to the continuation and enhancement of our cooperation with DCAF, aimed towards raising the awareness and strengthening of the capacities of judges, prosecutors and representatives of all relevant institutions, thus strengthening the national response to any challenges arising from the use of these measures.

Prof. Dr. Natasha Gaber Damjanovska
Director, Academy for Judges and Prosecutors

CONTENTS

SUMMARY	13
REVIEWS	15
ACRONYMS	18
INTRODUCTION	19

PART 1

DEFINITION, PRINCIPLES AND STANDARDS FOR INTERCEPTION OF COMMUNICATIONS

1. Definition of privacy and right to privacy	23
1.1. Scope of the right to privacy and areas of protection	23
1.2. Home privacy	24
1.3. Secrecy of communications as an aspect of privacy	24
1.4. Personal data as an aspect of privacy	26
2. Right to privacy versus the need for efficient measures in the interest of security and fight against crime	27
3. Legitimate restriction of the right to privacy	28
4. International principles and standards for the implementation of measures for interception of communications	29
4.1. International principles	29
4.1.1. Legality principle	30
4.1.2. Subsidiarity principle	30
4.1.3. Proportionality principle	31
4.1.4. Principle of judicial approval of intrusive measures	31
4.2. International standards	33
4.2.1. Standards related to the legality principle	33
4.2.2. Standards related to the subsidiarity principle	34
4.2.3. Standards related to the proportionality principle	34
4.2.4. Standards related to the principle of court approval of intrusive measures	36
5. Cases of secret surveillance	36

PART 2

SPECIAL INVESTIGATIVE MEASURES IN CRIMINAL PROCEDURE

1. Introduction	43
1.1. Types of special investigative measures in the national legislation	44
2. Crimes entailing the use of special investigative measures	46
2.1. Domestic case law examples	47
2.2. Commencement of the special investigative measures and making a decision over their use	49
2.3. Request by the Public Prosecutor's Office for interception of communications	50

2.4. Receipt and registration in the Public Prosecutor's Office	52
3. Procedure of issuing special investigative measures by the court	53
3.1. Anonymization	54
4. Grounds for suspicion as an assumed standard for measures' activation	55
4.1. Elaborated reasons why data or evidence cannot be collected by other means	56
4.2. Urgency of procedures	57
5. Use of special investigative measures as evidence in the criminal procedure	58
6. Duration of measures and their extension	59
6.1. Rejection of a request for issuance of special investigative measures	60
6.2. Expansion of the order	60
6.3. Termination of SIMs	61
6.4. Notification of person concerned	61
6.5. Legal access to the obtained data	62
6.6. Erasing or destroying collected personal data	62
6.7. Storage and disposal of data collected using special investigative measures for interception of communications	62
ANEXES TO PART 2	64

PART 3 NATIONAL SECURITY

1. Definition of national security	71
1.1. Defining national security and defense in the domestic legislation	71
1.2. International legislation on national and international security	72
2. Regional and international cooperation	75
3. Role and position of the security-intelligence services in a democratic society	76
4. Intrusive measures as integral part of the working methods of the security-intelligence services	78
5. Prevention in security	80
6. Threats to national security and defense	80
7. Authorized institutions for implementation of measures for interception of communications for the purpose of protecting state security and defense	81
8. Measures for interception of communications	82
8.1. Criteria for use of measures for interception of communications	84
8.2. Criteria for issuing an order	85
8.3. Request for issuance of an order and deciding on the request	85
8.4. Justification of the use of measures for interception of communications	86
8.5. Content of the order for interception of communications and its anonymization	87
8.6. Anonymization method	88
8.6.1. Anonymization of the order for OTA	89
8.6.2. Anonymization of the order for oversight and control	89
8.6.3. Recording in the Order Register	90
8.7. Duration and extension of the measure for interception of communications	90

8.8. Reports	91
8.9. Termination of the measure for interception of communications	91
9. Urgent procedures	91
10. Storage and disposal of data collected using measures for interception of communications	92
11. Obligation for keeping official secrets	93
ANEXES TO PART 3	95

PART 4

CONTROL AND OVERSIGHT ON THE USE OF SPECIAL INVESTIGATIVE MEASURES

1. Introduction	101
2. Oversight of the measures for interception of communications pursuant to the domestic legislation	103
3. Control of the measures for interception of communications in the domestic legislation	104
4. Public (independent) oversight of measures for interception of communications	107
4.1. Citizens' Control Council	107
4.2. Directorate for Personal Data Protection	107
4.3. Directorate for Security of Classified Information	108
4.4. Ombudsman	108
4.5. Annual report of the Chief Public Prosecutor of RN Macedonia	108
4.6. Other authorities	109
ANEXES TO PART 4	110
BIBLIOGRAPHY	111
ANEXES TO THE BENCHBOOK	113



SUMMARY

The project “Benchbook on the Implementation of Measures for Interception of Communications” is part of the DCAF’s programme for reform of the security-intelligence services in the Republic of North Macedonia, launched in 2017, supporting the national reform efforts aimed at increasing the level of responsibilities in the security-intelligence sector in compliance with the European standards and good practices. The Project’s goal is to enhance the judicial capacity and expertise in the authorization and supervision of the use of special investigative measures (SIMs) for the purpose of collecting information by the security and intelligence services.

The Benchbook is drafted by legal experts and members of the judicial system for whom it is intended. The Benchbook encompasses all 12 legally prescribed SIMs, presenting their scope and providing fast access to them by the users. In addition, the Benchbook provides a detailed presentation of the measures for interception of communications. It provides a concise and practical overview of the principles and existing standards that could guide prosecutors and judges in the processes of requesting, authorization and supervision of interception of communications.

The process of creating this Benchbook lasted for about a year and it was conducted by the Review Board – a group of Macedonian judges, prosecutors and legal experts. DCAF provided the methodological guidelines in the drafting process and facilitated the access of the Review Board members to the relevant European case law and best practices, thus contributing to the development of knowledge, skills and expertise within the group.

While analyzing international standards, especially the jurisprudence of the European Court of Human Rights, but also the national legislation in this field, the Benchbook incorporates four separate but complementary parts and offers clear and practical indicators and guidelines that should serve as a starting point for prosecutors and judges in the processes of drafting requests, approving, applying and supervising the use of special investigative measures and other intrusive methods for information collection by the security and intelligence services.

In this respect, the **first part** of the Benchbook provides a brief overview of the personal rights that might be potentially jeopardized by the use of SIMs and methods. The emphasis of this section is placed on the presentation of the well-established international principles and standards and their content, as starting grounds for harmonized use of such intrusive measures and methods. The analysis of the above mentioned aspects is followed by an overview of the case law of the European Court of Human Rights, related to specific cases involving this subject matter.

The **second part** of the Benchbook individually elaborates the basic features of the special investigative measures identified in the national legislation, as well as the relevant elements in submitting requests for the use of these measures and their approval, period of use, criteria for expansion of the orders, notification of concerned parties, destruction of collected evidence etc.

The **third part** of the Benchbook discusses the measures applied by specialized state authorities, such as military and security-intelligence services, aimed towards protecting the country from any actions that could jeopardize its survival, sovereignty, core institutions or vital values. Special emphasis has been given to the measures for interception of communications in the interest of the country’s security and defense, identified in the new national legislation for interception of communications.

The **fourth part** of the Benchbook deals with the control and supervision of the use of special investigative measures, the competent institutions and the public (independent) oversight of their use..



REVIEWS

Authors of the Benchbook on implementation of measures for interception of communications provide a comprehensive but rather theoretical presentation of the legislation related to the measures, which is important in acquainting the reader with the subject matter at hand. Intervention in the right to privacy is elaborated through European Court of Human Rights case law, which is a positive step in this regard.

Instruments used for communication are also explained from the aspect of their legality, using the standards of clarity, precision and predictability, as well as the need for balance and proportionality in the restrictions that are set to protect the rights of the others. Beneficiaries of the Benchbook are able to understand and assess with certainty and clarity which are the designated institutions that can ask for interventions in the right to privacy and the reasons thereof.

The list of institutions to carry out interventions in the interception of communications by giving orders and requests for their termination is clearly presented. The Benchbook also includes practical examples of such orders and requests, which will surely be of use for all stakeholders in the implementation of the measures for interception of communications.

The Benchbook lacks a more detailed elaboration and analysis of the control and oversight of the implementation of measures for interception of communications, as is the case for other segments in this field. There is also a lack of practical examples of provisions related to control and oversight of legality in procedures. This is maybe due to the inexistence of proper legislation.

Considering that the Benchbook has elements of an academic thesis, which needs to be highlighted, the abovementioned analysis is required, especially since the Law on Interception of Communications experiences certain problems in its content and implementation.

In general, the Benchbook's continual use will facilitate the work of all listed institutions and contribute to proper proceedings on their part, having in mind the legality over security and defense and the fight against severe crimes, as well as the non-violation of other human rights.

Margarita Caca Nikolovska

Vice-President and Judge of the Constitutional Court of Bosnia and Herzegovina
Former judge to the European Court of Human Rights

* * *

The Benchbook on implementation of measures for interception of communications, a part of the DCAF programme for security-intelligence reform in the Republic of North Macedonia, is an interesting and important resource not only for legal practitioners but also for the wider public. The Benchbook deals with one of the most sensitive areas in the law and justice system: the authorization and oversight on the use of special investigative measures (SIMs) for information collection by law enforcement, security and intelligence services. It was carefully drafted and reviewed, in a collective process that lasted about one year, by law experts and members of the judicial system that gave serious consideration to the jurisprudence of the European Court of Human Rights (ECtHR) when analysing national legislation. Therefore, the recommendations given throughout the Benchbook are following legal boundaries and following main principles set by ECtHR. Hence, this Benchbook will

without a doubt be an excellent guide for prosecutors and judges when requesting, approving, using and performing the oversight of the implementation of special investigative measures and other intrusive methods for information collection by law enforcement, security and intelligence services.

It is impossible to emphasise which Chapter is most important. However, regardless of whether the Benchbook will be used by practitioners in criminal proceedings or by military and security-intelligence services, it is recommendable that Chapter One and Four is read in any case by all stakeholders. It is extremely important to be aware of the content of the established international principles and standards when one is using intrusive measures and methods. The same is relevant for their oversight.

I sincerely congratulate all the authors for succeeding in creating important guidelines in this very sensitive area.

Doc. dr. sc. Sunčana Roksanđić Vidlička

Assistant professor at the Department of Criminal Law, Faculty of Law, University of Zagreb
Researcher in the Max Planck Partner Group Balkan Criminology

* * *

Special investigative measures (SIM) are requested, ordered and implemented by law enforcement agencies, intelligence and security agencies and courts across the globe to fight serious crimes, including terrorism, and to avert dangers to national security.

Courts and judges are often in a difficult position when exercising judicial ex-ante authorization and ex-post control of SIM due to various reasons such as legal ambiguity and loopholes, secrecy of operations and files, limited access to relevant information and evidence in the early stage of the proceedings, lack of procedural competence, or considerations that policy elements outweigh the adjudicative elements. The requirement for judicial authorization and control subordinate's public safety and national security concerns to the rule of law, representing a major safeguard against abuses; however, this does not automatically prevent a massive overuse of SIM. The case-law of the European Court for Human Rights (ECHR) reveal serious challenges in the application of minimum human rights standards, not just for governments and legislators of the Council of Europe Member States, but also for their judiciaries. For example, how to apply the standard that any ordered SIM should have reasonable basis in facts? What is meant by the standard that reasons presented in a request for the use of SIM must be relevant and sufficient? What is the difference between the standard of necessity and the standard of strict necessity? Should the collection and storage of information concerning emails and personal internet usage at the work place be considered as interference with the right to respect for private life, home and correspondence? How to ensure the access to and assessment of classified information by judges? Does the standard of *quality of law* include the quality of national case-law?

Answers to these and many other questions can be found in this resource. The Benchbook is not a source of substantive law, but a practical guide for prosecutors and judges on how to interpret and apply basic principles of the rule of law and the protection of human rights and fundamental freedoms. The Benchbook does not and, in fact, cannot exhaust all relevant legal issues, which might occur within the decision-making process concerning SIM. Nevertheless, the added value of this Benchbook is multi-faceted. It addresses in separate chapters the authorization of the use of SIM for

the purpose of criminal proceedings, and for the protection of national security, allowing the reader to compare the procedural steps, as prescribed by domestic procedural laws and regulations, and through legal principles, rules and standards of substantive laws as interpreted in domestic and European jurisprudence. Selected ECtHR landmark decisions are summarized to explain most important principles and standards.

The writing of the Benchbook by local experts represented a peer to peer learning process. Being a completely locally owned product, the co-authors will surely have the vigilance and the interest to ensure that the Benchbook will be constantly updated and supplemented with relevant commentary on amended laws and regulations and on developments in domestic and European case-law. In such a way the consistency and foreseeability of national case-law concerning authorization and review of SIM will be ensured on a long run.

The Benchbook will hopefully contribute to strengthen the judicial courage, a necessity when additional information, clarification or documentation must be requested from powerful security institutions, prior to issuing or extending a judicial warrant for the use of measures that are highly intrusive to the right of privacy.. It happens too often in European courts that no sufficient factual information is provided in the request for a judicial warrant, and the court consequently cannot balance the interest of public safety or national security against the seriousness of the interference with individual human rights. Courts should courageously order, whenever they deem it necessary or appropriate, certain conditions for the judicial warrant, inter alia, to receive reports on the implementation of SIM and even transcripts of intercepted communications.

Although drafted by prosecutors and judges, the Benchbook will hopefully inspire the legislators as well, in exercising parliamentary oversight concerning implemented SIM and in drafting and improving legislation on SIM because it provides clear guidance as regards the application of the constitutional principle of separation of powers.

Last but not least, the Benchbook represents a first and innovative attempt in European developing democracies, as a practical guidance for prosecutors and judges as well as for members of other law enforcement, security and intelligence agencies, when dealing with SIM. Its structure and parts on European standards could serve as a model for similar handbooks to be developed in other countries. I am sincerely grateful to DCAF for being able to contribute to this important project.

Aleš Zalar

President of the European Centre for Dispute Resolution
Former Judge and President of the District Court in Ljubljana
Former Slovenian Minister of Justice

ACRONYMS

ACCMIS	- Automated Court Case Management Information System
ARNM	- Army of the Republic of North Macedonia
CC	- Criminal Code
CoE	- Council of Europe
ECHR	- European Convention on Human Rights
ECtHR	- European Court of Human Rights
EU	- European Union
ICCPR	- International Covenant on Civil and Political Rights
LCP	- Law on Criminal Procedure
LEC	- Law on Electronic Communications
LIA	- Law on Internal Affairs
LIC	- Law on Interception of Communications
LNSA	- Law on National Security Agency
LP	- Law on Police
MoI	- Ministry of Interior
MoD	- Ministry of Defense
NATO	- North Atlantic Treaty Organization
OTA	- Operational Technical Agency
PPO/BPPO	- Public Prosecutor's Office / Basic Public Prosecutor's Office
RAIC	- Register of authorized interception of communications
RNM	- Republic of North Macedonia
SCRNM	- Supreme Court of the Republic of North Macedonia
SIM	- Special Investigative Measures
UN	- United Nations

INTRODUCTION

Incorporation of intrusive measures in criminal and procedural legislation is a relatively new development in the comparative and international law. These are measures that were, until recently, only used in the operations of the so-called secret (intelligence and security) services, where they still remain the basic *modus operandi*. By nature, the measures in question are quite suited for detection, identification and interception of criminal activities even before the commencement of any illegal actions, in compliance with the new concept of preemptive action, i.e. the concept of *ante delictum*. They represent a strong and adequate weapon available to security-intelligence services in fighting and intercepting different forms of organized crime, corruption, terrorism and other severe forms of crime.


The legalization of these intrusive measures has gradually extended the number of authorities that can legally use this methodology in response to the newly-emerging forms of organized crime, terrorism and other contemporary security threats. Intrusive measures are used only when necessary and with the purpose of securing evidence and data required for the successful management of the criminal procedure or for the protection of interests of national security, but cannot be collected otherwise.

As such, they undoubtedly contribute to the efficient fight against severe forms of crime and other violations and endangerment of public and national security. However, their implementation also represents a real intrusion in an individual's private life. Therefore, when legalizing their use, it is essential to achieve a balance between two opposing antipodes: efficiency of the criminal legislation and protection of the fundamental human rights and freedoms of the individual.

The concept of preemptive action involves normative regulation of security and defense issues in adequate laws, doctrines and strategies, while operations involve measures and activities by state institutions based on consistent implementation of the normative and theoretical regulations for protection of the state's vital values and interests.

Prevention of security and defense also involves diplomatic, political, security, intelligence, informative, financial, customs, judicial and other activities, as an important prerequisite for effective state security and defense. Prevention, being the fundamental form of security protection, has been a subject of long-standing discussions by a large number of scientists and experts of diverse academic fields. These discussions are aimed to theoretical understanding of prevention, differentiation of preventive measures and activities, as well as to identify the institutions-carriers of prevention activities and the need to draft an analysis of the state of security. In general, prevention is related to a series of measures and activities that should make it possible to avoid any threats and risks on security and defense.

Security prevention can be defined as: measures that reduce or in other way contribute to the quantitative and qualitative reduction of threats and risks to security and the sense of insecurity



among citizens, directly or through the reduction of any threatening activities or through political interventions, in order to reduce the probability of attacks on the security and the defense.

All preventive efforts are essentially focused on the social environment and the specific situation, the potential perpetrators or groups and organizations, and possible victims and targeted facilities for an attack. Nowadays, in the security-scientific sense, the “threat” term or concept is used to describe the entities involved in any possible event, which can potentially cause damages to the state or its citizens.

PART 1

DEFINITION, PRINCIPLES AND STANDARDS FOR INTERCEPTION OF COMMUNICATIONS





1. Definition of privacy and right to privacy

The right to privacy is one of the fundamental human rights. Although the term *privacy* seems to be generally familiar to us all, there is still no commonly accepted definition of privacy. Certain authors believe that “the word ‘privacy’ is very vague because there are so many things in our daily lives that we cannot keep to ourselves and yet many other things that we want to keep private” (*Garrett, 2001, p.7*). Privacy is an intrinsic personal right and implies limited access of others to the individual (*Flaherty, 1989, p.8*). It protects the individuality, independence, dignity and integrity of the individual (*Bloustein, 1964, p.971*). Through the legislative standardization of the privacy concept, the state should in effect ensure the observance of this right by all other individuals, institutions and the state itself.

The European Court of Human Rights (ECtHR), although establishing that private life is a broad concept, for which it is impossible to give a comprehensive definition, provides certain guidelines in its case law regarding its significance and scope (*Harris, O’Boyle, Warbrick, 2009, p.364*). In the case of *Niemietz v. Germany*, the ECtHR finds that it would be too restrictive to limit the notion to an “inner circle” in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.

Attitudes related to privacy (legal, sociological, ethical etc.) differ across societies, and privacy is also experienced differently among individuals, resulting in different expectations about privacy. Furthermore, “attitudes about privacy have certainly changed over time”. (*Garrett, 2001, p.7*). Especially today, reasonable expectations about privacy are susceptible to the influence of current social tendencies in different fields and the need to adapt these reasonable expectations with modern tendencies. Therefore, establishing the term privacy must be put in a context of the general societal circumstances in the given time period and reviewed in that context.

1.1. Scope of the right to privacy and areas of protection

The right to privacy protects an exceptionally broad scope of personal interests. The scope of privacy and spheres of protection is a complex issue that mainly refers to identifying the segments of an individual’s life that can be observed under the right to privacy. The scope of protected personal interests expands to diverse aspects of the personal life and family relations, including identity and parental rights, up to the right to a healthy environment as an aspect of private life. ECtHR also broadly defines the scope of Article 8 of the ECHR that refers to the protection of private and family life, home and correspondence, even when a specific right of this article is not established. Still, its scope is not unlimited (*Guide on Article 8 of the ECHR, 2019*).

The scope of the right to privacy has an expansion tendency. The development of the contemporary information-communication technology strongly influences this tendency. The evolution of positions on certain human relations generates new relations and issues that can be encompassed within the scope of private life.

Privacy can also be distinguished as:

- **spatial privacy** that refers to the home but also other areas where the individual lives;
- **information privacy** as an aspect of privacy relating to the collection of data about the individual, management of this data and its use; and

- **communication privacy** relating to personal records, correspondence and other type of communication. (Boban, 2012, p.584).

Privacy and secrecy, but also **intimacy** as a separate field in the secret sphere, can be distinguished as the main areas in private life (Dropulic, 2002, p.48). According to the so-called *Theory of Three Spheres*, which is relevant in the settlement of the conflict between the search for the truth in criminal procedures and the protection of individual interests (Resner, 2007, p.6; Schroeder, 2010, p.83), one can distinguish a **social sphere** that incorporates business conversations and other events, versus the **private sphere** that includes private conversations and other private events, and an **intimate sphere** as a sphere of intimate life and internal processes.

1.2. Home privacy

The right of privacy of the home guarantees the continual enjoyment of private and family life in the area that a person has determined as a place for his/her stay and residence. The inviolability of the home is a core issue in relation to any police activities focusing on searching certain areas, arrest of a suspect or defendant by intrusion in the home of that person, as well as in relation to any seizure of items that are relevant and can be used as evidence in a criminal procedure.

When interpreting the notion of a 'home' in the sense of Article 8 of the ECHR, the ECtHR does not restrict it only to the place or space in which the individual lives, but also the area in which the individual resides temporarily. For example, a home in the sense of Article 8 Paragraph (1) is a hotel room used by a homeless person, with the housing fee paid by the local authorities (*O'Rourke v. United Kingdom*).

In addition, the ownership of a facility is not a required condition, because a 'home' in the sense of Article 8 is also the space in which a person lives or resides by way of lease or other grounds. A relevant fact for each specific case is the continuity of the link with a certain space and certain aspects such as a registered address of residence, postal address, sharing maintenance costs etc.

The ECtHR also includes office space and other official areas encompassing a business activity under the term 'home', in the sense of the right provided in Article 8 of the ECHR. The court formed this position in *Niemietz v. Germany*, establishing a breach of Article 8 of the ECHR by saying that the search of the law office of the applicant was not proportionate to its objective. In addition, the ECtHR noted that the search warrant was drawn in broad terms and allowed for search and seizure without any limitations and without any procedural requests for search of the office where the attorney (applicant) also kept confidential materials of other clients. The explanation for this extensive interpretation of the home lies in the fact that business activities, especially of persons engaged in freelance professions, such as lawyers, artists etc., can often be identified with the home as the place where they are undertaken. In addition, many private relations can be realized in the scope of the official activities and therefore it is sometimes impossible to precisely distinguish these areas and the relations within these areas.

1.3. Secrecy of communications as an aspect of privacy

Within the scope of human rights, the right to secrecy of communications belongs to the category of first-generation human rights, along with the right to life, equality before the law, freedom of speech, right to fair trial, freedom of religion or the right to vote. Today it is given the status of "old right in a new world" (Ruiz, 1997, p.1). Namely, the development of the computer era has dramatically altered the manner of communications and significantly enlarged the possibilities of the contempo-

rary communication technology. As a result of the changes, a so-called information society has been established. Electronic communications and media play a central role in its establishment, as contemporary forms of instant textual, audio or visual communication that is functioning regardless of the geographic location of the communicating individuals. This expansion of modern means of communication has changed the forms and ways of communication, and in doing so, surfaced the important issue of secrecy of communications.

The secrecy of communications can be defined as a right of the one who is telling, announcing, writing or confiding something to another as an information, data or secret, or sharing or experiencing as an emotion with another, and it is for this person to decide whether someone else, or who, should know the content of the things that have been said or confided (*Karovska-Andonovska, 2013, p.100*). The core of this right is comprised of the uncensored communication with other people, regardless of the type and means of the communication process. Thereby, the right shall not be violated if the content of the communication is revealed to the other side that took part in that communication. Revealing the content of the communication by a person that took part in that communication is an issue of trust between the individuals who communicated, and in case of a lawsuit filed by the other person, any violation of secrecy could possibly be treated as an issue of violation of the right to private life.

The right of secrecy of communications also relates to self-communication expressed in a form of saved personal material records (diaries, notes, written positions, personal archives and other notifications). Personal material records can contain notes by which the person is not directly concerned, as well as notes that refer to the private or business life of the owner of the material record. Regarding self-communication and its treatment as evidence in the criminal procedure, certain German authors (for ex. D.Roessner, F.K.Schroeder) point to the use of the so-called "Theory of Three Spheres" and consider that notes by which the person is not affected can be used as evidence, while notes relating to the private life should be inviolable, their submission or use is banned, except for those notes that can be used as evidence in the procedure under special conditions and when having a higher social interest.

The right protects the secrecy of the act of communication itself, while the content of the communication is irrelevant. The scope of the right in case of verbal communication protects the secrecy of the uttered words from the moment when the verbal contact began, through the entire course of the conversation until its conclusion. Article 8 of the ECHR protects the secrecy of the direct spoken communication, as well as the secrecy of the verbal communication through the use of telephone devices (*Klass and others v. Germany; Margaret and Roger Andersson v. Sweden*). In case of spoken communication through mobile telephony, the protection of the secrecy refers both to the uttered words and the information on the location of the mobile units.

Moreover, the secrecy of communications through a public telephony system is protected, as well as communications through internal communication systems governed by the public authorities. For example, in *Halford v. United Kingdom*, the ECtHR found a breach of Article 8 of the ECHR because the interception of official and private communications of the applicant (police officer) within the internal communication system of the police did not comply with the existing regulations, and there was no other alternative regulation that would otherwise regulate the interception of communications beyond the public communication systems.

In case of written communication, the scope of the right extends to and protects the right to secrecy of sent and received letters and other correspondence. The right to secrecy should be respected from the time the channel (distributor of the content of the communication) receives the written material (notification, letter, congratulating note, document, e-mail etc.) from the sender, up to the moment when it is delivered to the individual to whom the content is intended. According to the ECtHR

stance, the right to secrecy encompasses the less used telegraph communication (*Guzzardi v. Italy*) and communication by pager (*Taylor-Sabori v. United Kingdom*), and the increasingly used electronic (e-mail) communication (*Copland v. United Kingdom*).

1.4. Personal data as an aspect of privacy

The contemporary treatment of the right to privacy, especially in the European countries, acquires a broader dimension through the treatment of personal data as a separate aspect of privacy, even as a separate new right arising from the right to privacy. Personal data represent a key segment of privacy of each individual, especially today, when social activities in all spheres are operating on the basis of high-capacity databases. Personal data can be used in establishing the identity of an individual or different aspects of an individual's identity (physical, physiological, mental, economic, cultural or social).

For data to be personal, the information must refer to a specific individual, i.e. must be "about" the individual. Any type of information can be personal data, including audio, video and genetic data, fingerprints etc. (*Gunderman, 2010, p.10*). Linking the theme of information security and personal data protection has resulted in the establishment of a new sphere of privacy or e-privacy. The issues of e-privacy are most commonly linked to e-mail and personal data protection collected through computer network stations (*Boban, 2012, p.587*). Therefore, the progress of technologies imposes an obligation on contemporary legislative systems to continually redesign the personal data protection by following the pace of that progress.

Processing of personal data related to crimes, fines, alternative measures and security measures should, as a sensitive topic, be reviewed both from the perspective of the offenders, whose identity must be protected at least by the end of the appeals procedure, and the victims' perspective. According to *Gunderman*, this means that the name of the suspect will not be released, and in case of a recording the face of the suspect will be blurred, whereas the police authorities will carefully assess the amount of information to be released to the public, for the purpose of protecting the identity of the defendant. From the victims' perspective, their personal data should be treated with utmost respect for their privacy and should be kept confidential unless they wish otherwise (*Gunderman, 2010, p.35-37*).

The system of principles and safeguards of privacy through personal data protection in the European countries has been established by series of international documents. The 1981 Council of Europe **Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data (CETS No.108)** is the first and fundamental binding international document that was adopted in order to ensure the respect of fundamental freedoms and rights, especially the right to privacy, the automatic processing of personal data, for every single individual in the Convention signatory-states. In this context, the 2000 **European Union Charter of Fundamental Rights** is also significant, explicitly identifying the right to protect personal data in Article 8, right after Article 7 that refers to the protection of personal and family life, home and communications.

The European Union legal framework for personal data protection was consolidated by several legal acts and documents adopted in April 2016 and their implementation begun two years later, in 2018. The most significant documents are **Regulation (2016/679) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data** and **Directive (2016/680) 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**. Regulation 2016/679 repeals all national laws and Directive (EU) 95/46/CE on the protec-

tion of individuals with regard to the processing of personal data and on the free movement of such data, as the basic and comprehensive document that hitherto regulated the protection and transfer of personal data within the EU.

The new EU rules establish a single pan-European legislation for personal data protection, instead of the current inconsistent collection of national laws. In fact, this is considered as one of the largest benefits of the reform package. This is the “One Continent, One Law” principle that is set to enable equal treatment of personal data of individuals and use of identical rules for data protection in all EU member-states.

Amongst other, the reform package confirms, and through certain mechanisms, even enhances the basic principles of data processing:

- **legality;**
- **fairness and transparency;**
- **limited purpose;**
- **data minimization;**
- **accuracy;**
- **limited storage;**
- **integrity and confidentiality;**
- **responsibility.**

2. Right to privacy versus the need for efficient measures in the interest of security and fight against crime

The seriousness of global threats, primarily perceived in organized crime and terrorism, and especially their transnational forms, has faced the international community with the need to find alternatives for more efficient ways to manage them. In the efforts to find an efficient system of measures and actions, not only to detect crime, but also to prevent it, the democratic community has again been faced with the serious challenge of creating a fair balance between:

- The use of intrusive investigative measures as an adequate instrument to achieve greater efficiency of the criminal legislation; and
- The protection of the set of human rights and freedoms from excessive violation and threats when achieving the initial objective.

In such circumstances, the enactment of intrusive investigative measures and techniques for evidence collection has been imposed as a forced response to the rising threat of severe forms of crime. On the other hand, the use of new “unconventional” measures in the fight against national and global threats to security resulted in regression from some of the traditionally protected human rights, especially the right to privacy in all of its aspects (secrecy of communications, personal data, privacy of the home etc.).

Considering the above, there is an evident overlapping between security as a public interest and privacy as a personal right. This overlapping often imposes the need to *a priori* restrict privacy for the purpose of protecting national and public security. National and public security is undoubtedly the highest priority of every country. However, it also goes without saying that security cannot be achieved by violating individual rights and freedoms. Therefore, there needs to be a fair balance and proportional relationship between the common interest for protection of security and the interest of individuals to maintain privacy. Concessions from the individual interest to protect privacy can be made only if assessed as the only way to protect a higher state interest. The assessment should not be general.

The necessity to intrude into individual privacy must be carefully considered in each individual case and in the context of all circumstances of the case. Otherwise, this intrusion will be seen as *a priori* underestimation of privacy before the interest of protecting security.

The safeguards in the contemporary penal procedure have already reached the level of universal standards, which would be difficult to reverse considering their civilizational achievements (*Kambovski, 2005, p.382*). Every response to crime must confirm the fundamental principles of democratic states through the rule of law and the observance of human rights (*CoE, Rec. 1996*).

3. Legitimate restriction of the right to privacy

Article 8 of the **European Convention on Human Rights** guarantees the right to respect privacy by establishing the following:

Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is *in accordance with the law* and is necessary in a democratic society *in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

Article 8 Paragraph (1) of the ECHR establishes the scope of privacy and the spheres of protection, while Paragraph (2) includes a guarantee on the non-interference of the public authorities in the privacy right, but also the conditions and type of state interests because of which this right can still be restricted. Namely, the privacy right is not absolute and this right can generally be restricted at the expense of some other higher social interests or at the expense of other rights of the individuals. Thus, the state can legitimately violate the general right to privacy of the individual under certain circumstances (“in accordance with the law” and “necessary in a democratic society”) if this is “in the interest of national security, public safety or economic well-being of the country”, or for the purpose of preventing a crime (“for the prevention of disorder or crimes”), “for the protection of health or morals, or for the protection of the rights and freedoms of others.”

The above mentioned state interests as grounds for legitimate restriction of the right to privacy of the individual are only seemingly precise. These are the interests of national and public security, economic well-being, prevention of disorder and crime, protection of the health or protection of the rights and freedoms of other people, as well as protection of the morals. In practice, states most often call on national security or the prevention of crime, as higher state interests that need to be protected, while least on the protection of the economic well-being or health of their citizens. With regards to the protection of the morals as a high state interest, standards of what is moral and what’s not differ among countries and even within a country. In each specific case, the discretion right of the country to intrude in the privacy of the individual depends on the context of the specific circumstances, as well as on the existence of different customs, policies and practice in different countries. When assessing the necessity of such intrusion in the private life of the person concerned, states apply the doctrine of “margin of appreciation”.

Margin of appreciation (or **margin of state discretion**) is a doctrine with a wide scope of application in international human rights law. The doctrine was developed by the ECtHR as a guide of the ECtHR jurisprudence in judging whether a state party to the ECHR should be sanctioned for limiting the enjoyment of citizens' rights protected by the ECHR. The doctrine allows the Court to reconcile any practical differences in implementing the articles of the Convention, thus creating a limited right, for Contracting Parties, "to derogate from the obligations laid down in the Convention".

The doctrine also reinforces the role of the ECHR as a supervisory framework for protection of human rights and freedoms. In applying this discretion, ECtHR judges must take into account the differences between domestic laws of the Contracting States as they relate to substance and procedure. The margin of appreciation doctrine contains concepts that are analogous to the principle of subsidiarity, which occurs in the unrelated field of European Union law. The purpose of the margin of appreciation is to balance individual rights with national interests, as well as to resolve any potential conflicts. Still, this doctrine does not give states unlimited power of judgment, because it is indisputable that the "domestic margin of appreciation goes 'hand in hand' with European supervision" (*Kilkelly, 2001, p.7*).

ECtHR case law shows that the necessity principle is mostly used as discretion right of national courts when assessing whether the deviation from the right to privacy in the specific circumstances is legitimate. The discretion right of the court is to assess the necessity considering the specifics of the concrete case, as well as in the context of the safety and security environment in the country, but also the necessity from the aspect of moral values, customary norms, political and other circumstances.

4. International principles and standards for the implementation of measures for interception of communications

4.1. International principles

Intrusive investigative measures (the Macedonian legislation refers to them as special investigative measures - SIMs) undoubtedly represent a serious threat to the set of individual rights and freedoms of citizens, considering the aggressive and strong penetrating power in the sphere of an individual's private life. However, they are the inevitable and lesser evil than the one of organized crime and terrorism.

The Conclusions of the Resolution from the XVIth International Congress of Penal Law, Budapest, 5-11 September 1999, Section III, p.10 are of exceptional significance for the regulation, practical implementation and validation of the obtained knowledge from the implementation of these measures. The Resolution recommends that intrusive methods and techniques can be used if:

- the use of such measures is legally regulated (**legality principle**);
- there are no less restrictive legal means to accomplish the same objective (**subsidiarity principle**);
- the measures are applied only for severe crimes (**proportionality principle**); and
- there is prior authorization from the court, i.e. they are applied under its supervision (**principle of judicial approval of intrusive measures**)

The listed principles and the adopted standards related to the use of these principles are validated and upgraded by other acts of relevant international organizations, such as the United Nations,

Council of Europe and the European Court of Human Rights case law. In establishing the standards and principles, these organizations insist on ensuring balanced actions by competent authorities in the use of intrusive measures versus the need to observe basic human rights and fundamental freedoms. The creation of standards is a process that is continually advanced and upgraded.

Equally significant are the international UN conventions that were subsequently adopted (*UN Convention against transnational organized crime, 2000, Article 20; UN Convention against corruption, 2003, Article 50*), the established standards by the Council of Europe on the use of intrusive measures (through its bodies - Committee of Ministers, Venice Commission, Parliamentary Assembly, Commissioner for Human Rights and Committee on Legal Affairs and Human Rights), recommendations by the Committee of Ministers to the Council of Europe member-states (*CoE, Rec. (1996)8; CoE, Rec. (2001)11; CoE, Rec. (2005)10*) etc.

4.1.1. Legality principle

The legality principle imposes an obligation of the state to precisely regulate the procedure, criteria and other circumstances related to the use of the intrusive measures, for the purpose of avoiding arbitrary discretion of the state.

The provision of Article 8 Paragraph (2) of the ECHR allows for the state to breach the general right to privacy of the individual given in Paragraph (1) of the same Article, if two conditions are cumulatively met: "in accordance with the law" and "necessary in a democratic society". The requirement "in accordance with the law" represents an explicit requirement and promotion of the legality principle. In other words, measures must be legally prescribed and the law must specifically define the circle, i.e. the category of persons that could be the object of the measures' use, the type of crimes for which their application is allowed, their duration which must be reasonably acceptable, the manner of the measures' implementation and the manner of conducting an inspection and oversight of their implementation, the regime of use and storage of obtained recordings from the measures' application and other circumstances that are important for their application, but at the same time are reflected on the freedoms and rights of the individual.

In fact, such a requirement directly touches upon the principle of legal certainty of citizens, which is the foundation of the concept of the rule of law, i.e. lawful state. The existence of this principle ensures protection from legal uncertainty and lack of fairness when implementing the law, at the same time ensuring that the state practices its authority in accordance with the prescribed regulations.

4.1.2. Subsidiarity principle

The subsidiarity principle imposes an obligation for exceptional use of intrusive measures and succession in the delivery of the measures - from less to more intrusive - i.e. mandatory use of less intrusive investigative measures if they can achieve the legitimate aim.

The subsidiarity principle incorporates two cumulatively binding elements:

- first, the state primarily uses conventional operational measures and uses intrusive investigative measures only as a last resort; and
- second, if the state uses these measures, it must observe the succession in the selection of measures from less intrusive to more intrusive.

The use of these intrusive measures is *ultima ratio*, i.e. last resort of the state in its efforts to improve the efficiency of the criminal legislation. In other words, any intrusion in the individual's private life shall not be in accordance with the subsidiarity principle if the state had other alternative meas-

ures at its disposal, without or having less intrusive character and which use could have achieved the same legitimate objective.

The subsidiarity principle logically incorporates the ban for measures to turn into a method of collecting indications. Intrusive investigative measures are the last resort in the system of measures for prevention and detection of crime, which the state surely uses because of the impossibility for the crime to be investigated by other alternative measures, at the same time having an urgent need to protect a certain common good.

Their use is the last instance undertaken by the community in an attempt to protect the vital interests of the society. Their approval requires the existence of certain facts or prior knowledge that a crime has been committed or is to be committed. The increasing use without observing the subsidiarity principle, namely the *ultima ratio* rule, creates psychosis and persuasion (features of police organizations) that “technical means can ensure access to the crime scene even before the arrival of the perpetrator of the crime”.

4.1.3. Proportionality principle

The proportionality principle incorporates the proportion in the use of intrusive investigative measures, between the value of the social interest being protected and the degree of intrusion in the private life of the individual when achieving that protection.

In fact, the proportionality principle means finding the right balance between the protection of individual rights on one hand, and the interests of the society as a whole on the other. This balance can be achieved only if the restrictions of the individual’s rights referred to in Article 8 Paragraph (1) of the ECHR are proportionate to the legitimate goal. The proportionality principle requires balancing between the degree and intensity of the intrusion in the right to privacy of the individual and the specific benefit of the undertaken investigation.

Moreover, considering the intrusive nature of the measures, proportionality should exist between the goal to be achieved and the means used for that purpose, versus the general interests of the community and the protection of the individual’s rights. Although the proportionality principle, similar to the subsidiarity principle, is not explicitly listed in Article 8 Paragraph (2) of the ECHR, it plays a key role in the ECtHR case law.

4.1.4. Principle of judicial approval of intrusive measures

The core significance of the principle of judicial approval is that the use of intrusive measures should undergo prior approval by a court, i.e. their use should be under the court’s oversight and control.

The principle of judicial approval establishes a legal obligation of authorized institutions to ask for prior approval from the judiciary for each planned use of intrusive measures. The sense of this, in a way, subordinated position of the executive branch of government versus the judiciary, is necessary in a democratic society and represents a safeguard of the human rights and fundamental freedoms of the individual from their excessive breach when applying the measures.

Moreover, it is desirable that the procedure of proposing these measures incorporates an independent external institution, beyond the scope of the executive, which would realistically and impartially assess the necessity to apply intrusive measures in every individual case, completely “unburdened” by the urge to increase the efficiency of the criminal persecution. Therefore, the judiciary is the suitable and desirable external impartial party, because besides its independence, professional competence and position, it is functionally interested in the legality and efficient use of the meas-

ures, since the court is, eventually, the instance using the collected evidence and data from the measures' application when administering justice.

The objective of this principle is to ensure respect of the legal authority and restrictions in the use of the measures by authorized institutions, for the purpose of preventing their abuse and excessive use. In other words, one needs to impose the observance of the rule that these measures are the last resort of the state in its efforts to improve and increase the efficiency of penal justice.

The principle of judicial approval represents a professional and in-depth oversight and control in an exceptionally important and crucial stage in the procedure of applying the measures, i.e. the stage in which the criminal prosecution bodies reached a final decision to apply the measures and therefore require approval. The application by the authorized petitioner should list all circumstances and facts pointing to the fact that the case cannot be treated otherwise, and there is a pressing need for reaction by the state for the purpose of protecting a certain good or common value.

Therefore, this symbolically called approbate judicial oversight and control of the intrusive measures is of key importance because it is the essential, final, external, professional oversight and control of whether to approve the intrusion in the sphere of an individual's private life, while all other further forms of oversight and control refer to stages in which the use of the measures has already started (current oversight and control) or has already been completed (*ex post* oversight and control).

This oversight and control in this stage, by its content, overlaps with the so-called *ex ante* control of the court over the use of the measures, representing an integral part of the court's procedure when deciding on an application for the measures' application. In this procedure, the court assesses the facts, evidence, knowledge and data in the application, and passes a meritorious decision on the approval of the measures. The approbate oversight and control, i.e. *ex ante* judicial control in this stage establishes if the criminal prosecution bodies had observed the principles of legality, subsidiarity and proportionality in proposing the intrusive measures, but also establishes the expediency and prudence in the planning and realization of the projected objectives of the institutions charged with the measures' application, i.e. their efficiency.

A significant legal instrument of controlling the judicial (and prosecutorial) authorities in the stage of the measures' approval, but also in the course of their implementation, in preventing the emergence of mass interception of communications is the provision of Article 68, paragraph (6) of the Law on Interception of Communications, which imposes the obligation of operators to ensure unambiguousness in the interception of communications.

In other words, the court has the legal option of not approving the use of the measures for interception of communications or terminating their use, although all legal conditions for their use are met, if the operators do not possess the technical equipment that can ensure and guarantee unambiguousness in the interception of communications. The unambiguousness relates both to the subject whose communication is intercepted and the content that is intercepted, thus legally banning the interception of other persons' communications (undetermined and unlimited number) who are not encompassed with the court order, as well as content other than the one indicated in the order. Any failure to observe the abovementioned obligation shall result solely in a fine imposed on the operators.

This approbate judicial oversight and control on the use of the intrusive measures should not be compared to the classical oversight and control of the use of intrusive measures by the courts because:

- the appropriate judicial approval and control is implemented prior to the use of the intrusive investigative measures, unlike the classical oversight and control, which is implemented either continually or *ex post*;
- the purpose of the judicial approval is to give consent on the use of the measures, while the classical court oversight and control aims to observe the legality principle over the use of the intrusive measures;
- having in mind the appropriate judicial approval's crucial and exceptional importance, it is "exempted" from the classical oversight and control and seen as an independent principle in the procedure of using intrusive measures, whereas the classical oversight and control on the use of the intrusive investigative measures is an integral part of the legality principle; and
- although an *ex ante* judicial oversight and control by its content, the judicial approval is, considering its functionality, a part of the judicial decision-making procedure on the application for use of intrusive investigative measures.

4.2. International standards

4.2.1. Standards related to the legality principle

The ECtHR concludes that intrusive measures represent a necessary instrument for the law enforcement authorities in contemporary democratic societies, as an adequate means for prevention of crime, but if their use is not legally regulated, there is a threat of undermining or even destroying democracy under the justification of its defense (*Klass v. Germany*).

The ECtHR case law defines the term "law" as any legal framework of the domicile state that regulates the use of intrusive measures. In this regard, if the state does not have a legal framework, this is also a breach of Article 8 of the ECHR. The ECtHR does not insist that the legal framework is in the form of a legal act - law, but requires a legislative act that has legal weight (*De Wideandau. v. Belgium*).

Besides the formal aspect of the legal framework, certain content features that the law needs to meet are insisted upon, relating to precision, clarity and distinctness of norms, enabling citizens to predict, to a certain reasonable degree, when their private life can be breached (*Sunday Times v. UK*). Any protection from abuse of intrusive measures must involve accessible and precise provisions that regulate the authorization for surveillance. (*Malone v. UK*).

The rules must be in a form that is legally binding and must be accessible to the public (*Hewitt and Harman v. UK*). The rules must define the categories of people that are targets of surveillance, the types of crimes that justify the investigation, the acceptable period of surveillance and the circumstances under which any recording shall be kept in a case file by the state (*Huvig v. France*). The rules must also define the volume and manner in which the surveillance is carried out in practice (*Kopp v. Switzerland; Taylor-Sabori v. UK*).

In the context of the above stated and in accordance with the judicial interpretation of the ECtHR, the law should be sufficiently accessible for the citizens, so that they are acquainted with the possibility of their individual rights and freedoms being in jeopardy. On the other hand, this does not mean that the law should create a possibility for citizens to predict in advance that they are subject of certain special measures, because this would disrupt the efficiency of the criminal prosecution and the state would disarm itself. The law provisions should also be precise and unambiguous so that citizens can align their conduct with the law. However, the requirement for the law's precision is not threatened if certain provisions may be interpreted in several ways (*Castells v. Spain*).

4.2.2. Standards related to the subsidiarity principle

The subsidiarity principle is not explicitly listed in Article 8 Paragraph (2) of the ECHR as is the legality principle, but it is incorporated in the content and it is implied in the meaning of the used term “necessary”. When presenting its opinion over the meaning of the term “necessary”, the ECtHR concludes in the case *Campbell v. UK* that “any intrusion in the private life of the individual shall not be considered necessary, if the state had other alternative measures at disposal, which application could result in the same objective.”

The subsidiarity principle means succession in the use of intrusive measures, in the sense that all other means at the state’s disposal should be utilized, whereas intrusive measures should be used only as means of last resort. When implementing the subsidiarity principle, it is of exceptional importance to build procedural safeguards when proposing measures in the institutions that have the jurisdiction to apply them. Namely, the multilayered control of the procedure of proposing these measures in the authorized institutions, creates certain guarantees that they will not be abused, turning them into a routine method of collecting indications.

Some of the requirements for a quality law, although referring to the legality principle, are of exceptional importance also for realization of the subsidiarity principle. Therefore, the requirements for procedural safeguards and reduction of the state’s discretion have a direct effect in establishing safeguards that the intrusive measures shall not be applied arbitrarily.

While these rules do not have to incorporate comprehensive definitions (*Hewitt and Herman v. UK*), they cannot simply leave the decision to whether the surveillance shall occur at the free discretion of the executive or the court (*Valenzuela Contreras v. Spain*).

Moreover, the legislation should be accompanied by appropriate procedural safeguards from the arbitrary discretion right of the executive over the measures’ application (*Huvig v. France*). If the state has some discretion rights, which cannot be understandably eliminated, it is obliged to highlight the volume of this discretion with sufficient clarity (*Silver v. UK; Leander v. Sweden*), in order to achieve fairness in the proceedings. In addition, the state should reduce any discretion rights to the minimum. (*Sunday Times v. UK*).

4.2.3. Standards related to the proportionality principle

The proportionality principle, similarly to the subsidiarity principle, is not explicitly implied in Article 8 Paragraph (2) of the ECHR, but the used term “necessary” incorporates both principles. Namely, the ECtHR has presented its opinion on numerous occasions over the significance of the term “necessary”, noting in *Sunday Times v. UK* that the “Phrase ‘necessary in a democratic society’ implies that interference in the individual’s private life is a response to a pressing social need, and it is not sufficient that such interference is not only desirable and reasonable, but the state should also demonstrate the existence of a proportionality relationship between the purpose and the means”.

The “proportionality” term implies two aspects (*James v. UK*):

- proportionality between the means employed and the aim sought to be realized;
- proportionality or fair balance between the demands of the general interest of the community and the requirements of the protection of the individual’s fundamental rights.

When determining proportionality, it is considered whether a certain interference in the people’s private life is too aggressive or imposes a large burden for certain individuals, and also if the community interest justifies this. In addition, the state must demonstrate that the interference in the private life of the individual was not excessive.

In this context, it is implied that when the interference in the private life of the individual is aggressive or the information collected by the state is especially sensitive (for example, secret surveillance of persons with special functions and duties such as: judges, politicians, religious leaders etc.), the state's justification should be backed by strong arguments (*Kopp v. Switzerland*).

The state needs to secure clear evidence on the necessity of the use of intrusive measures and build a legal framework that ensures proper and efficient protection from abuse. In this regard, it is argued that different investigative techniques such as surveillance of telephone calls and mail (*Kopp v. Switzerland*), processing of phone calls, i.e. identification of incoming and outgoing numbers (*PG v. UK*), pager surveillance (*Taylor Sabori v. UK*), use of secret tapping devices (*Khan v. UK*) and video surveillance (*Govell v. UK*) are *prima facie* breaches of the right to privacy and require justifications in accordance with Article 8 Paragraph (2) of the ECHR.

All other investigative techniques used for surveillance in police stations, business premises and homes have the same treatment. Moreover, cases where surveillance is done by a person not belonging to the police structures, but did that upon request, at the advice, or with the assistance of the police also have this treatment (*Halford v. UK*). However, the ECtHR notes there is no breach of Article 8 of the Convention in all those investigative techniques where surveillance or recording of a certain person is done in a public place, under circumstances in which the person has no reasonable or justified expectation about privacy (*PG v. UK*). In correcting this viewpoint, it is argued that if the collected information is systematized in a continual recording, Article 8 of the ECHR could be applied (*PG v. UK*), as would be the judgment in situations when information regarding the public is collected and analyzed, irrespective of the use of any of the special investigative measures (*Rotary v. UK*).

Secret or undercover operations can, in certain cases, lead to breaches of Article 8 of the ECHR. Namely, considering the dominant perception of the term "private life", both with the use of undercover agents and secret cooperation, it can be concluded that the right to free development of relations among people is compromised and the reasonable expectation of privacy in communication is violated. In other words, there is a violation of the right of the individual to communicate freely without fearing that the communication involves secret agents or informants.

On the other hand, the suspect is not aware that he/she is subject to special surveillance by the state, nor is informed about the right to silence, i.e. refusing to give statements that could incriminate him/her or a person close to him/her. Therefore, there are increasing considerations and expectations that the ECtHR shall classify, in the near future, secret operations and secret cooperation as *prima facie* intrusion in the right to privacy of citizens and consequently ask for strict regulations in accordance with Article 8 of the ECHR.

In the context of the above mentioned, the ECtHR distinguishes the police actions that represent cunning but not unlawful method to collect evidence (*A v. Germany*) and in the same case elaborates that such procedures do not represent a breach of Article 6 of the ECHR, if the contested evidence is supported by other evidence and the person's free will has not been violated by the police.

Regarding the use of undercover agents, the ECtHR explicitly argues that it is unlawful to incite or entice a perpetration of a crime, and any evidence collected in such a way shall constitute a breach of Article 6 of the ECHR. In other words, the state allows but also cannot and should not ban even the most hideous criminal thought in the mind of an individual, but should in no way allow a person, and least itself, to contribute to the realization of the criminal intent of a person. In case *Teixeira de Castro v. Portugal*, the ECtHR argues that "the use of undercover agents must be restricted and safeguards put in place even in cases concerning the fight against drug trafficking. While the rise in organized crime undoubtedly requires that appropriate measures be taken, the right to a fair administration of

justice nevertheless holds such a prominent place that it cannot be sacrificed for the sake of expedience. The general requirements of fairness embodied in Article 6, apply to proceedings concerning all types of criminal offences, from the most straightforward to the most complex. The public interest cannot justify the use of evidence obtained as a result of police incitement.”

On the issue of using informants as evidence in the procedure, when they had been involved in the perpetration of a crime (this person is attributed with different synonyms: witness accomplice in a crime, repentant witness, collaborating witness, collaborators of justice etc.), the court recommends caution regarding evidence obtained from them, arguing that there is no violation of Article 6 of the ECHR if the informant is discredited through cross examination in the procedure and if the testimony of the informant is not the only evidence (*Charlene Webb v. UK; Baragiola v. Switzerland*).

4.2.4. Standards related to the principle of court approval of intrusive measures

Regarding the prior consent for use of the measures and the permanent oversight and control of the measures, the ECtHR notes that the rules must regulate the circumstances in which the intrusive surveillance is allowed (*Kruslin v. France*) and must contain a proper and efficient protection from abuse, ensuring that the intrusive surveillance is not ordered by coincidence and without the proper attention (*Klass v. Germany*).

The rules must highlight the volume and manner in which the surveillance is to be carried out in practice (*Kopp v. Switzerland*) and there must be proper methods of accountability for the authorization of the surveillance, its control and oversight. The court might not be entrusted with this oversight (*Klass v. Germany*), although it is desirable and even important (*Kopp v. Switzerland*), but it must be entrusted to an independent and capable institution for the purpose of continual control.

One of the democratic forms of public oversight and control is the notification of the person concerned in case the measures have been suspended. This right of the individual can be taken from the German constitutional principle on information self-determination. The ECtHR argues that “the person concerned may be informed after the termination of the surveillance measures, although there is no rule saying that such information is necessary” (*Klass v. Germany*).

The ECtHR does not pretend to create an obligation for the state to always inform citizens on the use of the measures. Namely, in case the collected evidence from the application of the measures is used as evidence in a criminal procedure, the targeted persons concerned shall be informed, while in cases when the measures had been suspended, the court claims that after the surveillance is terminated, it might be necessary to inform the subject under surveillance “but this is not required when such information is not practical or could undermine the efficiency of the operation” (*Klass v. Germany*).

5. Cases of secret surveillance

With regards to the legality principle, in *Khan v. UK*, the ECtHR rejected the applicant’s complaint that the judgment of the national court based on unlawfully obtained evidence is a breach of Article 6 of the ECHR, reasoning that acceptance of unlawfully obtained evidence from the national court was due to the nature of the unlawfulness. Namely, the ECtHR considered that the disputed recording had been made using guidelines from the authorities, and the only cause for violation of Article 8 of the ECHR is that they had not been prescribed by law. However, the ECtHR also argues that the incriminating statements in the recording were given voluntarily and without incitement, whereas the recording is solid and valid evidence. The applicant had the opportunity to challenge the recording’s authenticity

and the fairness of the recording being used as evidence before the national court. Therefore, the court established that the trial and the judgment before the national court, although constituting a violation of Article 8 of the ECHR, is not a violation of Article 6 of the Convention as a whole.

In fact, although seemingly contradictory, the ECtHR and the UK case law argue that fairness and truth precede the legality principle when the breach is of technical nature. In other words, the court procedure shall not be considered unfair by the sole acceptance of an unlawfully obtained evidence *per se*, but requires the establishment of certain circumstances – whether the evidence is valid and given voluntarily, whether the defendant had the opportunity to challenge its presentation in the procedure and above all, what is the nature of the violation of the legality when obtaining the disputed evidence, i.e. whether the violation is of technical nature or there is a case of abuse of jurisdiction on the part of the criminal prosecution authorities.

In the case of *Allan v. UK*, the appellant had been suspected of taking part in a murder, arrested and informed of his right to silence, a right that he used. The police attempted on several occasions to interrogate him in the presence of a defense attorney but to no avail. Lacking sufficient evidence, the police wired his cell and the visiting area, justifying these methods by saying that all other investigative methods had failed. In addition, the police infiltrated a police informant in the same cell, who was supposed to entice the suspect into talking about the event. In this case, similarly as in other cases versus Great Britain, the ECtHR established violation of the right to privacy of Article 8, because the audio and video recording was carried out without the existence of a defined legal framework.

However, regardless of this fact, the legal dilemmas considered by the court referred to the issue whether the recordings in question could be used in the criminal procedure without violating Article 6 of the ECHR – the right to a fair trial. The court said that the decision on the issue would depend on numerous circumstances in the case, and especially on the type of illegitimacy. Namely, as in the case of *Khan v. UK*, the court says that the judicial procedure shall not be considered unfair by the acceptance of the unlawfully obtained evidence *per se*, but requires the establishment of other circumstances related to the validity of the evidence, whether it was given voluntarily, whether the defendant had the opportunity to challenge its presentation in the procedure, and above all, what is the nature of the violation of the legality when obtaining the disputed evidence.

The court found an obvious problem with the use of an informant as a witness, looking at this problem from the aspect of the right to silence and the privilege against self-accusation. The court derives these rights from the concept of fair trial, although not clearly stated in the ECHR, as important implicit safeguards. According to the ECtHR, the purpose of these principles is to protect the freedom of the suspects, to choose by themselves whether they would speak or remain silent during the interrogation by the police or other competent authorities. This freedom was denied in this case by the very fact that despite the persistent refusal of the suspect to respond to any question, the authorities used deceit to force a confession. The statements by the defendant were not spontaneous, but in a way coerced from the persistent inquiry by the witness (informant), which according to the ECtHR was very similar to a police interrogation, but without the guarantees that any formal police interrogation carries within. In this sense, the defendant did not get the necessary guarantees such as the presence of a defense attorney, information about his rights etc. Therefore, the Court concluded that the evidence obtained in this way was essentially not given voluntarily, thus violating the defendant's right to silence and the privilege against self-accusation.

In *Doerga v. The Netherlands*, regarding the quality of the law, the ECtHR found that the wiretapping was conducted based on rules that lacked both clarity and detail and gave no precise indications as to the circumstances in which prisoners' conversations could be monitored, recorded or retained by peni-

tentiary authorities, underlining that the law must indicate the competence of the authority that issues the intrusive measures, give precise details over their duration and the manner of implementation, for the purpose of ensuring protection of the persons concerned from arbitrary actions. A quality law provides adequate conditions for storage of materials from surveillance of communications, identifying situations when the recorded communications can or must be erased or destroyed, as well as the manner and procedure of their erasure or destruction. In the same case, ECtHR did not agree with the interpretation of the Supreme Court of the Netherlands that the established obligation to erase the conversations of inmates, which the penitentiary authorities had recorded, means that conversations should, in fact, be “immediately erased after the head of the institution’s security service listens to them”. According to the ECtHR, those conversations should be erased “as soon as the danger which gave rise to their recording ceased to exist.” Regarding the adequate storage of the recorded materials, the ECtHR found in the case of *Craxi v. Italy* that after the transcripts of the recorded interceptions were filed in the register, the authorities did not undertake the proper measures for their safekeeping, because parts of the recordings (some of which were private) were released by the media.

ECtHR’s opinion in the case *Dragojevic v. Croatia* refers to the subsidiarity principle. Namely, the applicant was suspected of involvement in an international drug-trafficking scheme. At the request of the public prosecutor’s office, an investigating judge authorized the use of secret surveillance measures to covertly monitor the applicant’s telephone. In 2009, the applicant was found guilty of drug trafficking and money laundering and sentenced to nine years imprisonment. The Supreme Court upheld his conviction in 2010, and his constitutional complaint was dismissed in 2011.

Upon reviewing the application, the ECtHR concluded that the wiretapping of the applicant’s phone constituted a breach in his right to respect private life and correspondence. Based on the domestic law, the use of secret surveillance is subject to prior authorization. However, in the case of the applicant, the orders issued by the investigating judge were based only on a statement referring to the requests by the public prosecutor’s office and the assertion that “the investigation could not be conducted by other means,” without any information as to whether less intrusive means were available. The investigating judge’s approach was endorsed both by the Supreme Court and the Constitutional Court. In an area as sensitive as the use of secret surveillance, the ECtHR had difficulties accepting such an interpretation of the domestic law, which envisaged and required prior detailed judicial scrutiny of the proportionality of the use of secret surveillance measures to the offense alleged. The domestic courts’ circumvention of this requirement by retrospective justification opened the door to arbitrariness and did not provide adequate and sufficient safeguards against potential abuse.

In the applicant’s case, the criminal courts had limited their assessment of the use of secret surveillance to the extent relevant to the admissibility of the evidence thus obtained, without going into the substance of the ECHR’s requirements concerning the allegations of arbitrary interference with a person’s Article 8 rights. The government did not provide any information on remedies that could be available to a person in the applicant’s situation. Therefore, the relevant domestic law, as interpreted and applied by the domestic courts, was not sufficiently clear regarding the scope and manner of exercise of the discretion conferred on the public authorities, and it did not secure adequate safeguards against possible abuse. Accordingly, the procedure for ordering and supervising the implementation of the interception of the applicant’s phone conversations did not comply with the legality requirements, nor was it adequate to keep interference with the applicant’s right to respect for his private life and correspondence to what was “necessary in a democratic society”. The ECtHR found (unanimously) that there is a breach of Article 8 of the ECHR, which refers to the violation of the subsidiarity principle when issuing intrusive measures, but did not find any violation of Article 6 Paragraph (1) of

the ECHR as regards the alleged lack of impartiality of the trial bench and the use of evidence obtained by secret surveillance.

In the case against Zeljko Sabo, mayor of Vukovar, the Supreme Court of Croatia accepted evidence obtained through secret surveillance but without a court order. The court found that the recording, although unlawful, can be used as legal evidence in the criminal procedure because of the prevailing public interest, contrary to the violation of the personal rights of the defendant guaranteed by the Constitution. The Supreme Court of Croatia based its decision on Article 10 Paragraph (3) of the Croatian LCP that regulates the relationship between the public interest and the individual's right to privacy.

In this case, the mayor was secretly recorded offering a bribe to Marija Budimir, city councilor and member of the HDZ political party, for her transfer to the group of independent councilors and support in establishing a majority in the city council. Sabo was sentenced to 16 months in prison, and the Supreme Court judgment was confirmed by the Constitutional Court upon the defendant's appeal.

In the case of *Roman Zakharov v. Russia*, the applicant was suing three mobile operators, claiming they had installed equipment which permitted the Federal Security Service (FSB) to intercept all telephone communications without prior judicial authorization. The ECtHR found that the domestic legal provisions did not provide for adequate and effective guarantees against arbitrariness. The ECtHR said that "since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."

The case of *Ramanauskas v. Lithuania* relates to inciting the perpetration of a crime while using special investigative measures. Namely, the applicant claimed that he had been approached by the person A.Z., whom he did not know, mediated by V.S., a personal acquaintance of the applicant. In this case, the court considered that the actions by the individuals had an effect of inciting the applicant to perpetrate the crime for which he was sentenced and there are no indications that the crime would have been committed without their intervention.

Unlike this case, *Shannon v. UK* is about accepting evidence that had been obtained through a "set-up" i.e. after a journalist set a trap. In this case, the ECtHR noted that the role of the state was restricted with regards to the indictment against the applicant, which was based on information given by a third person. The applicant was "set up" by a journalist, a natural person, who was not a state agent, did not proceed on behalf of the police, did not proceed by given instructions or guidelines from the police and was in no way under their control. The police did not have any prior information about the operation, but was given audio and video recordings after the event had already taken place. The ECtHR notes that the circumstances under which the evidence had been collected were initially assessed by a first-instance judge, with an emphasis on the context of their use regarding their inadmissibility, i.e. exclusion, based on the fact that they had been collected by setting a trap. In this case, the ECtHR concludes that the acceptance of the disputed evidence did not result in violation of Article 6 of the ECHR.



PART 2

SPECIAL INVESTIGATIVE MEASURES IN CRIMINAL PROCEDURE





1. Introduction

The legal basis for the use of special investigative measures was set by the adoption of Amendment XIX of the Constitution of the Republic of Macedonia in 2003, replacing Article 17 of the Constitution.

The freedom and inviolability of correspondence and other forms of communication is guaranteed. Only a court decision may, under conditions and in procedure prescribed by law, authorize non-application of the principle of inviolability of correspondence and other forms of communication, in cases if necessary, in preventing or detecting crime, for the purpose of a criminal investigation or when required by the interests of security and defense of the Republic.

Similar to Article 8 of the ECHR, the first paragraph of the amendment regulates the scope of the privacy that is protected (freedom and inviolability) and the spheres of protection (correspondence and other forms of communication) of the privacy of an individual. Unlike Article 8 of the ECHR, the sphere of protection of privacy is narrower and relates only to correspondence and other forms of communication, and not to the private and family life of the individual. This legal gap in the constitutional legal framework is completed by a direct application of the ECHR provisions (Article 8), which ratification makes it a direct source of law in the national legislation.

The second paragraph lists the four fundamental principles that determine the use of intrusive measures and the legitimate grounds for their use. The principle of judicial approval of the measures (“only based on a court decision”) and the legality principle (“under conditions and in procedure prescribed by law”) are explicitly listed, whereas the subsidiarity and proportionality principle, as in Article 8 of the ECHR, are contained in the meaning of the phrase necessary (“if necessary”).

Regarding the objectives, the Constitution has designated two segments of interests as legitimate grounds for use of intrusive measures:

- the first segment incorporates the use of intrusive measures for criminal purposes (“for the purpose of a criminal investigation”); and
- the second segment relates to the use of intrusive measures for the purpose of protecting national interests (“when required by the interests of security and defense of the Republic”).

Based on this, the amendments to the Law on Criminal Procedure were adopted in 2004, which promoted eight special investigative measures. A new law, the existing Law on Criminal Procedure was adopted in November 2010, which identified twelve special investigative measures. The procedure of surveillance and recording of telephone and other electronic communications, as one of the special investigative measures was regulated by the 2006 Law on Interception of Communications, which was significantly amended on two occasions, in 2008 and 2012. The new, currently applicable Law on Interception of Communications was adopted in 2018, while certain structural and technical aspects of the interception of communications are regulated in the Law on the Operational Technical Agency and the Law on Electronic Communications. The normative framework has been completed by the laws that establish the jurisdiction of the authorities charged with the interception of communications, such as the Law on Internal Affairs, Law on Police, Law on Defense, Law on the Public Prosecutor’s Office and the Law on the Customs Administration.

1.1. Types of special investigative measures in the national legislation

The types of special investigative measures are prescribed in Article 252 of the Law on Criminal Procedure:

1. Surveillance and recording of telephone and other electronic communications in a procedure defined by law (LIC).

The measure relates to telephone communications and all other types of electronic communications between people, which represent an integral part of the term private life, determined according to the legal understanding of the ECHR. This measure does not incorporate: direct communications (oral communications or so-called ambient surveillance) and letters and postal packages as an indirect form of communication.

This measure can be imposed through a special written order by a competent judge, upon a reasoned proposal by a public prosecutor that lists the reasons for the necessity of the measure. Regarding the use of this measure (as for all others), the legislator requires that two general criteria are met: the probability that its use will secure data and evidence for successful conduct of the criminal procedure and that evidence and data cannot be collected by other means.

2. Surveillance and recording in a home or enclosed space belonging to the home or office space designated as private or in a vehicle, and entry in such facilities in order to create the required conditions for interception of communications

This measure incorporates only direct communications (wiring of the room where the communication takes place, i.e. the so-called ambient surveillance) in the home of the individual, i.e. the area designated as private. *There is a specific restriction (Article 268 of the LCP) that the measure can be directed only to areas or vehicles belonging to the person suspected of a certain crime. Only by exception, the home of other persons can be a subject of the measure, but there needs to be a reasonable suspicion that the suspect resides in that home for the measure to be allowed. Otherwise, there is no ground for the preliminary procedure judge to allow this special investigative measure to be used in a home of a person not suspected of involvement in incriminating activities.*

Recording, in the sense of the meaning of the terms from Article 21 of the LCP, means video-audio or only video or only audio recording, depending on the assessment of the needs and requirements of a specific case. Considering there are other members of the family or household in the home of the suspect, it is compulsory to terminate the recording in case of statements or actions within the sphere of intimate private or family life or having no connection to the aim of the measure.

3. Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private

The aim of this measure is not only to register the outside developments of the observed facility (the most common understanding in the judicial-prosecutorial practice) and obtain information about the movement of the suspect, communication with certain individuals, presence in certain places, connection to certain items etc., but also the content of the communication of the person concerned. It relates to the direct verbal communications in a public space, and not telephone and other electronic communications incorporated by the measure referred to in item 1. The measure could be accompanied by physical surveillance of the person concerned, but there is almost no exception to the use of technical means for recording of all suspicious actions, activities, contacts and developments that could benefit the establishment and validation of the legally relevant facts - co-perpetrators, aides and abettors, items used for perpetrating the crime etc. The suspect can, by using this measure, be caught *in flagrante* during the perpetration of the crime. The recording could be video or video-audio.

4. Secret access and search of computer systems

The measure involves electronic surveillance that can easily turn into a complete oversight of the content of communications with the assistance of contemporary IT “tools”. This is like a search of one’s home, only done without the knowledge of the person concerned and relates to a smaller “space”. However, the effect on the individual’s private life is enormous. Contemporary IT devices and programmes are remarkable tools for secret intrusion in an individual’s “computer life”.

The measure is carried out with the help of special IT devices and procedures, undertaken by especially equipped departments within the competent authorities, whose aim is to covertly conduct a search of the data in the computer system of the person concerned. This measure is also known as online search, considering that the information and evidence is remotely collected, over the Internet, and with the help of special forensic computer programmes that are installed at the computer subject of the processing, enabling the search without the computer user knowing about it. The measure can be a one-off or used on a longer term, depending on its aim. Having in mind the degree of intrusion in the privacy of the person whose computer is subject to the measure, this special investigative measure can only be approved by a written order of a preliminary procedure judge upon a reasoned motion by a public prosecutor.

5. Automatic search and comparison of personal data

This measure is a so-called raster search. According to its content, it is an online comparison of personal data of citizens listed in the personal databases of private and state institutions that record personal data of citizens on diverse grounds. The measure does not relate to already recorded personal data at the disposal of security services.

6. Insight in telephone and other electronic communications

This measure could be seen as “surveillance” of the content of prior communication, corresponding (as does the measure of Secret access and search of computer systems) to the investigative measure ‘home search’, only carried out without the knowledge of the person concerned, relating to a smaller “space” and *post festum*, not in real-time (*online*). This measure uses the benefits of the electronic communications traffic, i.e. the option of storing (12 months according to the LEC) all activities (meta-data) of stakeholders in the electronic communications traffic in the form of electronic traces (logs).

Considering the implementation method (by Internet or by remote forensics software), it is very close to the measure of secret access and search of computer system, but affecting the personal data of the person concerned to a much lesser degree and it is also not carried out in real time. Therefore, access is provided into all telephone conversations over the Internet, as well as all forms of electronic communications (e-mail, Facebook, chat etc.).

The public prosecutor imposes this measure by a written order at the motion of the judicial police. If the public prosecutor needs data only for realized contacts (pen registers) in the communications traffic (without entering the content of the communications), a request could be filed to the operators of public communications instead of issuing an order for this special investigative measure. The operators are obliged to proceed upon the request (Article 287 Paragraph 8 of the LCP).

7. Simulated purchase of items

This measure is a form of using an undercover agent. From a criminal law standpoint, it is a fictitious participation of the undercover agent in a specific stage of the crime perpetration (only in purchasing and not in selling), in the capacity of a co-perpetrator of the crime. Its aim is to detect and prove crimes, especially in the field of illicit trade, through simulated purchase of items. This measure ensures information and evidence about persons involved in illicit production, distribution and trade with the items, their aides and abettors, the *modus operandi* of the crime etc. The measure is imposed by means of a written order by a public prosecutor.

8. Simulated offering and receiving bribes

This measure, like the previous one, is a form of using undercover agents. From a criminal law standpoint, it is fictitious participation of the undercover agent in a specific stage of the crime perpetration, in the capacity of a co-perpetrator of the crime. Its aim is to help detect and prove corruption-related crimes. An especially sensitive legal element of this measure is the “establishment” of the criminal intent of the person concerned before activating the measure. The measure is imposed by means of a written order by a public prosecutor.

9. Controlled delivery and transport of persons and objects

The measure entails secret observation, but in certain cases also a combination of the measures secret observation and undercover agent (if the transport involves “an infiltrator”). From a criminal law standpoint, it is a fictitious participation of the undercover agent in a specific stage of the crime perpetration, in the capacity of co-perpetrator or abettor of the crime. The measure is imposed by means of a written order by a public prosecutor.

10. Use of persons with secret identity for surveillance and collection of information or data

The measure is one of the forms of using an undercover agent. It incorporates all forms of fictitious participation of the undercover agent in any stage of the crime perpetration, but with a limited participation in the abetting of criminal activities for the purpose of collecting information and data. The measure is imposed by means of a written order by a public prosecutor.

The undercover agent is not allowed to take part in the process of creating the criminal intent of the crime perpetrator, but only to give focus on the already shaped criminal intent of the perpetrator. Otherwise, such actions by the undercover agent would be seen as actions taken by an agent provocateur, which are otherwise prohibited. These persons have a special regime of participation in the criminal procedure in the sense of being questioned as protected witnesses. The identity of the persons with a covert identity shall remain a secret (Article 270 of the LCP), i.e. their identity is classified (Article 259 Paragraph 4 of the LCP). The measure is imposed by means of a written order by a public prosecutor.

11. Opening a simulated bank account

This measure, like the previous one, is a form of the undercover agent measure. From a criminal law standpoint, it is a fictitious participation of the undercover agent in any stage of the crime perpetration (preparation, realization and post-crime). The aim of the measure is to help detect and prove crimes related to corruption and illicit monetary transactions for the purpose of distributing cash, movable property or real estate acquired through crime, i.e. originating from incriminating operations. The measure is imposed by means of a written order by a public prosecutor.

12. Simulated incorporation of legal entities or using existing legal entities for the purpose of data collection

The measure is one of the forms of using an undercover agent. From a criminal law standpoint, it is a fictitious participation of the undercover agent in any stage of the crime perpetration, but with limited (passive and observant) participation in the criminal activities (only abetting is allowed) for the purpose of collecting evidence and data. By content, it is a measure offering simulated business services or actions undertaken by undercover agents or other persons of confidence. The measure is imposed by means of a written order by a public prosecutor.

2. Crimes entailing the use of special investigative measures

Having in mind that the special investigative measures are perceived as measures that are justified only for the most severe crimes, a kind of “necessary evil”, one can understand the restrictive

approach by the legislator, who precisely regulated the criminal offences for which they can be used and the required conditions. Pursuant to Article 253 of the LCP these measures may be imposed when the following grounds for suspicion exist:

- 1) Crimes that are punishable by a prison sentence of at least four years and are prepared, currently committed or already committed by an organized group, gang or other criminal enterprise; or
- 2) Crimes listed in the Criminal Code, including Murder of Article 123, Kidnapping of Article 141, Mediation in prostitution of Article 191, Paragraphs 1, 3 and 4, Showing pornographic materials to a minor of Article 193, Production and distribution of child pornography of Article 193a, Enticing a child under the age of 14 into statutory rape or other sexual activities of Article 193b, Unauthorized production and distribution of narcotics, psychotropic substances and precursors of Article 215 Paragraphs 1 and 3, Damaging and unauthorized access to a computer system of Article 251 Paragraphs 4 and 6, Extortion of Article 258, Blackmail of Article 259 Paragraph 2, Appropriation of goods under temporary protection or cultural heritage or natural rarities of Article 265, Exporting goods under temporary protection or cultural heritage or natural rarities of Article 266 Paragraph 1, Transfer of ownership of cultural heritage of special importance to the state of Article 266a, Money laundering and other crime proceeds of Article 273 Paragraphs 1, 2 and 3 and Paragraphs 5, 6, 8 and 12, Trafficking of Article 278 Paragraphs 3 and 5, Customs fraud of Article 278a, Abuse of an official position and authority of Article 353, Embezzlement in service of Article 354, Defraud in service of Article 355, Helping oneself in service of Article 356, Receiving a bribe of Article 357 Paragraphs 1, 4, 5 and 6, Giving a bribe of Article 358 Paragraphs 1 and 4, Unlawful mediation of Article 359 Paragraph 6, Illegal influence on witnesses of Article 368a Paragraph 3, Criminal association of Article 394 Paragraph 3, Terrorist organization of Article 394a Paragraphs 1, 2 and 3, Terrorism of Article 394a and Financing of terrorism financing of Article 394c; or
- 3) Crimes against the state (Chapter XXVIII) and crimes against humanity and international law (Chapter XXXIV) of the Criminal Code.

Special investigative measures can be imposed on a person who committed one of the crimes listed above, a person that undertakes an action to commit any of the crimes listed above and also a person that is preparing the commitment of any of those crimes, when the preparatory activities are defined as punishable based on the Criminal Code provisions.

These measures can also be applied to a person who receives or forwards shipments from a suspect or when the suspect uses his means of communications.

2.1. Domestic case law examples

Supreme Court of RN Macedonia

Kezharovski case

Reg.no.14/2017 Supreme Court of RNM

Although the defense asked for the SIM orders to be presented as evidence and to allow the defense to inspect the orders, the court did not allow it. The first instance court reasoned this decision by the fact that the orders are official secrets and all court attendees did not possess an appropriate security certificate to access such type of classified information. On the other hand, they were not tendered into evidence and can only be evaluated by the court but not by the clients, since all participants in the proceedings did not possess appropriate security certificates.

Pursuant to the opinion by the Supreme Court of RNM and in accordance with the ECtHR case law, the principle of fair trial implies that each of the parties is given reasonable opportunity to present the case before the courts and enjoy all safeguards contained in Article 6 of the European Convention for Protection of Human Rights and Fundamental Freedoms. This implies that defendants should be given the opportunity to determine the material truth and be able to apply the principle of equality of arms as stipulated in the LCP and the ECHR.

According to the case law of the European Court of Human Rights, the facilities which should be enjoyed by everyone charged with a criminal offence, include the opportunity to acquaint himself, for the purposes of preparing his defense, with the results of the investigations carried out throughout the proceedings (*Natunen v Finland (dec) application no.21022/04, judgment of 31 March 2009, s 42, C.G.P v The Netherlands, (dec) app.no.29835/96, decision of 15 January 2007 etc.*).

Any failure to present material evidence, which contains such particulars that could enable the accused to exonerate himself or have his sentence reduced would constitute a refusal of the facilities and conveniences necessary for the preparation of the defense, and therefore a violation of the right guaranteed in Article 6, Paragraph 3 (b) of the ECHR.

In the specific case, having in mind the ECtHR case law, the Court finds that the failure to disclose the SIM orders to the defense, as well as the failure to present them before the Court, considering that the defense requested their presentation as evidence in the procedure, goes against the principle of establishing the material truth and the principle of equality of arms. In this case, there was a possibility to secure them as evidence in line with the Law on Classified Information, which states that classified evidence can, by request, be declassified and presented during the proceedings, as was the case with the listening of the recordings and reading of the written communication records, for the purpose of ensuring equality of the parties without violating the right to defense.

Decision by the Supreme Court of RN Macedonia

Case Mayor

1. Reg.no. 97/201. Article 357 Paragraph 1 in relation to Article 22 of the Criminal Code. The Court finds that SIMs cannot be applied for this crime and orders those files to be removed and not to be used as evidence.

2. Reg.no. 3/2013. The first instance court violated the provisions of the criminal procedure of Article 355 Paragraph 1 Item 8 of the LCP by presenting prior judgments as evidence, which were already found to be unlawful by the Supreme Court, because they were based on evidence obtained through SIMs contrary to the law.

Appellate Court Skopje, RNM reg.no.1619/08

Case Bogorodica

The Appellate Court Skopje, on 3 February 2009, proceeding in the criminal case reg.no.1619/08 for the crime of Receiving a bribe of Article 357 Paragraphs 1, related to Articles 22 and 45 of the Criminal Code, and for the crime of Assisting an offender after a crime has been committed of Article 365 Paragraph 2, in relation to Paragraph 1, in relation to Article 45 of the Criminal Code, has passed a Decision reg.no.1619/08 to separate the evidence collected by using special investigative measures in accordance with Article 142b Paragraph 1 of the LCP from the case file III KOK no.5/07, and following the enforceability of this Decision, the evidence are to be placed in a separate binder and kept separately.

Namely, the Court's decision is based on the conclusion that the use of special investigative measures for the purpose of collecting evidence constituted a breach of the legality of the proceedings.

In the specific case, both looking at the order of the Court reg.no.25/07 of 15 January 2007 and the order by the Chief Public Prosecutor of the RNM, the Department for organized crime and corruption, it is obvious that the special investigative measures had been approved for the crime of Receiving a bribe as referred to in Article 357 Paragraph 1 of the Criminal Code, punishable by a prison sentence of 1-10 years.

Considering that the legal prerequisites for the use of the special investigative measures of Article 142b Paragraph 1 of the LCP have not been met (i.e. the special investigative measures have been imposed and undertaken regarding a crime that is not punishable by at least 4 years in prison, or the crime has not been perpetrated by an organized group, gang or other criminal enterprise), the undertaking of special investigative measures cannot be ordered. Thus, this evidence has been unlawfully secured, which goes against the quoted provision from the law, and they cannot be used as evidence that a judgment can be based on.

2.2. Commencement of the special investigative measures and making a decision over their use

One of the most intrusive special investigative measures, which, according to the annual reports of the Public Prosecutor's Office is the most often used, is the surveillance and recording of telephone and other electronic communications. In fact, this means secret learning of the content related to the technical process of sending, transmitting and receiving any type of speech, data, sounds, signals, written text, static or moving images, which serve to exchange information among people, between people and objects, among objects, or for the purpose of guiding any object with the help of a tele-communications system, as well as internet protocol, voice over internet protocol, website or e-mail, up to accessing technical equipment of operators through OTA or by using special technical devices and equipment without the mediation of OTA and operators, and parallel creation of a technical record on the content of the communication with a possibility for its reproduction.

Before using this investigative measure, but also any other special investigative measure that intrudes heavily into privacy, the criminal investigation bodies must possess relevant operational information in advance with regards to the individuals to be encompassed in the process of further processing, specifically relating to:

- their modus operandi,
- form, type and quantity of communications,
- number of involved individuals,
- dynamics of undertaken activities;
- types of undertaken activities;
- structure and structural relationships between the individuals;
- group.

This primarily relates to the possibility of obtaining preliminary data that can be used in the decision-making process whether the use of such an investigative measure is to be initiated. All of this clearly points to the conclusion that this is a pre-investigative procedure during which many information and data are collected, followed by their analysis and selection, towards creating a quantum of data that will further dictate the proceedings.

This is not a coincidence, but a necessity, because there must be a logical link between what is transmitted as information in the communication with the specific actions undertaken by the involved individuals as a natural consequence of what has been discussed and agreed. This is the only

way to get a full picture of the undertaken actions that arise directly from the previous communication, which contain illicit elements. Therefore, when referring to the necessity and success in the use of this type of data and evidence collection that cannot be collected by other means, one must first ensure certainty and efficiency in documenting.

The public prosecutor in charge of the pre-investigative procedure must ensure a proper logistical approach and facilities. This means that the judicial police have to secure the required human and material resources for the implementation of this investigative measure. This must be achieved in agreement with the public prosecutor, who must insist on a compact and experienced team that will be in continual coordination with the public prosecutor. In certain cases, this is dictated and imposed by the number of the involved individuals, the scope and territory of their operations, as well as the dynamics of the undertaken operations, while paying special attention to their connections in and out of the country. A successful implementation of these intrusive measures is possible only if the judicial police are properly manned and trained over their use.

The **motion** for the use of SIM is initiated by an authorized person of the judicial police and it should include the following:

1. accurate data about the persons or objects for which the special investigative measure is proposed,
2. designation whether the person's identity has already been established,
3. the type of the proposed special investigative measure and a proposal over the duration of its use, and
4. sufficiently elaborated reasons by listing all operational data in possession of the judicial police about the specific individuals indicated in the motion, alongside a reasoned explanation whether the judicial police had undertaken other prior measures and activities of securing data and evidence relevant to initiate a procedure, the results of their activities i.e. any threats and obstacles they came across in their obtaining, so that the public prosecutor is truly assured of the necessity to use these special investigative measures in this stage of the procedure.

The judicial police is the institution that most often proposes this way of collecting data and evidence, however, the law gives the option to the public prosecutor, who is managing the pre-investigative procedure, to initiate their use by his/her own assessment.

2.3. Request by the Public Prosecutor's Office for interception of communications

After receiving the motion, the public prosecutor drafts a **request** for the use of a special investigative measure, which must also be elaborated and accurately list the persons, telephone numbers and the items that will be subject of the special investigative measures. The request should be accompanied by the motion of an authorized authority within the judicial police.

The public prosecutor files the request for SIM to the competent preliminary procedure judge at his or her own initiative or at the proposal of an authorized person from the judicial police in writing, and this request should include the following:

1. legal title of the crime;
2. indication of the person or items subject of the special investigative measure;
3. technical means to be used;
4. scope and place of implementing the special investigative measure;

5. information and evidence that support the grounds for suspicion and reasoning why data and evidence cannot be collected otherwise;
6. the authority that has to implement the order;
7. duration of the special investigative measure;
8. type of telecommunications system, telephone number or other identification data, as well as identification numbers for each of them.

The principle of subsidiarity (“evidence and data cannot be collected by other means”) is a crucial protective principle, but one that has been most commonly “forgotten for critical checks and assessment” in practice thus far. This goes both for the measure applicant, i.e. the authorized bodies for the measure’s implementation, but unfortunately, also for the measure petitioner – the public prosecutor, but also for the court, as the last and final instance of approval, resulting in the devastation of the subsidiarity principle, i.e. the *ultima ratio* rule when applying intrusive measures.

The judicial police’s practice of imposing such measures by routine and as a common tool for information collection points to the lack of an efficient mechanism for procedural protection in the procedure of its proposal.

The request that the public prosecutor forwards to the preliminary procedure judge should contain sufficient *arguments* to convince the preliminary procedure judge of the necessity of using this type of collection of material evidence, i.e. the request by the public prosecutor should be clear, precise and properly elaborated.

Other files should also be attached to this request:

- the motion by the judicial police over the necessity to use the measure,
- any files related to the type and manner of collected information that are required for implementation of the measure,
- additional files in order to establish the involvement of the target individuals, the types of their mutual linkages, places in the hierarchy, and in the event of a criminal enterprise, the frequency of communication and possible movement locations.

All this data is required for the preliminary procedure judge to get the real picture and therefore to be able to make a free, unobstructed and meritorious decision on the necessity to use some of the measures. In the absence of sufficient information, the preliminary procedure judge can be put in a situation where he or she is not able to decide whether the implementation of a measure is required. Hence, it often occurs in practice that the request filed by the public prosecutor is accepted without any scrutiny, the simple reason being that the preliminary procedure judge accepts the *assessment* made by the public prosecutor when he or she decided to use this intrusive method of collecting evidence.

This is why detailed and comprehensive reports should be an integral part of the request that the public prosecutor submits to the competent preliminary procedure judge. In this way, the preliminary procedure judge can establish the probability that the use of the measure would result in data and evidence for successful management of the criminal procedure and that evidence and information cannot be collected by other means.

The highlighting of this need is also imposed by the very fact that all reports on communications intercepted on the grounds of an order issued by a preliminary procedure judge are drafted in one copy that is only submitted to the public prosecutor’s office. Another copy remains with the drafting

authority, but the copy submitted to the public prosecutor's office is the only one used as evidence in the procedure, in certain time intervals depending on the duration of the measures. It is not allowed to re-record, copy or modify evidence secured through the use of the measures, which are delivered on a CD, accompanied by written transcripts organized in separate binders.

2.4. Receipt and registration in the Public Prosecutor's Office

The registration of the motion for issuing special investigative measures is carried out in special logbooks in the public prosecutor's office, depending on the type of the measure, with full respect of the degree of confidentiality. The receipt and registration is done by a person designated by the head of the public prosecution office by means of an internal decision and these logbooks, as all other documents related to the use of the special investigative measures, are kept in a special safe deposit box that can be accessed only by this person.

The need for such security at the appropriate level of confidentiality and secrecy arises from the specific and sensitive character of the special investigative measures, especially the measure related to interception of communications, because their use significantly violates the human rights and fundamental freedoms guaranteed by the highest legal documents.

The process of data protection begins at the moment of drafting a motion for special investigative measures by the authorized institutions, and after registering this motion in the public prosecutor's office, it gets its unique identification number, which is the single valid reference number for the entire duration of the special investigative measures registered in the public prosecutor's office's internal records.

The **identification number** is the required technical condition so that the order issued on the grounds of the request can be successfully implemented in OTA from a technical aspect, because this is the way to ensure non-repetitiveness and the particularity of features and unambiguity of the operator during their technical recognition in the system of electronic communications.

This is a specific identification number that must contain a maximum of 25 features and it needs to be unique for every telephone number that is individually intercepted. These features are most often an abbreviation for the institution that filed the motion or the request, the day, month and year of filing the motion or request, the ordinal number of the communication in the motion or the request, the identification designations of each operator etc.

The necessity for a new way of designating documents drafted by the public prosecutor's office is not an additional burden or complete change in the system, i.e. the *modus operandi*, but a move that ensures a high degree of data protection. Namely, the manner of registration, processing and delivery of these documents was not previously precisely laid down in the legislation, and that was accompanied by the absence of bylaws that would accurately prescribe and determine not only the degree of confidentiality and *modus operandi*, but also the required security measures related to the reception, drafting and sending requests to a preliminary procedure judge, considering the routine ways of receiving and sending all other acts in and out of the prosecutor's office.

The use of transmission devices is forbidden during delivery, as well as expediting such requests by mail or unauthorized individuals. Any documents classified as "State Secret" (SS) and lower are properly packed and transferred (within the country) by an official delivery service or by persons having authority to access information classified as "State Secret" and lower, who have a special authority to transfer such information (based on the Regulation on administrative security of classified information, Official Gazette of RM no.82 of 19 November 2004).

The request must be properly sealed and stamped (with 3 or 5 stamps, as prescribed), with the stamps placed at a different distance on the external part where the envelope is closed. Documents classified as “I” (Internal) and higher are packed in a non-transparent cover, placed in two envelopes. The inner envelope is designated by security classification corresponding to the classification of the document, and if possible, contains the complete data on the job position of the user and his address.

A receipt note is drafted for the document that is being delivered, placed in the inner envelope. The receipt note, which should not be classified, contains a log number, date and number of the document copy, but no data on the document’s content. The inner envelope is placed in an outer envelope that includes only the title and address of the recipient and the notice number. The outer envelope should not display the security classification of the document that is delivered. The reception of notices with documents classified as “I” and higher is confirmed in the delivery book of the couriers, including a signature of the person authorized for reception, below the sending number of the notice.

3. Procedure of issuing special investigative measures by the court

The procedures of issuing special investigative measures include actions by a preliminary procedure judge and members of the trial chambers in the courts, from the moment of receipt of the request (written or oral) for issuance of SIM, up to the day of archiving the issued order.

As mentioned above, some of the special investigative measures are approved by the court, at the request of a public prosecutor. The notices arriving at the court, i.e. the requests for issuance of special investigative measures are personally delivered to an authorized person – court clerk possessing a security certificate with a proper level of security classification.

These types of requests are not distributed through the Automated Court Case Management Information System (ACCMIS), but after the notice gets a receipt seal, including the date and time, the authorized clerk forwards the request to a judge who is next in line to receive such a request, only if the request or the motion is new, meaning that the use of the special investigative measure is sought for the first time. Namely, this type of *ex officio* requests get a so-called “natural judge”, since a written record is maintained of judges proceeding on requests for issuing SIM, and the requests are distributed in turn.

If the request refers to the extension of the intrusive measure, even when it relates to a new person for whom the necessity resulted from the surveillance within an already issued order against other individuals, the request for extension of the intrusive measure is given to a different judge.

The orders issued at the request of a public prosecutor and referring to the special investigative measure of *Surveillance and recording of telephone and other electronic communications within a procedure established by a special law* as referred to in Article 252 Paragraph 1 Item 1 of the LCP are entered in a register designated as Register of Authorized Interception of Communications (RAIC).

This register is maintained manually and there is no electronic record thereof – *there are no electronic files for this type of cases*, because the court Rules of Procedure do not stipulate the formation of cases designed as RAIC.

This **Register** includes the following information:

1. Ordinal number of the issued order;
2. Date of receipt of the request;
3. Request petitioner;
4. Persons for whom SIM is sought;
5. Title of the crime;

6. Duration of measure; and
7. Date of issuance.

Unlike this investigative measure, cases are created for all other special investigative measures after the requests have been electronically recorded in the ACCMIS system.

After obtaining a registry number, the written request is submitted to the judge who is supposed to proceed on it, alongside a delivery list that includes the number of the created case, classification level, designation by the public prosecutor's office and the date and time of receipt. The section related to records of persons acquainted with the case content includes all individuals who have access to it, and must possess a security certificate. These individuals are obliged to put their signatures and date.

After drafting the order, it is placed in an envelope and the proceeding judge returns it to the authorized clerk, who signs and dates it. Afterwards, it is delivered personally to the authorized person designated by the public prosecutor's office, who confirms the receipt with his signature.

The drafting of the classified notice is done in a special room within the court building, on a protected PC that is not connected to a network, with continual video surveillance of the entrance, in order to record each entry and exit from the room for drafting of the SIM.

The order is drafted in three copies and the **classification** determined by the petitioner - confidential, secret and state secret - should be displayed in the upper center section on every page of the order. One copy of the order remains in the court, where it is placed in a separate envelope together with the request, the folder from the public prosecutor's office, other annexes and the delivery list of the case. Three seals are put on the envelope itself and the classification of the information in the envelope is also displayed on the front side of the envelope, including the number of the order and the date of issuance.

Four copies of the order are delivered to the public prosecutor's office in two separate envelopes, in the same way as the copy for the court, of which three copies are anonymized in line with the Rulebook - one anonymized copy for OTA and two identical anonymized copies for oversight and control. One anonymized copy of the order for OTA and one anonymized copy of the order for oversight and control are put in the envelope intended for OTA. The non-anonymized copy of the order and one anonymized copy of the order for oversight and control are placed in the other envelope intended for the authorized institution for implementation of the SIMs.

3.1. Anonymization

Based on the new rules for the use of special investigative measures that refer to the necessity of ensuring a high level of data protection regarding phone numbers, persons and items that are targets of special investigative measures, two Rulebooks on the anonymization of judicial orders have been adopted, one related to the manner of anonymization of the court order when measures are undertaken for criminal purposes, while the other related to the manner of anonymization of court orders when measures are undertaken for the purpose of protecting the interests of security and defense of the state.

Anonymization is a process in which all identifying elements listed in the order, including personal and other data, are removed in a way that prevents the direct or indirect identification of the personal data.

The establishment of the Operational Technical Agency (hereinafter OTA) and its launch (1 November 2018) as a technical-intermediary institution (mediating in the transmission of the signal, but not 'listening') uncovered certain shortcomings of "technical" nature between the competent authorities for implementation of the measures and the operators, which hinder and sometimes prevent the use

of the measures. Namely, the introduction of the “identification” number (tool for anonymization and protection of the measure’s secrecy) as an element in the court order, caused initial misunderstandings about the institution charged with its determination (is it the court or the public prosecutor’s office) and its form, followed by serious technical obstacles for the measure’s implementation if it is not properly determined and technically formatted (this turning into a “key” shortcoming of the court order).

The envelope for the court, including all sealed materials, is delivered to the authorized clerk who is obliged to place these materials in special safe deposit boxes located in a specialized facility for safekeeping of classified information. This specialized facility must be under 24-hour video surveillance and maintain electronic records of every entry and meet the standards for management of classified information. These standards refer to the area surrounding the facility, which represents a minimal distance from the area where the classified information is stored – **secure area** or room within the facility that holds or stores classified information designated as “classified” or higher, and requires appropriate physical protection, i.e. a so-called **secure zone**.

The judge who issued the court order is charged with its anonymization and the anonymized copy of the order submitted to OTA should contain the following data:

1. number of order and issuing authority;
2. technical means to be applied;
3. duration of the special investigative measures and identification number; and
4. type of telecommunications system, phone number and other identification data, as well as an identification number for each of them individually.

In order to ensure control over the use of the measure, the law provides that the anonymized copy of the order must contain the following data for the purpose of oversight and control:

5. number of order and issuing authority;
6. duration of the measure; and
7. identification number.

The preliminary procedure judge immediately submits the issued order, alongside the anonymized copy of the order for the purposes of OTA and the anonymized order for the purpose of oversight and control to the public prosecutor, who immediately submits the anonymized copies of the order to OTA if the measure is to be used. If the special investigative measure is enforced by the judicial police, the public prosecutor submits the issued order and the anonymized copies of the order to the authorized person in the judicial police, who then delivers them to the authorized person in OTA, who is obliged to proceed without delay.

The rulebook on the manner of anonymization of orders does not stipulate the anonymization of the order’s reasoning, as it is provided for other types of decisions or judgments. This reasoning also contains data that could directly or indirectly identify the person, and that is why this data must be designated by “X” in the reasoning section of the order.

4. Grounds for suspicion as an assumed standard for measures’ activation

Although SIM have the grounds for suspicion as the assumed activation standard, it is entirely irrelevant in correlation to the necessity in the society to protect certain values and properties, or in different terms, the initial and assumed importance for the use of SIM is *the proportionality principle*. When it comes to the use of SIMs, the proportionality principle is always cumulative and complementary to the *subsidiarity principle*.

Considering that the special investigative measures always infringe the right to privacy of the individual protected by Article 8 of the ECHR, the court should especially evaluate and assess the justification of the interference in the privacy of the individual by the executive when approving the orders for such measures. In other words, the legitimacy of the executive to intrude in the private sphere of the individual on the grounds of legality, proportionality and subsidiarity must be restricted and controlled by an independent judiciary through the principle of prior court approval of the measures.

When proposing these measures, it is necessary to list the facts and circumstances that point to the existence of *suspicion* that a crime is in preparation or has been committed, and it is not possible to conduct the investigation in a less intrusive way.

The lack of clear and precise regulations and standards creates the possibility of “looser” interpretation of the legal provisions, resulting in requests submitted by the public prosecutor and issued orders for special investigative measures that have the identical reasoning that “*the investigation cannot be conducted in another way*” without listing any facts and circumstances that would support such a statement.

The biggest weakness in the use of the measure “interception of communications” is its personal and subject matter indiscrimination. Namely, there is no technical option to completely elude or select communications of persons who have no links to the crime (personal indiscrimination) or avoid conversations in no way related to the crime (subject matter indiscrimination) when using this measure.

In the course of the measure’s implementation one should provide for personal and subject matter selection, through the so-called procedure of minimization of the intrusion and endangerment of privacy of those concerned, but also *post festum*, i.e. after the measure ends. However, regardless of the regime of protection and secrecy of the obtained information from the use of the measure and the obligation to erase recorded contents that have no relevance to the crime, the fact that the private life of innocent individuals has been violated cannot be neglected. Considering the degree of infringement into an individual’s private life, the issue of the approval regime for this measure is always a matter of debate.

4.1. Elaborated reasons why data or evidence cannot be collected by other means

The order for the use of special investigative measures must include reasoning for its issuance, namely facts about the case, circumstances pointing to the reasonable suspicion that a crime has been committed and especially any circumstances suggesting that the investigation could not be carried out in a less intrusive way.

The degree of suspicion can only seemingly be considered as defense against excessive use of the measures, because the crucial aspects for the measure’s approval are the two cumulative factors: the necessary social need to protect certain goods and the inability to collect the information by other means. In other words, the use of this measure is not primarily determined by the degree of suspicion, but above all by the inability to collect information by other means while there is an urgent need in the society to protect the proclaimed interest.

The grounds for suspicion exist when the quantum of information is sufficient to lead a reasonable man into believing that a certain crime has been committed.

Although the LCP still has no clear definition on the term “grounds for suspicion”, it is clear that the grounds for suspicion is a lower standard than the “reasonable suspicion”, not only because it can be ascertained by information that is lower by quantity and content than the ones required for a reasonable suspicion, but also because grounds for suspicion can arise from information that is less credible than the ones required for reasonable suspicion. For example, information acquired from an anonymous phone call is not sufficient to assert the existence of grounds for suspicion, but the overall circumstances can point to the fact that some significant aspects of the informant’s story are sufficiently supported by other information of the police, which would justify the existence of grounds for suspicion in that case.

4.2. Urgency of procedures

One of the main features of the criminal procedure is the principle of urgency, which demonstrates the legislator’s intention to conduct the procedure swiftly, efficiently and without delay. Despite the fact that this is not one of the fundamental principles of the special investigative measures, it is still used in the procedure of applying special investigative measures because actions contrary to this principle could harm the permanent or vital interests of the state, as well as the operations and efficiency of the institutions of the Republic of North Macedonia.

A preliminary procedure judge is deciding on the request for applying SIM within 72 hours from the filing of the request. In special cases of reasonable suspicion that the delay could have a negative effect on the criminal proceedings, the preliminary procedure judge can issue a temporary written order. *This type of order, due to its urgency, is issued at once, i.e. no later than 12 hours from the filing of the request, and this order allows the implementation of the investigative measure only for a period of 48 hours.* Despite the fact it is a procedure in urgent cases, the public prosecutor must file a written request based on which the judge issues a temporary written order.

Unlike before, when there was an option of issuing an oral order, the new law does not provide this option. Instead, in case of urgency, and upon a written request, a decision is made at once, i.e. no later than 12 hours, instead of the regular 72 hours.

The principle of urgency is also highlighted in Article 10 of the Law on Interception of Communications, **“when there are grounds for suspicion that the delay can negatively affect the implementation of the procedure”**, however, without stating specific circumstances as criteria based on which the real state of urgency can be measured and ascertained.

This inconsistency of the law (the deleted Article 14 of the LIC of 2006 defined the circumstances that point to the need for urgency) affects the uniqueness and unification of the legal interpretation of the urgency aspect in the procedure, meaning that judges are left to their own judgment and feeling of legality and fairness when assessing it. Of course, the right of free judicial conviction is not arbitrary decision-making, but judges are guided by certain rules (analogy) that are already established in other legislative branches that refer to assessing the state of urgency. The state of urgency can usually be recognized:

- when there is a threat of causing death or severe bodily harm to one or more persons;
- when there is threat of causing material damages of property of large scale;

- when there is a threat of flight of a person who committed a crime punishable by life imprisonment; and
- in other cases when there are circumstances that point to the state of not repeating or the damage being irreparable, which can occur if the required measures are not urgently undertaken.

5. Use of special investigative measures as evidence in the criminal procedure

The special investigative measures must be ordered and implemented in accordance with the provisions that regulate them. Otherwise, any evidence arising from the use of the measures cannot be used before the court and a judgment cannot be based on them.

Article 259 of the LCP regulates the use of evidence collected through the use of SIM, in a procedure before a court and the examination of the undercover agents who took part in the measures' implementation as witnesses.

Paragraph 1 stipulates that data, information, documents and items collected through the use of special investigative measures can be used as evidence in the criminal procedure if they are collected under conditions and in a manner regulated by law. The presentation of this evidence before the court is carried out in line with the general rules for presentation of written and material evidence before the court.

Paragraph 2 regulates the *exception* from the use of evidence collected through the use of special investigative measures. Statements by persons who are exempted by law from the duty to testify (clarified in Article 214 of the LCP), obtained through the use of special investigative measures, cannot be used as evidence.

Undercover agents taking part in the implementation of the measures of Article 252 Paragraph 1 Item 10 of the LCP can be questioned as protected witnesses, under the conditions of Articles 226-232 of the LCP, which regulate the protection and questioning of endangered witnesses. The identity of these individuals is an official secret.

In cases where undercover agents are questioned as endangered witnesses, the court must, when making a decision, consider the provision of Article 400 Paragraph 1 of the LCP, which states that the judgment cannot be based solely on the testimony of the endangered witness, in compliance with the ECHR case law. The examination of these persons before the court should be a required evidence in the procedure, primarily aimed to control and confirm the presented evidence collected through the use of special investigative measures, and not be evidence in itself.

If the SIM are implemented in the absence of the conditions required for their undertaking (Article 252 Paragraph 1 of the LCP); or for a crime not covered by Article 253 of the LCP; or without an order from the authorized authority; or the order has been overstepped during their use; the obtained data from such illegally implemented measures cannot be used before the court and the court decision cannot be based on them. The situation is identical when the provisions of Article 263 and Article 268 Paragraph 1 of the LCP are not observed when undertaking the measures.

Therefore, SIMs have the equal legal significance and importance as other investigative operations, because they can provide evidence in the form of statements, which in a criminal-legal sense can be seen as an admission by the defendant or the witness, but also can be used for obtaining material evidence, which in a criminal-legal sense are identical to any evidence collected during the crime scene investigation, searches or different types of expert examinations.

Any evidence collected by using special investigative measures can be used in a criminal procedure, as long as it has been lawfully obtained, as prescribed in the court order. Therefore, the court order and its modality comprise the *condition sine qua non* over the lawfulness of evidence obtained by using special investigative measures and therefore, any other manner of obtaining evidence would be an absolute breach of the criminal procedure provisions.

Article 12 of the LCP encompasses the matter of legality of evidence in the criminal procedure, and the same article (first paragraph) contains an explicit prohibition to collect evidence by using any form of force, and prohibition (in the second paragraph) for assessment of unlawfully obtained evidence (contrary to the way prescribed in the law), by violating the freedoms and rights established by the Constitution of the Republic of North Macedonia, the laws and international treaties and all other evidence derived from the previous two types of evidence.

6. Duration of measures and their extension

Based on Article 260 of the LCP and Article 11 of the Law on Interception of Communications, special investigative measures can last up to four months, and Paragraph 2 stipulates that a preliminary procedure judge can extend the measures **for another four months** upon a reasoned written request of the public prosecutor. For crimes entailing a prison sentence of at least four years, for which there is reasonable suspicion they had been perpetrated by an organized group, gang or other criminal association, the measures can be *extended* for additional six months after the initial eight months, i.e. measures can last up to 14 months in such cases.

The principle of legality in the use of special investigative measures means it has been established in advance how long the measures can last, i.e. their duration is limited in time. The duration of the measures is gradual and their extension can also be done in one-month intervals, but their overall duration is limited in time. The use of special investigative measures ends when their deadline expires or the reasons for their use no longer exist.

As mentioned above, if the special investigative measures of Article 252 Paragraph 1, Items 1, 2, 3 and 4 are applied for crimes that entail a prison sentence of at least four years and there is a reasonable suspicion they had been perpetrated by an organized group, gang or other criminal enterprise, the deadline of Paragraph 2 of this article can be extended by the preliminary procedure judge for another **six months** at most. Besides a written request from the public prosecutor, the preliminary procedure judge decides on the extension of the deadline in this case based on the assessment of the value of the collected data through the use of the measure and the existence of a reasonable expectation that the measure can continue to provide data in the interest of the procedure.

Regarding the special investigative measures of Article 252 Paragraph 1, Items 5-12 of the LCP that are imposed through a written order by a public prosecutor, the duration of their use can be extended until the achievement of the aim for which the measure has been approved, but no later than the completion of the investigation.

If the preliminary procedure judge does not accept the written request of the public prosecutor and decides to deny the extension of the special investigative measures, the public prosecutor is entitled to file a complaint against the decision to the trial chamber, which is set to decide on the complaint within 24 hours.

6.1. Rejection of a request for issuance of special investigative measures

Based on Article 294 Paragraph 3 of the LCP, a preliminary procedure judge issues an order for special investigative measures upon a motion by a public prosecutor. The previous paragraph of the same article precisely stipulates that if the preliminary procedure judge does not agree with the motion of the public prosecutor over the issuance of an order for search of a home, other premises and individuals, he/she shall put forward this disagreement to the trial chamber comprised of three judges whose composition and competence is established by Article 25 Paragraph 5 of the LCP. The trial chamber decides on the disagreement within 24 hours, either confirming it and thus rejecting the motion for issuance of the order, or rejecting the disagreement by the preliminary procedure judge and issuing the requested order. The disagreement to issue an order is confirmed by a decision, with no right to an appeal, considering it is passed in second instance and is final.

Unlike the procedures related to search orders of a home, other premises and individuals, it is not regulated what would happen if the preliminary procedure judge fails to approve the issuance of an order for special investigative measures. According to Article 11 of the Law on Interception of Communications, if the preliminary procedure judge does not agree with the motion for a special investigative measure, the LCP provisions regulating the procedure when a preliminary procedure judge does not agree with the motion of the public prosecutor are applied. Accordingly, if the judge disagrees with the issuance of an order for implementation of a special investigative measure, he/she shall put forward the disagreement to the trial chamber, which either confirms it by a decision with no right to an appeal, or rejects it and issues the required order.

Despite the legislator's failure to clearly regulate what would happen in a case of a preliminary procedure judge disagreeing with a motion for a special investigative measure, it is clearly stated that a trial chamber comprised of three judges decides within 24 hours on the decision of a preliminary procedure judge rejecting the *extension* of the measure's duration, upon an appeal by the public prosecutor (LCP, Article 260 Paragraph 5).

6.2. Expansion of the order

Special investigative measures can be applied only for the crimes listed in Article 253 of the LCP. However, during the implementation of a special investigative measure one may also obtain information related to other crimes that are not covered by the order.

Two aspects are to be considered regarding the issue of order expansion:

1. the first relates to the issue of the order expansion to (subject or target) persons that had not been encompassed by the order before but emerged during the application of the measures; and
2. the second relates to the issue of the order expansion regarding (item or object) a new crime that emerged during the application of the measure.

In such cases, the law stipulates that the special investigative measure shall continue despite the fact that the crime is not listed in the order, but only if it is a crime covered by Article 253 of the LCP, i.e. a crime that allows the use of special investigative measures. Any information obtained in this manner can then be used as evidence in the criminal procedure initiated against the perpetrator of the crime. Namely, the obtained data from the special investigative measures in cases when information point to another crime of Article 253 of the LCP perpetrated by the same person covered by the order for the special investigative measure has not been a problem in the case law so far.

The problem emerges when the information relates to a crime of Article 253 of the LCP, but another person appears as the perpetrator and not the one under the special investigative measure. Considering the LCP provision that a special investigative measure can be applied only against a known (identified person) or against an object of crime (Article 252 Paragraph 2 of the LCP), the current provision might be seen as meaning that the data about a crime committed by another person cannot be used in the procedure because there is no order against that person, *which is not the law's intention*. Therefore, this provision should be broadly interpreted, i.e. that any information obtained about a crime committed by another person can be used in the procedure if the other conditions listed in the LCP are fulfilled.

Case law:

When the public prosecutor waived his or her right to prosecute for the crime of "criminal association" of Article 394 Paragraph 1 of the Criminal Code that involved special investigative measures, the court did not have any legal grounds to assess the evidence collected through the use of the special investigative measures and to found its judgment on them. The defendants were found guilty of the crime "receiving a bribe" according to Article 357 Paragraph 1 in relation to Article 22 of the Criminal Code, which is a crime that does not justify the use of special investigative measures.

Supreme Court decision, KVP-97/2010

The first-instance court breached the provisions of the criminal procedure of Article 355 Paragraph 1 Item 8 of the LCP when presenting as evidence prior judgments that the Supreme Court had found as unlawful because they were based on evidence obtained by special investigative measures contrary to the law.

Supreme Court decision, KVP KOK1-3/2013

6.3. Termination of SIMs

The authority that issued or extended the order is obliged to immediately terminate the measures when the aims for which they had been applied are achieved or the grounds for their approval have ceased to exist.

If the public prosecutor waives the prosecution of the crime or if the data collected by the special investigative measures is not significant to the procedure, they are to be destroyed under the judge's supervision, with the public prosecutor making a record thereof.

6.4. Notification of person concerned

According to Article 262 of the LCP, the person concerned can ask for the written order for the special investigative measures to be delivered to him or her, irrespective of the fact that an indictment had or had not been raised against that person after the implementation of the special investigative measures.

The public prosecutor makes the decision whether the order shall be submitted to the person concerned, because the law gives the public prosecutor the right to assess if this action would harm the procedure.

Unlike the Macedonian LCP, the Bosnia-Herzegovina LCP stipulates a compulsory notification of the person against whom a special investigative measure has been applied after its implementation. In this regard, it is not important why the special investigative measure had been terminated, i.e. was it terminated because of the expiry of its deadline or because the reasons for its use had ceased to exist. This provision is supported by the right of the person under the measure to assess its lawfulness, for the purpose of preventing unfounded and illegal restriction of the person's rights and fundamental freedoms. (*Sijercic Colic, H. Commentary on the Bosnia-Herzegovina Law on Criminal Procedure, Sarajevo 2005, p.371*).

The law says that the person concerned can also submit the request for the written order to the court, i.e. to the preliminary procedure judge as the authority who issues the special investigative measure.

Although not stated in the law, the preliminary procedure judge can decide not to deliver the order if there are indicators that this move would harm the procedure.

Besides notifying the persons concerned, the Chief Public Prosecutor of the Republic of North Macedonia submits an annual report to the Parliament of the Republic of North Macedonia on the special investigative measures requested during the previous calendar year. In this way, the public controls the use of the special investigative measures that must be legally regulated in order to prevent their abuse and any unfounded breaches of human rights and fundamental freedoms. However, the oversight by the Parliament of the Republic of North Macedonia is only an overview of the statistical dynamics in the use of these measures.

6.5. Legal access to the obtained data

Article 264 of the LCP regulates that each person who learns of data related to or arising from the use of special investigative measures is obliged to keep them as an official secret.

Article 31 of the LIC also provides an obligation for the persons in the competent authorities for implementation of the measures for interception of communications, persons from OTA and persons from the operators, who find out data related to or arising from the use of special investigative measures to keep them as an official secret. This obligation is valid for the entire duration of the persons' employment in OTA and five years after termination of the employment. This does not include data obtained unlawfully.

6.6. Erasing or destroying collected personal data

Considering that the subject of the special investigative measure of Article 252 Paragraph 1 Item 5 of the LCP is processing of citizens' personal data, the obligation to erase and destroy collected personal data is specifically regulated.

Namely, the deadline is related to the non-initiation of criminal procedures after the expiry of the 15 months from the completion of the measure implementation.

Article 267 of the LCP reads:

If a criminal procedure is not initiated within 15 months after the completion of the measure of Article 252 Paragraph 1 Item 5 of this law, any collected personal data shall be erased or destroyed under the supervision of a preliminary procedure judge, public prosecutor and representative of the Directorate for Personal Data Protection, with the public prosecutor making a record thereof.

The erasure or destruction is carried out under the supervision of a preliminary procedure judge as the competent authority for applying this special investigative measure, a public prosecutor and a representative of the Directorate for Personal Data Protection. The Directorate is an independent body, a legal entity authorized to conduct oversight over the legality of activities undertaken when processing personal data and their protection throughout the country's territory. The public prosecutor is obliged to make a record of the erasure or destruction of the collected personal data.

6.7. Storage and disposal of data collected using special investigative measures for interception of communications

One of the main issues in a democratic society is how to store or dispose of data obtained by using special investigative measures, i.e. who will guard the guards (*Quis custodiet ipsos custodiet*).

Any data collected and processed by enforcing an order for implementation of measures for interception of communications is stored by the public prosecutor in the course of their duration, but

are submitted to the court after a decision is made by the public prosecutor. If the public prosecutor decides to close the investigation without the option of its reopening, any data collected using special investigative measures are handed over to a preliminary procedure judge. If the public prosecutor raises an indictment and the court delivers a judgment of acquittal or rejection, any data collected by using special investigative measures are stored in the court until the expiry of the statute of limitations for criminal prosecution. In a case of a guilty verdict, the data is stored until the expiry of the statute of limitations on the enforcement of the sanction. After the expiry of the deadlines, the data is destroyed and a report is drafted.

A preliminary procedure judge makes the decision for destruction of the data based on a special request or ex officio. The public prosecutor or the person concerned submits the request. The destruction of data is carried out by a judge designated by the President of the court where the criminal procedures involving the data took place. The judge drafts a report on the destruction. Data collected using special investigative measures issued by Basic Court Skopje 1 Skopje have been stored in the court since 2007. A commission for the destruction of these materials is yet to be established.

Any data collected by using measures for interception of communications for the protection of the country's interests, defense and security, if believed that those are important for the measure, is stored with authorized bodies for the measures' implementation, in compliance with the regulations for protection of personal data and classified information, for a period of three years from the expiry of the order's duration. This period of three years can be reactivated in case of occurrence of new information that is directly linked to the specific data for which the storage period has not yet expired. In a case when the three-year period is extended, it is necessary to carry out and document a periodical assessment of the requirement to store specific data at an annual level. This data is subject to assessment with the aim of establishing whether they are significant to the aims for which the measure for interception of communications had been implemented. The Director of the National Security Agency and the Minister of Defense prescribe the respective method of establishing the relevance of data.

Any data and information obtained through the use of SIMs shall be destroyed under the supervision of a preliminary procedure judge, who needs to draft a special report on two occasions: if the prosecutor waives the prosecution and if the obtained information and data are not necessary in the criminal procedure. In this case, the person is notified in writing about the undertaken procedure of destroying and erasing. Upon undertaking the procedure, the preliminary procedure judge shall notify the person against whom the procedure has been undertaken without delay, and this person can ask the court to examine the legality of the order and the course of the procedure related to the undertaken measure. Accordingly, any person who considers that his his/her rights and freedoms had been violated through the use of the measure, can ask the court to examine its legality, manner of its use and the court orders providing the grounds for its use, which represents another aspect of the people's protection from unlawful interference in their rights and freedoms. Data and information obtained by undertaking special investigative measures are kept throughout the course of the entire court procedure.

Case law in the Republic of North Macedonia

This is the case called *Pepel* (Ashes) no.03/09, where the attorneys representing the defendants were targets of special investigative measures. There was no procedure initiated against the attorneys and they were not suspects in the case. All data was submitted by the public prosecutor's office upon completion of the investigative procedure, after an indictment was raised and the main hearing already begun. The public prosecutor's office withdrew those data from the subsequent proceedings, but no indictment has been raised until this day against these individuals and they have not been called yet to witness the destruction of the collected data from the SIM.

ANEXES TO PART 2

CHECKLIST FOR IMPLEMENTATION OF SIMs

MOTION

- **Judicial police drafts motion for SIMs to a public prosecutor.**
- **The motion includes:**
 - Accurate data on the persons and items for which the use of SIMs is proposed (if their identity has been established);
 - Type of proposed measure;
 - Reasoning why SIMs are being proposed.

RECEPTION AND REGISTRATION

- **Reception and registration of the judicial police's motion at the basic public prosecutor's office**
 - A person authorized by a public prosecutor registers the motion in separate internal books that are kept in a special safe-deposit box;
 - The motion receives a unique identification number that remains the same throughout the duration of the SIM.

ASSESSMENT

- **The public prosecutor, at his own initiative or at the proposal of an authorized person from the judicial police, assesses the need for SIM.**

DRAFTING A REQUEST

- **The public prosecutor drafts a request if there is a need for SIMs.**
- **The written request includes:**
 - Legal title of the crime, person or items subject to the SIMs;
 - Technical means to be applied;
 - Scope and place of implementation of SIMs;
 - Knowledge and evidence that establish the grounds for suspicion;
 - Reasoning why the data or evidence cannot be collected by other means;
 - The institution that is to implement the order;
 - Duration of the measure;
 - Type of telecommunications system, telephone number or other identification data, as well as identification numbers for each of them individually.

DELIVERY

- **The public prosecutor delivers the request to an authorized judge.**

PROCEDURE

- **Actions taken with regards to the request for SIMs by an authorized judge/preliminary procedure judge:**
 - The request by the public prosecutor for interception and recording of telephone and other electronic communications is entered into the RAIC register;

- The ordinal number of the issued order, the date of request's registration, the petitioner of request, the person for whom SIMs are sought, the crime, the duration of measure and the date of its issuance are registered;
- Upon receiving the registration number, the request is submitted to an authorized judge.

DELIVERY LIST

- **Drafting a delivery list.**
- **The delivery list includes:**
 - Case number, classification level, designation by the public prosecutor's office, date and time of receipt and data, signature and date for each person who has access to it.
- **All persons having access to these measures hold a security certificate.**

ORDER ISSUANCE

- **The judge/preliminary procedure judge drafts an order.**

ANONYMIZATION

- **Anonymization of the order delivered to OTA:**
 - Number of order and issuing authority;
 - Technical means to be applied;
 - Duration of SIMs and identification number;
 - Type of telecommunications system, phone number and other identification data, as well as the identification number for each of them individually.
- **Anonymization of the order for the purpose of oversight and control:**
 - Number of order and issuing authority;
 - Duration of the measure;
 - Identification number.

ORDER DELIVERY

- **The order is delivered to the Public Prosecutor's Office.**

REPORTS

- **In the course of the SIMs' implementation, the judicial police drafts a report that is delivered to the public prosecutor at his request and at every 30 days.**

FINAL REPORT

- **Upon implementation of the measures, the judicial police drafts a final report that is to be delivered to the public prosecutor.**

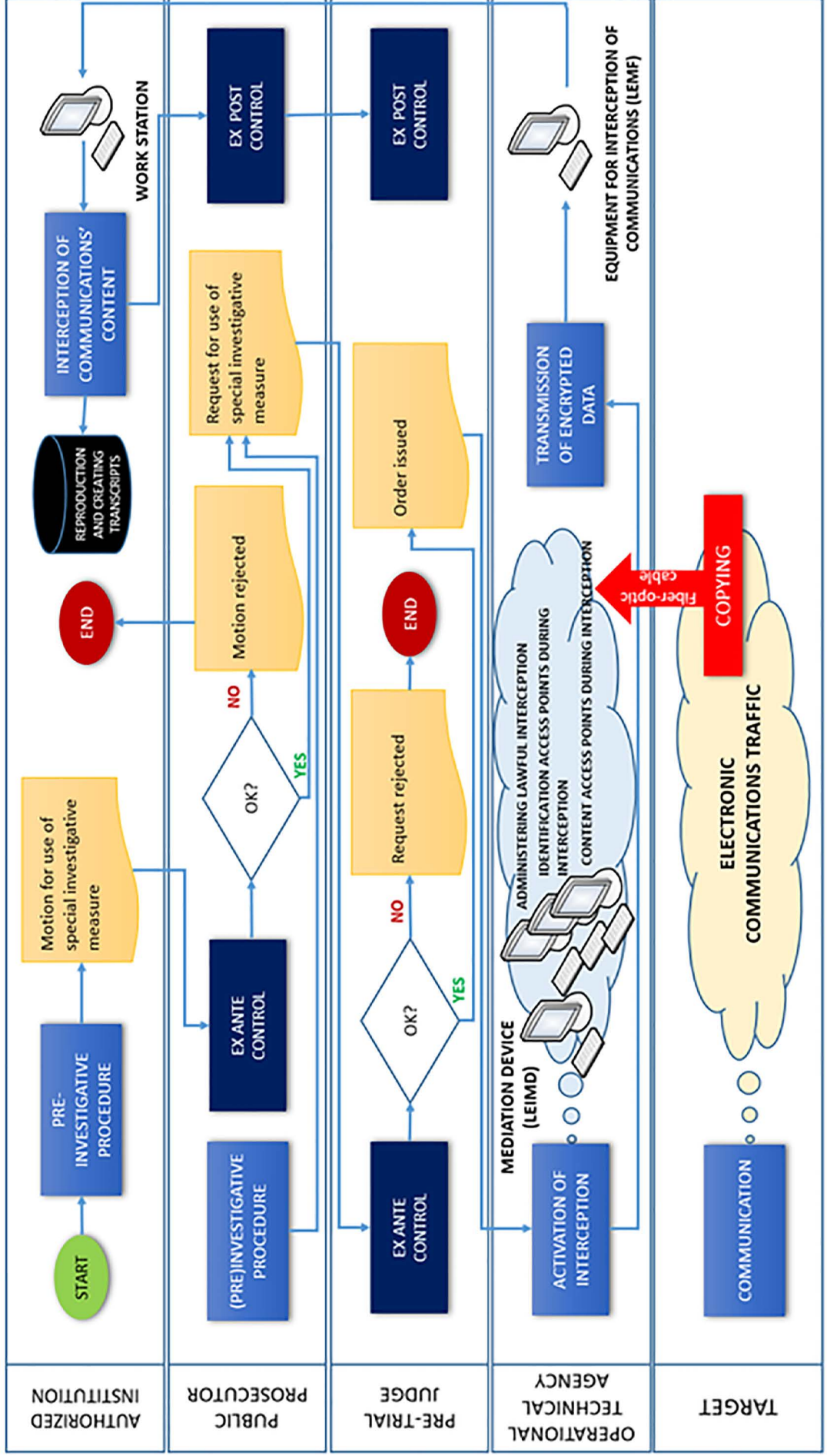
DECISION

- **The public prosecutor passes a decision.**

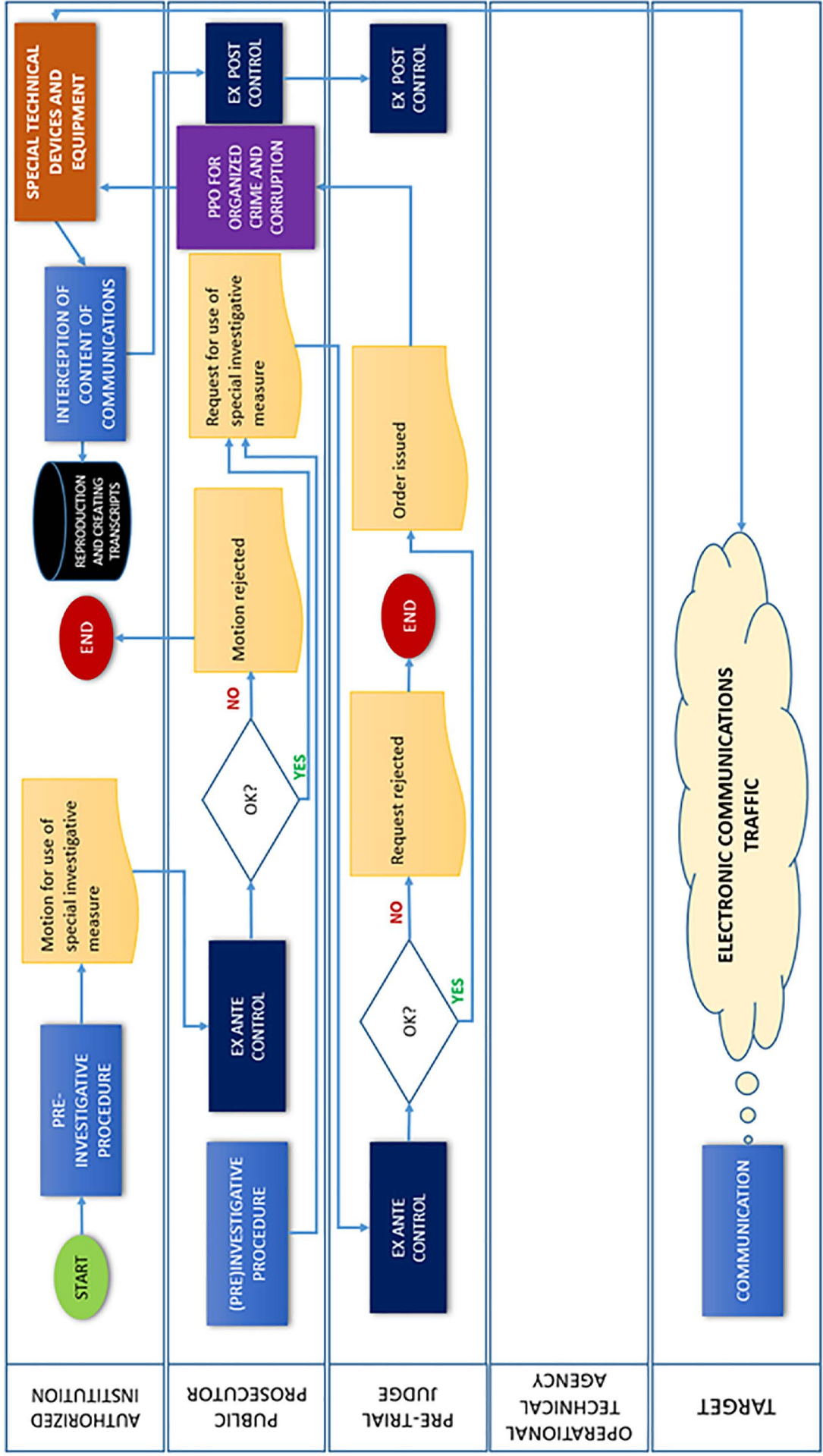
DELIVERY TO COURT

- **The public prosecutor delivers the final report and the entire technical documentation to the court within eight days.**

INTERCEPTION OF COMMUNICATIONS IN CRIMINAL INVESTIGATIONS WITH OTA AS AN INTERMEDIARY



INTERCEPTION OF COMMUNICATIONS IN CRIMINAL INVESTIGATIONS WITHOUT OTA AS AN INTERMEDIARY





PART 3

NATIONAL SECURITY



1. Definition of national security

1.1. Defining national security and defense in the domestic legislation

The term national security in our country was defined for the first time in the Law on coordination of the security-intelligence community (Official Gazette of RNM no.108 of 28 May 2019). **Namely, national security is a state of social, economic and political stability that is necessary for the survival and development of the country as a sovereign, democratic, independent and social state, as well as maintenance of the constitutional order, the state of unhindered attainment of human rights and fundamental freedoms in compliance with the Constitution.**

In fact, this legal definition has been aligned with the definitions in the international documents but determines national security in a more narrow sense.

The national security and defense interests of our country directly emanate from the core values in the Constitution:

- Maintenance of the independence, sovereignty and territorial integrity and the unitary character of the state as a fundamental framework for maintenance and promotion of the national identity and free fostering and expression of the ethnic and cultural identity of all citizens;
- Protection and promotion of peace and security, life and health, property and personal safety of citizens;
- Preservation and promotion of the democratic values of the state;
- Human rights and fundamental freedoms;
- Preservation and promotion of firm and functional multiethnic democracy;
- Political and defense integration in NATO, political, economic and security integration in the European Union and active participation in other forms of international cooperation.

The country's defense is a system defending its independence and territorial integrity, attained in line with the Constitution, Law on Defense and other laws, the country's Defense Strategy, other documents and international treaties ratified in accordance with the Constitution.

The country's defense is achieved by its citizens, state authorities and the Army as an armed force. Legal entities can, if required, carry out certain tasks in the area of defense. The country's defense can also be achieved through cooperation with the collective defense and security systems to which the Republic of North Macedonia has acceded (Law on Defense).

Today's world is characterized by swift and dynamic changes that bring about new and often unpredictable risks and threats to the security of states. Although the danger of classical military threat is not expected on the long term, non-military threats have not only become diverse, but have gained on intensity, space and time.

Besides its benefits, the globalization trend has also resulted in threats caused by the internationalism of certain threats, the most extreme of which are terrorism and organized crime. In addition, illegal migration and illicit trafficking in drugs, humans and strategic materials have experienced expansion. Furthermore, the threat of using weapons of mass destruction, which is banned according to international law, has increased.

The cooperation with international security organizations – UN, NATO, EU and OSCE provides for active participation in creating the global defense policy and improvement of the national capabilities to manage new threats, risks and challenges, and more efficient management of civil and military capacities.

The concept of national security relates to the state values: territory, sovereignty, foreign policy interests and national economy, which are protected from external armed attacks, internal armed rebellions and intelligence subversive activities by domestic and foreign actors.

Article 8 Paragraph (2) of the ECHR explicitly specifies the term of “national security” as one of the legitimate grounds for the use of intrusive measures and restrictions of the fundamental rights and freedoms protected by Paragraph (1) of the same article (“in the interest of national security”). The ECtHR’s case law implies on several occasions the justification and importance of this legitimate grounds for state enforcement.

In the case of *Klass v. Germany*, the ECtHR notes that “the powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.” In this sense, it is considered that organized crime, terrorism or espionage can create the need for high-level interference in the private life of the individual, because of their serious threat to the democratic society. In any case, the importance of the purpose on one hand and the level of intrusion in the private lives of citizens on the other, should always be considered.

The Constitution of RNM does not specify the term “national security” and there are no provisions that refer to a different specification of internal and external security. However, similar to Article 8 of the ECHR, Paragraph (2) of Article 17 (Amendment XIX) of the Constitution (same as Article 122) specifies that one of the legitimate grounds for use of the measures for interception of communications is when that is “required in the interests of the security and defense of the Republic”. The provision clearly indicates that the legislator differentiates between the terms “security” and “defense”. Namely, the Constitution refers to internal security under term “security” and external security of the state under term “defense”. Both represent different levels of security and are mutually linked in an unbreakable unity, representing an equivalent of the term “national security”.

Today, national security incorporates the security of the state and the society, regardless of the ethnic, religious, racial and ideological background of its citizens. States allocate significant resources (human, material-technical and organizational) to protect all levels of security against different challenges, threats and risks. Security is a state of continual implementation, development and protection of the national and state interests that are achieved, maintained and improved through the system of national security and security mechanisms, for the purpose of achieving absence of individual and collective fear from threats, as well as creating a collective feeling of calm, safety and control over future events that are significant for the society and the state.

This requires the establishment and building of specialized security institutions based on laws in accordance with the Constitution, but also international conventions, resolutions, charters, treaties, recommendations, judgments and decisions by international courts. The national legislation should be based on international law, and therefore the international legal basis of the national security will be explained in more detail below.

1.2. International legislation on national and international security

The **Charter of the United Nations** is one of the fundamental international legal bases of national security. The aims of the United Nations listed in Article 1 of the Charter are: to maintain international peace and security and to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and interna-

tional law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace; to develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, to achieve international co-operation in solving international problems and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion.

The **Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States**, adopted in accordance with the Charter of the United Nations, promotes the ideas and values of the Charter of the United Nations, including, above all, the following: maintenance of international peace and security; development of friendly relations; cooperation and tolerance among nations; respect to the rule of law and obligations undertaken when signing international treaties.

In this context, the **Organization for Security and Co-operation in Europe (OSCE)** is largely significant. Namely, the final documents of the OSCE summits reaffirm the cooperation among states in the field of security, respect of human rights, democracy and rule of law; economic freedom, social justice and commitment to the environment; friendly relations among participating states; security on the grounds of reducing conventional armed forces and enhancement of mutual trust; guidelines for the future regarding the human dimension (human and minority rights and freedoms); culture and development; rights of migrant workers; enhancing the role of non-governmental organizations etc. OSCE's Lisbon Declaration of 1996 refers to a common and comprehensive security model for Europe in the 21st century. In this sense, the Declaration highlights the need for joint efforts in the challenges that affect the security and sovereignty of states and stability of societies. The 2003 OSCE Strategy to Address Threats to Security and Stability in the 21st century identified the most serious threats to security in Europe and mechanisms to fight these threats. The most serious threats involve conflicts in and among states and their links to terrorism, proliferation of weapons of mass destruction, excessive accumulation and uncontrolled spread of small arms and light weapons, human rights violations, deterioration of the socio-economic situation and illegal migration; terrorism; organized crime, especially smuggling of migrants and trafficking in human beings, illicit trafficking in narcotic drugs, in small arms and light weapons as well as in sensitive materials and technologies; discrimination and intolerance, especially xenophobia, racism, anti-Semitism and violent extremism; economic challenges and threats that endanger stability and security; environmental risks and threats, primarily the unsustainable use of natural resources, mismanagement of wastes and pollution etc. Furthermore, the Strategy includes strategic directions for prevention, mitigation of the effects from these challenges, risks and threats to security, through international cooperation among national security systems and a multidimensional approach to a common, comprehensive, cooperative and integral security.

On the other hand, the **Council of Europe** creates and advances its standards for oversight and lawful use of intrusive measures, but also oversight of the competences of law enforcement institutions, through its bodies: *Venice Commission*, *Parliamentary Assembly of the Council of Europe* and the *Office of the Commissioner for Human Rights*.

In this respect, the Council of Europe **Venice Commission** plays an important role in ensuring democratic control over security services. The 1998 Report on the Democratic Oversight of Security Services was the first document that refers to the introduction of oversight mechanisms of security services. Through other comprehensive reports, the Commission provides a comprehensive analysis of different forms and models of oversight of security services, including detailed conclusions on parliamentary, judicial and expert oversight of these services.

The recommendations are related to:

- enhancement of the capacities for control of the security services in the surveillance of communications;
- introduction of mechanisms for responsibility and establishment of an appropriate complaints mechanism.

In its reports, the Commission identifies the need for effective internal controls within the security services and the use of intrusive measures in line with the law, including control of police officers applying these measures, a procedure of ensuring a request for the use of intrusive measures in cases of protecting state security, and judicial oversight and training on human rights and democratic values of all stakeholders participating in the process.

Concerning parliamentary oversight, the Venice Commission recommends the parliament to have an exclusive jurisdiction to elect the members of the parliamentary body for oversight of the use of intrusive measures, without any suggestions from the executive. The composition of the oversight body should be bipartisan with fair representation of the opposition, as well as supporting staff having the proper expertise.

Regarding judicial oversight, the Venice Commission recommends the implementation of specialized training for judges on the approval and oversight of the use of intrusive measures for the purposes of national security.

The recommendations on expert oversight bodies note that the Parliament (not the executive) should appoint the members of expert bodies and review their reports. Any influence by the executive is reduced. Moreover, the report indicates that it is not sufficient to have oversight mechanisms only on theory, but also to have the adequate mechanisms and human capacities in place for their practical use. With regards to the oversight of security services, the 2015 Venice Commission report gives detailed recommendations on the safeguards and oversight of security services and the use of intrusive measures in untargeted surveillance and the use of metadata.

The **Parliamentary Assembly of the Council of Europe** also contributes to the legal framework for the oversight of security services in all member-states by adopting the principles for oversight of security services and the use of intrusive measures in the form of resolutions, recommendations and reports. The adopted recommendations of PACE (comprised of 47 states) focus on the establishment of specialized committees within the national parliaments for the purpose of improving the capacities of parliamentary oversight on the use of intrusive measures and the work of security services. The emphasis of the recommendations is put on the institutional cooperation and sharing of information among the security services of Council of Europe member-states.

The **Committee on Legal Affairs and Human Rights** focuses on the need to establish effective oversight mechanisms aimed at exchanging information among security services. This is especially important considering the volume of information sent and received by foreign partners.

The **Office of the Commissioner for Human Rights** has also adopted conclusions and recommendations for the oversight of the security services related to general surveillance of communications. In the recommendations, the Office of the Commissioner highlights the importance of respecting human rights within the use of intrusive measures by security services, for the purpose of establishing an efficient system for democratic oversight. The recommendations highlight the importance of the internal management of security services and their oversight and control, as noted in the Venice Commission recommendations. The Office of the Commissioner is competent to give individual recommendations for enhancement and observance of human rights, as stipulated in the European Convention on Human Rights for every member-state, from the aspect of strengthening the oversight of security services in using intrusive measures.

Regarding the **European Union**, the 1992 Maastricht Treaty is a serious project for justice and home affairs, EU's third pillar. More specifically, the provisions say the Union and its member-states define

and implement a common foreign and security policy with the aim of protecting the common values, fundamental interests and independence of the Union; enhancing the security of the Union and its member-states in all forms; maintaining peace and enhancing international security in accordance with the Charter of the United Nations, rule of law and respect of human rights and fundamental freedoms. The Union achieves these aims by establishing continuous cooperation among the member-states in implementing policies through information exchange and decision making in the Council on every issue of general interest in the field of foreign policy and security, aligning of national policies through common positions of the member-states in other international organizations, and implementation of joint activities by using procedures established in the provisions for the common security policy.

Macedonia is a member of the **Partnership for Peace of the North Atlantic Treaty Organization (NATO)**, but the signing of the Accession Protocol and the expected full-fledged membership in the Alliance imposes the need for greater alignment of the legal framework, procedures and practical operations in the field of security. The 1949 North Atlantic Treaty commits the member-states to a further development of peaceful and friendly international relations by strengthening their security institutions and elimination of conflict in their international economic policies and development of economic collaboration. For this purpose, the parties of the treaty are committed to maintaining and developing their individual and collective capacity to resist armed attacks, separately and jointly, by means of continuous and effective self-assistance and mutual support. An armed attack against one or more of them shall be considered an attack against them all.

As of 2010, NATO's new strategic concept highlights several issues: commitment to prevent crises, manage conflicts and stabilize post-conflict situations, mainly by working more closely with the United Nations and the European Union; open-door policy to all European democracies that meet the membership standards, because enlargement contributes to the goal of united Europe, increases the efficiency of NATO's defense from threats such as proliferation of nuclear weapons and other weapons of mass destruction and terrorism, conflicts beyond the Alliance borders, cyber attacks, threats from the use of laser weapons, electronic warfare, technologies etc. Finally, it point out the importance of the environment, natural resources, health risks, lack of water and rising energy needs.

2. Regional and international cooperation

The international security features swift, complex and dynamic changes and faces new asymmetric threats and risks on the rise, such as terrorism, transnational organized crime, proliferation of weapons of mass destruction, radicalism and extremism, illegal migration and cyber attacks.

Any challenges such as energy dependency and climate change can also have a negative effect on the international security. Taking into consideration the dimensions of contemporary threats and risks, the global approach and cooperation with the UN, NATO, EU and OSCE is a required instrument for successful management by each individual country, especially small countries such as RN Macedonia.

The cooperation with international security organizations - UN, NATO, EU and OSCE - ensures active participation in creating the global defense policy and improvement of the national capabilities for management of new threats, risks and challenges, along with more efficient management of civil and military capacities.

Our country is obligated to international cooperation because of numerous international documents ratified in the country's Parliament, such as the UN conventions suppressing acts of nuclear terrorism, suppressing terrorism financing, money laundering, search, seizure and confiscation of proceeds from crime and terrorism financing, as well as the Council of Europe conventions related to the same or similar areas of security and other criminal matters.

Fighting terrorism and organized crime is an exceptionally complex task that requires the undertaking of a series of specific measures and activities, including the alignment of mechanisms and procedures for inter-state data exchange, cooperation and undertaking of joint activities, especially those that are well established in EU and NATO member states.

With regards to the democratic norms and principles, and the observance of international law, our country takes part in the prevention and resolution of crises in cooperation with the international community, especially its partners, for the purpose of protecting its interests. In this regard, members of the Army of RNM are taking part in exercises and other activities within the Partnership for Peace Programme, as well as in humanitarian and peacekeeping missions organized and led by NATO.

The strategic partnership with the United States is of special importance for the security, stability and economic development of RN Macedonia and the region. The partnership with and the support by the U.S. has resulted in strong assistance in building the military capacities of the Army of RNM and significant contribution by the RN Macedonia in the global fight against terrorism. The further activities will focus on strengthening of the institutional capacities for identification and sharing of obligations arising from the NATO and EU membership.

The security services have to restructure and intensify their cooperation with the counterpart institutions of NATO member-states in the process of Alliance accession, by implementing the established standards for collection and exchange of data and information in the common interest.

The cooperation among security services incorporates the collection of data and information in the common interest or in the interest of one country. However, when it comes to a NATO member state, being an ally imposes the obligation to collect information for another country, if the person/s who pose a security risk are staying at the territory of our country. When assessed that the information cannot be collected by other means, but only by using special investigative measures - interception of communications, then the security service of RNM shall proceed in compliance with the regulations of the country. In such cases, the prosecutor's office and the court should assess any motions or applications as in other cases, but also take into consideration the existence of any regional and international security risks.

3. Role and position of the security-intelligence services in a democratic society

The term "security-intelligence services" refers to all counter-intelligence and intelligence, military and civilian services that are authorized by law to undertake measures and activities aimed at protecting the state's national security. They play an important role in the protection of national security and respect to the rule of law. Their main aim is to collect, analyze and transfer information that help national policy makers and other competent institutions in undertaking measures for protection of the national security and protection of people's human rights and fundamental freedoms. The functions of the intelligence services differ from country to country, but the collection, analysis and spreading of information that is relevant for the protection of national security is their essential task.

In fact, many countries restrict the role of their so-called secret services, in order to prevent them from undertaking other activities related to security that are already carried out by other state institutions and authorities. Many countries clearly define the activities of their intelligence services in laws, thus restricting their activities to the protection of the constitutional values related to national security.

The tasks and competences of the security-intelligence services that are precisely defined in a law, must be limited to protection of the legitimate interests of national security and any identified threats

to the national security that are supposed to be prevented by those services. In many European countries, (Romania, Germany, Croatia, Austria etc.) the laws precisely formulate and list all threats to national security, which facilitates the process of accountability, enabling the oversight bodies and legal protection authorities to control the intelligence services in the execution of their specific functions. In addition, many countries have adopted legislation that provides precise definitions on terrorism, terrorist groups and activities, which reduces the possibility of undertaking other activities against individuals and groups that do not represent a terrorist threat under the pretext of the fight against terrorism.

Security-intelligence services are state authorities and part of the executive with an obligation to respect the national legal system and international legal documents ratified by the country, especially those relating to human rights and fundamental freedoms. Therefore, if state security institutions breach certain provisions of the international law, they cannot justify it by national laws or other regulations. The idea of the rule of law requires from these secret services to refrain from undertaking any actions that could violate domestic and international law. In many states, the bylaws referring to the internal organization and systematization of the services, as well as the methods of implementing certain measures are secret, i.e. not accessible by the public, but accessible by controlling bodies.

Domestic laws should ban security services from engaging in any political activities or act in the interest of a certain political, religious, ethnic, social or economic group. States are also internationally responsible for the activities of their security-intelligence services and their staff, regardless of the location of these activities and the victims. The constitutional, administrative and international criminal laws treat the members of the security services as any other civil servant.

On the other hand, staff in the security services should be able to report certain irregularities or violations of laws in the operations of the service. Practice in some countries shows that there are several ways of reporting: to internal controlling departments within the service, to external oversight and controlling institutions, and by addressing the public. Any public disclosures of irregularities refer to severe violations such as death threats.

Institutional culture in the security services relates to the values, attitudes and conduct of staff. In fact, having only a legal and institutional framework cannot ensure that representatives of these services will abide by the rule of law and the respect of human rights.

A number of countries and their intelligence services have passed codes of ethics or principles of professionalism in order to promote their institutional culture. The codes of ethics usually include provisions for proper conduct, discipline and moral values that staff in the services have to demonstrate. A good practice is that codes of conduct be subject of control by internal and external oversight institutions.

The code of ethics must be accompanied by continual staff training for the purpose of professional enhancement. Many security services have training programmes that give emphasis to professionalism and educate staff over the relevant constitutional and legal standards, and international law. Professional ethics and culture can be enhanced through internal policies for human capital management and if ethical and professional behavior is rewarded.

The security-intelligence community of RNM is composed of three security-intelligence institutions:

1. National Security Agency;
2. Intelligence Agency; and
3. Organizational unit for military security and intelligence at the Ministry of Defense.

The National Security Agency (NSA) is an independent agency. By nature, it is a counter-intelligence, civilian service responsible for detection and prevention of espionage activities of foreign intelligence services, detection and prevention of threats, activities and operations against the constitutional order, detection and prevention of terrorism and other forms of serious and organized criminal activities against the state. It incorporates separate organizational units with a centralized hierarchical setup and linear-territorial operational methods.

The Intelligence Agency (IA) is an agency under the jurisdiction of the President of RNM, responsible for collection and processing of political, economic and military data about foreign states, institutions, services and persons of interest for Macedonia. It incorporates separate departments for fighting terrorism and organized crime. It is internally systematized in several organizational units, with a centralized hierarchical setup and linear-territorial operational methods.

The Organizational unit for military security and intelligence at the Ministry of Defense (the former military counter-intelligence and intelligence service), which represents a military counter-intelligence and intelligence agency within the Ministry of Defense, is responsible for detection and prevention of operations by foreign military-intelligence services in Macedonia, as well as for undertaking intelligence activities against foreign states and persons of interest for the country's national security. It is internally systematized in several organizational units, with a centralized hierarchical setup and linear-territorial operational methods.

There are separate units for use of intrusive measures in the NSA, IA, and the Ministry of Defense, especially with regards to the measures for interception of communications. Within these services, there are also units for monitoring and surveillance of persons and objects.

The security system of the RNM, which incorporates the security-intelligence community, faces a number of difficulties, one portion being a relic of the past, while the other a consequence of the insufficiently built legislative "architecture" related to the unambiguous establishment and separation of the jurisdiction of security services and their competences. The following anomalies have been detected in this regard:

- overstepping of legal competencies, i.e. security treatment of issues that do not fall under the jurisdiction of the proper service;
- abuse of intrusive measures as method of collecting indications;
- lack or failure to observe the existing mechanisms for elimination or reduction of the personal or content-wise non-selectiveness of measures for interception of communications etc.;
- there is some overlapping of competences within the security-intelligence community with regards to the subject and scope of work. It often occurs that certain events or phenomena, and certain domestic and foreign individuals whose activities have been classified as threats to the national security, emerge as the objects in focus of all three security services.

4. Intrusive measures as integral part of the working methods of the security-intelligence services

The measures for interception of communications are part of the range of secret means and methods of operation, which have been the exclusive right of the security-intelligence services, i.e. the secret services, for years. This exclusivity was due to the functional task of these services to protect the vital interests of the state. The protection of the state's vital interests can be successfully achieved only if the destructive threats are detected, identified and prevented in the early, preparatory stage, when there is no specific threat on the protected asset yet. The object of protection, which is in the

focus of these services, is not directly in jeopardy at this stage, but there are indications or a so-called abstract danger of its endangerment in the near or further future. This concept of pre-offence action that was characteristic only for the secret services, is now imposed as an obligation also for criminal services in charge of detection and prevention of organized crime and terrorism.

Therefore, it was natural to expect that the range of means and methods of operation by the secret services would be inevitably replicated and accepted as an instrument for legal operations of the criminal services as well, because this instrument has been adequate, efficient and verified for years in responding to the challenge of intercepting and preventing crime before it takes place. This legal instrument of pre-offence action is known in the criminal literature under different synonyms: *special investigative measures, undercover operations, special measures etc.*

The range of intrusive measures legally used by the security-intelligence services should and must comply with the generally adopted principles and standards of using intrusive measures.

Namely, security-intelligence services are part of the state executive, and as such, are not and cannot go beyond the system of control and observance of the generally accepted principle of the rule of law. The fight against terrorism, espionage and other subversive activities cannot turn into an instrument for termination of the democratic society.

Therefore, the application of the principles of legality, subsidiarity, proportionality and (prior) judicial approval of intrusive measures, as well as the adopted standards thereof, is compulsory in the work and operations of the security-intelligence services.

5. Prevention in security

The work of the security-intelligence services and the use of special measures for protection of the national security are based on the concept of acting in defense from any threats. Such a proactive concept of acting *ante delictum*, which is inseparably linked to the penal term of an “abstract threat”, incorporates the zone of pre-investigation, i.e. the zone of pre-criminal realization. By their nature, the measures are exceptionally suitable for interception of all activities that pose a threat to national security.

Unlike this proactive concept of action, the reactive concept of criminal persecution *post delictum* begins with the already perpetrated breach or endangerment of the protected asset, encompassing the preliminary stage of the criminal procedure, i.e. the investigation.

Therefore, the fear that the use of these measures poses a threat to erase the boundary between the investigation and pre-investigative procedure is entirely justified, which consequently creates “a threat that the substantive and procedural criminal law become, in a way, some kind of police-tactical instruments through the use of these measures.” (*Bacic F.: Criminal and legal aspects of organized crime, HLjKPP, 1/1999*)

In this case, the legislative sensibility is upped by the fact that the threat or the crime is in its earliest stage of preparation, in the broadest sense of the word, which is by rule unpunishable in principle. It incorporates operations and activities from the earliest stage of shaping the criminal intent, up to the operations and activities related to the preparation of the crime (inciting, organization, planning, preparation etc.). These early, pre-offence stages of the crime are, understandably, rarely sanctioned, and most of them remain in the realm of impunity, because the criminal intent of the perpetrator is still not demonstrating any forms of external reality, which represents, in the criminal-legal sense, a violation or at least a concrete endangerment of the protected asset.

In other words, there is no objective damage or endangerment of the protected asset, and the threat is still far away, in the form of an abstract, legally unpunishable threat. All information regard-

ing the suspect's threat of perpetrating a crime is in the sphere of assumptions, which by rule represents grounds for suspicion, sometimes even on a lower scale. Therefore, the legislator proceeds by using great caution and a high degree of selection when establishing the set of crimes for which these intrusive measures can be used, because of the real threat of criminal law entering the forbidden zone of punishing thoughts.

The fear that measures can be abused in this regard, thus legalizing the totalitarian regime and the political police, is real and omnipresent, but it seems that finding an efficient mechanism for control and oversight of their use can overcome this threat.

Security-intelligence services cannot affect the reasons for the security threats and risks, but can reduce the possible conditions and causes for activities aimed against the national security. The basic method for this is the use of an intelligence analysis, which represents the collection of data and information, their processing and drawing relevant conclusions regarding certain events or phenomena.

Incorporating prevention as an integral part of a comprehensive approach will help eliminate the prerequisites that might lead individuals into joining violent extremist groups, i.e. the preventive approach in the fight against threats to security and defense is oriented to "early signs". As with crime prevention, results are not immediately visible and require a long-term and patient engagement. Therefore, the use of special measures, interception of communications in this case, requires a longer period when it comes to security and defense, compared to their use in investigations of other crimes.

6.Threats to national security and defense

The Law on the National Security Agency (LNSA) and the Law on Defense list the threats to the security of the state.

According to Article 4 of the LNSA, the security threats (and risks) to the state's national security include the following:

- Espionage;
- Terrorism and its financing;
- Violent extremism;
- All forms of serious and organized criminal activities directed against the state;
- Prevention of crimes against humanity and international law;
- Illicit production and proliferation of weapons of mass destruction or their components, as well as materials and devices required for their production;
- Obstruction of the vital economic interests and financial stability of the state;
- Obstruction of the security of top office holders and facilities of strategic significance to the state; and
- Detection and prevention of other activities related to security threats and risks to the national security of the state.

According to the Law on Defense, the threats are the following:

- Detection and prevention of intelligence and other subversive activities of foreign military-intelligence and intelligence services in the country and abroad, aimed at the state's defense;
- Detection and prevention of all forms of terrorist activities aimed at the state's defense; and
- Counterintelligence protection of tasks and plans, documents, material-technical means, areas, zones and facilities in the interest of the country's defense.

According to the Criminal Code, these threats represent serious crimes against the state, armed forces, humanity and international law. The security forces undertake activities primarily for the pur-

pose of preventive actions in the event of preparation, organization or participation in crimes against the state's interests or disabling its security system in performing its functions.

In the enforcement of their legal competences, the security services can use secret measures and activities established by law and complying with the Constitution. The criteria for the use of the measures for interception of communications for the purpose of protecting the interests of state security and defense are clearly regulated in the Constitution and elaborated in detail in the Law on Interception of Communications and the LNSA.

7. Authorized institutions for implementation of measures for interception of communications for the purpose of protecting state security and defense

The authorized institutions for implementation of measures for interception of communications for the purpose of protecting the interests of security and defense of the state are the following:

- National Security Agency; and
- Ministry of Defense: Organizational unit for military security and intelligence in the Ministry of Defense (Military intelligence and security service), and the Center for Electronic Reconnaissance of the Army of North Macedonia, in the field of the frequency spectrum of radio waves of high, very high and ultra-high frequencies (HF, VHF and UHF).

The National Security Agency, being the only civilian counter-intelligence service, has the leading role in the use of the measures for interception of communications for the protection of national security. The agency is authorized by law to treat persons and phenomena from a civilian standpoint, i.e. it has no right and competence to treat persons and phenomena of military nature.

The Organizational unit for military security and intelligence at the Ministry of Defense, or the former military counter-intelligence and intelligence service, has no tradition of frequent use of the measures for interception of communications, but has a continual and frequent use of the so-called reconnaissance, i.e. military-radio intelligence in the field of the frequency spectrum of radio waves of high, very high and ultra-high frequencies.

According to LIC and LNSA provisions, the measures for interception of communications encompass all forms of communication: telephone or so-called wired communication, direct or so-called oral communication, all forms of electronic communication, and letters and postal packages as a form of communication among people. The measures relate to both national and international telecommunications traffic.

The law allows for the use of special technical means of interception (so-called bugs) that can have a short-term or longer-term lifespan (depending on the charging source) and they are most commonly used for "wiring" of an enclosed area where the person of security interest is staying or working.

Regarding the so-called personal or consensual interception of communication, the current LIC, unlike the one of 2006 (Article 2) has no provisions that explicitly regulate this matter. Namely, according to the existing provisions and legal perceptions, the essence of the constitutional ban for unlawful interception of communications aims to prevent and ban unlawful state intrusion in the citizens' private communications, while in personal communication, each participant in the communication bears the risk that the conversation could be recorded without his/her consent or knowledge by the other participant in the communication.

Although there is no explicit provision that would ban the recording of the content in personal communications without the consent of the other participant in the communication, the law does

not accept such intercepted conversations as evidence in the procedure, because they had not been previously approved by the court. On the other hand, besides the violation from a moral standpoint (betrayed trust), the participant of concern in the communication can also hold the other participant in the communication criminally responsible if the published conversations contain data about the private and family life of the person concerned.

The same goes for any consensual interception of communications, i.e. interception of communication without a court order, but with a prior consent of one participant in the communication. Namely, the law does not allow it but leaves room for acceptability, if the person is an undercover police investigator (member of the service or a police collaborator), but such an acquired knowledge shall have no court value, but only operational significance.

The law (LIC) allows, for the purpose of protecting national security, for a more liberal approach and use (without judicial approval, but only at the request of an authorized institution and subsequent notification of the Chief Public Prosecutor of RNM) of the meta data of the participants in the electronic communications traffic, which, besides the measures for interception of communications, is one of the most commonly used tools in the work of the security-intelligence services.

8. Measures for interception of communications

Based on Article 18 of the Law on Interception of Communications, the measures for interception of communications for the purpose of protecting the interests of state security and defense include the following:

1. Interception and recording of telephone and other electronic communications;
2. Interception and recording of the interior of facilities, closed premises and objects, and the entrances of those facilities, closed premises and objects in order to create the necessary conditions for the measure's implementation;
3. Interception and visual recording of persons in open spaces and public areas; and
4. Interception and audio recording of the content of communications of persons in open spaces and public areas.

The measure of point 1 - Interception and recording of telephone and other electronic communications - relates to all communications that represent a technical process of sending, transmitting and receiving any type of speech, data, sounds, signals, written text, static or moving images, and which serve to exchange information among people, between people and objects, among objects, or for the purpose of guiding any object with the help of a telecommunications system, as well as internet protocol, voice over internet protocol, website or e-mail. This measure does not incorporate direct oral communications, i.e. the so-called ambient surveillance between people, letters and postal packages as separate forms of communication between people.

By content, the measure relates to the same communications incorporated in the measure of Article 252 Paragraph 1 Item 1 of the LCP, *differentia specifica* being the aim and conditions for the measure's application. Namely, with regards to the aim (Article 18 of the LIC and Article 34 Paragraph 1 of the LNSA), the measure is intended to protect the interests of state security and defense, while regarding the conditions, the measure is preventive and incorporates:

- The stage of pre-criminal realization - preparation, for crimes against the state, armed forces or humanity and international law;
- Prevention of a specific threat that represents, in a criminal-legal sense, inciting, organizing or participating in an armed attack against the state or disabling a security system from carrying out its functions; and

- Prevention of an abstract threat that, in the criminal-legal sense, represents the existence of grounds for suspicion on already undertaken activities referring to crimes: terrorist organization (Article 394a), terrorism (Article 394b) and financing of terrorism (Article 394c).

The legislator makes a distinction (Article 4 Paragraph 1 Item 4 of the LIC) between the interception and recording of telephone and other electronic communications for the purposes of the criminal procedure of Article 252 Paragraph 1 of the LCP, calling this measure – Special investigative measure and the same measure when it is intended for the protection of the national security and interests (Article 4 Paragraph 1 Item 5 of the LIC), when the same measure is called – Interception and recording of telephone and other electronic communications. In fact, this is an identical measure by its nature, aimed at secretly acquiring the content of the targeted communication, but with a different title from a legal standpoint due to the different purposes of its use.

The measure for interception and recording of telephone and other electronic communications provided for in the Law on Interception of Communications can also be implemented with the support of special technical devices and equipment that enable the measure's implementation without OTA and the operators as intermediaries. However, the measure's implementation can only be carried out when it is technically impossible to intercept and record the content of the communication without using OTA's special technical devices and equipment.

Malicious software (malware) represents a technical intrusion in the electronic system of the person concerned, enabling the monitoring of all forms of telephone and electronic communications of the person concerned through his or her electronic device. According to its scope and sphere of intrusion in privacy, it is an *online* interception of all communication of the person concerned through his/her electronic device.

For the purpose of using this special technique, the legislator has prescribed a consistent observance of the principles of prior judicial approval, legality, proportionality and subsidiarity.

The manner of use, control and application of the special technical equipment is regulated by the provisions of the LNSA, whereas the NSA director regulates, by means of a bylaw, the specification and technical features of the devices and the equipment, as well as the manner of their storage and handling.

The measure of point 2 - Interception and recording of the interior of facilities, closed premises and objects, and the entrances of those facilities, closed premises and objects in order to create he necessary conditions for the measure's implementation – is a counterpart of the measure of Article 252 Paragraph 1 Item 2 of the LCP. A *Differentia specifica* of this measure, besides the purpose and the conditions, is the enlargement of the scope of the measure's application to all types of enclosed spaces, both public and private. According to its scope and sphere of intrusion in one's privacy, the measure relates only to direct (but not indirect) electronic and other communications, oral communications (the so-called ambient surveillance) that are carried out in an enclosed area. Considering that the conditions for the measures' application for the protection of the interests of state security and defense are regulated by the LIC (Article 19), the enlargement of the scope of the measure's application also has repercussions in respect of the restrictions of the use of the special investigative measures (Article 268 of the LCP). Namely, *de legelata*, the measure can also be applied in the home of another person without asking for a degree of a reasonable suspicion that the suspect resides there.

The measure of point 3 - Interception and visual recording of persons in open spaces and public areas – represents a form of secret surveillance of the suspect in a public space using special technical means for visual recording (infrared, UV or other rays such as night vision, thermal vision etc.), which aim is not, by rule, the content of the suspect's communication, but (the external developments of the 'facility' under observation) the meetings and contacts of the suspect with other persons and places of movement.

According to its nature, this measure is more similar to the measure of Article 252 Paragraph 1 Item 3 of the LCP (secret observation), rather than to the measures for interception of communications. However, sometimes, based on such observation of the suspect, when he/she is farther from the visual field, one can get conclusive (direct) knowledge about the “content” of the suspect’s communication (movement to a certain target, handover of items, sign movements or mimics etc.) with other persons.

The measure of point 4 – Interception and audio recording of the content of communications of persons in open spaces and public areas – is a counterpart of the measure of secret surveillance and recording of persons and objects using technical means outside residences and offices designated as private (Article 252 Paragraph 1 Item 2 of the LCP) and only refers to audio interception and recordings (as the only difference to the previously cited measure) of communications in a public space with the assistance of special technical means for sound enhancement, ensuring the “capture” of the target communication from a larger distance. Of course, the measure is undercover, i.e. implemented in an inconspicuous way and the person concerned is not aware that he/she is being “listened to”. The measures for interception of communications in open spaces (and public places) are most commonly not banned due to the generally accepted position that the person concerned, based on the circumstances under which the communications is carried out, has no reasonable expectation of privacy. In other words, each person bears his or her own risk of communication privacy if it is conducted in an open space, where the number of persons having access is unlimited.

Besides the above mentioned measures for interception of communications for the purpose of protecting the interests of state security and defense, pursuant to the provisions of the LIC (Articles 32 and 33), upon a request by the authorized institutions for the measures’ implementation (the Chief Public Prosecutor of the RN Macedonia is informed about the request), the operators must submit the required metadata related to the participants in the electronic communications traffic.

NSA has the exclusive right, based on a court order (Articles 25, 28 and 32 of the LNSA) to carry out interception and recording of international telecommunications, with operators as intermediaries, when the interception of international telecommunications cannot be implemented by other means, and at the same time conduct oversight on postal and other shipments.

8.1. Criteria for use of measures for interception of communications

The legal basis, criteria, types of measures for interception of communication and the procedure of their use, for the purpose of protecting the interests of state security and defense, are clearly defined in the Constitution, LIC and LNSA. The constitutional provisions in Article 17, i.e. Amendment XIX (2003) define the legal grounds, scope and sphere of legitimate concessions from the constitutional guarantee over the inviolability of citizens’ communications privacy.

Some of the constitutional ambiguities in the Constitution of RNM regarding the use of intrusive measures are being complemented by the provisions of the ratified ECHR as the general legal framework and guideline for all aspects related to the use of these measures.

The Law on Interception of Communications (Chapter III) defines the criteria, procedure and types of measures for interception of communications for the purpose of protecting the interests of state security and defense.

Considering the controlling role of the court, it must take into account the ECtHR case law on the standards of using intrusive measures, in order to avoid the danger of their abuse and undermining the democratic order, under the justification that such actions are undertaken for the purpose of its protection.

8.2. Criteria for issuing an order

The criteria for issuing an order for interception of communications are provided in Article 19 of the LIC (identical provisions are also part of the LNSA). Paragraph 1 of this Article reads “the court can order measures for interception of communications of Article 18 when there are grounds for suspicion that the perpetration of a crime against the state, armed forces or humanity and international law is being prepared”.

De legelata, the law “requires” the existence of grounds for suspicion over the use of the measures and covers (only) the stage of preparatory actions for crimes against the state, the armed forces or against humanity and international law.

Article 19 Paragraph 2 of LIC also stipulates the use of the measures for the purpose of preventing actions (preemptive action), which in the criminal-legal sense would be classified as preparation, incitement, organization or participation in an armed attack against the state or disabling its security system from performing its functions, and for the purpose of preventing any activities related to the crimes of terrorist organization (Article 394a), terrorism (Article 394b) and terrorism financing (Article 394c). In the same paragraph, the law “requires” the unconditional fulfillment of the principle of subsidiarity, i.e. information on such activities cannot be collected by other means or their provision would cause great difficulties, and cumulatively, the law requires the existence of an already “established” direct threat from the execution of (any of the abovementioned) crimes, armed attacks or disabling security systems.

Paragraph 3 of the same article gives the possibility of choosing between the myriad of measures for interception of communications while always giving preference to the measure that least infringes the human rights and fundamental freedoms regulated by the Constitution, the law and international treaties ratified in line with the Constitution.

8.3. Request for issuance of an order and deciding on the request

Considering the seriousness of the protected asset, the legislator puts this measure at a higher level, both in relation to the applicant and the authorized institution, and is therefore laid down in a separate chapter of the Law, i.e. Chapter III – Criteria and procedure for implementing measures for interception of communications for the purpose of protecting the interests of state security and defense. Based on the provisions of Article 20 Paragraph 1 of the LIC, the Chief Public Prosecutor of the Republic of North Macedonia is the authorized person to file a request for issuance of an order for implementation of a measure for interception of communications for the purpose of protecting the interests of state security and defense, at the proposal of the NSA Director or a person authorized by him or her, or at the proposal of the Defense Minister or a person authorized by him or her. The content of the request referred to in this article requires the following compulsory elements:

- Type of the measure for interception of communications for which the request is filed;
- Information on the individual or legal entity targeted by the measure;
- Information on the facility, space or item that is targeted by the measure;
- The institution in charge of the order’s implementation;
- Explanation of the reasons and the need for implementation of the measure;
- Duration of the measure; and
- Type of telecommunications system, telephone number or other identification data, and the identification number for each of them individually.

There are differences in the content of the Request for a measure for interception of communications for the purposes of the criminal procedure (Article 8 of LIC) and the Request for issuance of an

order for interception of communications for the purpose of protecting the interests of state security and defense (Article 20 of LIC).

The requests for issuance of an order for interception of communications for the purpose of protecting the interests of state security and defense should not include data on:

- Legal title of the crime;
- Scope and location of the special investigative measure's implementation; and
- Information and evidence that establish the grounds for suspicion and reasoning why data and evidence cannot be collected by any other means.

In case of filing a request as referred to in Article 20 of the LIC for issuance of an order for multiple measures for interception of communications, it is compulsory to specify data for each measure separately. The Chief Public Prosecutor of the Republic of North Macedonia files the request with a Justice of the Supreme Court of the Republic of North Macedonia, designated by the court's internal schedule, who is obliged to make a decision immediately or within 24 hours from the request's submission at the latest.

By exception, in urgent cases and when there are threats of possible delays, upon a request by the Chief Public Prosecutor, the Supreme Court Justice can immediately issue a temporary written order for enforcement of the measure for a period of 48 hours (Article 30 Paragraph 1 of LIC). The judge submits the temporary written order and the anonymized copies of the written order for OTA and for the purpose of oversight and control to the Chief Public Prosecutor of the Republic of North Macedonia, who then delivers them to OTA through an authorized person in the authorized institution that petitions for the measure. If the petitioner is the Chief Public Prosecutor of RN Macedonia himself, then he submits them to OTA.

The authorized person in OTA must proceed immediately (Article 64 of LIC) and do the following:

- a) Activate and make available the communication for which the order has been issued;
- b) Stop the implementation of the measure for interception of communications in cases when the duration of the measure has expired or an order for the measure's termination has been issued.

Regarding the decision making on the Request of the Chief Public Prosecutor of the Republic of North Macedonia, the law (Article 21 of LIC) provides for a two-instance procedure. Namely, if the judge does not approve of the Request, the Chief Public Prosecutor of the Republic of North Macedonia has the right to a complaint to the Supreme Court of RN Macedonia within 12 hours from the notification on the disapproval. A chamber of three judges of the Supreme Court of RN Macedonia, not including the judge who disagreed with the request, rules on the complaint within 12 hours from its submission.

8.4. Justification of the use of measures for interception of communications

When deciding on the issuance of an order for the measures for interception of communications for the purpose of protecting the interests of state security and defense, the Justice of the Supreme Court of RNM or the chamber of three judges should possess sufficient theoretical and practical elements (assumptions, information) that would help determine the significance of the direct and specific harm to national security. In the context of deciding on the order, the minimum security information and assessments by the security services that are accepted by the Chief Public Prosecutor of RNM, which might be abstract in many cases and never become reality, are sometimes sufficient for the judge to accept the request and issue the order, if the expected threat and the asset that is protected prevail over the right of the individual's privacy due to their importance and priority.

Naturally, the purpose for which this intrusive measure has been established, and the protected asset, leaves more maneuvering room to the law enforcement authorities to unsubstantially and

routinely appropriate measures, even by abusing them, with the judge facing a *fait accompli*. However, considering the role of the court as a controller of the use of intrusive measures, the judge is not deprived of a possibility to make a relevant assessment, having in mind all elements that must be contained in the request for interception of communications submitted by the Chief Public Prosecutor of RNM must contain. On the contrary, the judicial authorization for approval of intrusive measures is considered as an important principle and significant preventive protection from unjustified endangerment of the privacy of individuals and abuse of the discretion authority of the state, but this cannot, by itself, ensure full protection from excessive use of these measures.

When assessing issues related to the national security and defense of the state, the court and the judges should be guided by the following criteria and rules:

- in case of assumptions, the individual right should always be favored (*in dubio pro reo*);
- the request for the use of measures for the purpose of protecting national security should be accepted and reviewed by using critical and healthy skepticism;
- development of professional cooperation and support between the security-intelligence services (especially the National Security Agency) and the prosecutor's office;
- the request must argue a direct, immediate, severe and specific harm to the national security;
- the requested restriction of the privacy of the person concerned must be carried out in stages, starting from a lesser to a larger intrusion of the individual's privacy;
- whenever possible, judges should formulate and apply strict and swift rules instead of a loose "balancing test". This especially refers to the profile of the subject targeted by the measure, data about the facility, space or item for which the measure is implemented, observing, at all times, the civil rights guaranteed by the Constitution and the international standards for use of intrusive measures.

Judges should insist, to a reasonable extent, to be sufficiently informed about the facts of the case, the assessed relevance, the validity of the claims in the request and about the possibilities of collecting the targeted information in a different way.

Moreover, every request for a court order should include an explanation and reasoning that the proportionality principle (besides the subsidiarity principle) has been observed, showing that a proper balance has been established between the issues of national security and the scope and sphere of intrusion in the human rights and freedoms.

These principles indicate that it is of enormous importance, when deciding, to present the judge with the relevant reasons for the use of the measures and explain why data and evidence could not be collected by other means, or why the other means of information collection would endanger the life or health of people. This fact, besides the other presented facts, has an indirect effect on the judge's decision when assessing the justification of the Request for issuance of an order for interception of communications. This is why the measures for interception of communications, as *ultima ratio*, help the grounds for suspicion to turn into a reasonable suspicion for organized crime offenses and other specifically listed crimes.

8.5. Content of the order for interception of communications and its anonymization

According to Article 22 of LIC (identical in Article 37 of LNSA), **the order for implementation of a measure for interception of communications for the purpose of protecting state security and defense incorporates the following elements:**

- Type of measure for interception of communication for which a request is submitted;
- Information about the natural or legal person who is targeted by the measure;
- Information about the facility, space or item that is targeted by the measure;
- Name of the institution in charge of the order's implementation;
- Explanation of the reasons and need for implementation of the measure;
- Duration of the measure; and
- Type of telecommunications system, telephone number or other identification data, and the identification number for each of them individually.

Regardless of the prescribed minimum elements of the request and the court order for interception of communications, the national legislation requires additional elements both for the request and the court order, for the purpose of aligning them with the standards developed through the ECtHR case law. In this regard, some of the more important issues that deserve the judge's attention and help him/her make a valid decision on the request for the use of the measures are the following:

- Legitimate purpose of the measures and whether it is necessary in a democratic society;
- Legal grounds for the use of the measures, seen through the prism of the domicile law, but also international principles and standards, especially the ECtHR case law.
- Does the request specify any circumstances that point to the consistency in the observance of the principles of subsidiarity and proportionality before the proposal of the measures;
- Quality of the specified grounds for suspicion, i.e. the reasonable grounds for credibility and relevance of the presented facts that justify the request for the use of the measures;
- Is it possible to guarantee the unambiguousness in the interception of communications when using the measures, i.e. is it possible through those measures to establish a so-called mass surveillance of people's communications.

The court can always ask the petitioner of the request for the intrusive measure for additional information, clarifications and explanations prior to deciding. The additional information can be delivered to the court in written or be presented orally during a hearing in a room that is closed to the public.

Holding a hearing in a room closed to the public can be appropriate when the security-intelligence agency wants to protect the source of information as an exchange of intelligence information with foreign partners and the judge should assess whether the source of information is sufficiently credible. The court may also schedule a hearing in a room closed to the public when an urgent procedure by an authorized institution has been initiated.

8.6. Anonymization method

The method of anonymization and recording of orders in the court register is prescribed by the Justice Minister in a Rulebook on the method of anonymization for implementation of the measure for interception of communications for the purpose of protecting the interests of state security and defense and the manner of recording in the register of anonymized orders (Official Gazette no.200 of 1 November 2018).

According to Article 22 of the LIC, the Justice of the Supreme Court submits the order for implementation of the measure for interception of communications along with the anonymized copies of the order to the Chief Public Prosecutor of RNM, who then submits the order to the authorized person in the institution that proposed the submission of the request to the Supreme Court Justice.

The authorized person submits the anonymized copies of the order referred to in Article 21 of LIC to the authorized person in OTA.

Pursuant to the LIC, the judge issuing the order for implementation of the measure for interception of communications is anonymizing it immediately upon its issuance, making copies as follows:

- one copy of the anonymized order for OTA; and
- two copies of the anonymized order for oversight and control, one of which for OTA and the other for the authorized institutions.

The copy of the anonymized order for OTA differs from the anonymized copy for oversight and control because the elements that remain visible in these two types of anonymized orders differ.

8.6.1. Anonymization of the order for OTA

The anonymization of the order for OTA is carried out by the judge in a way that all elements in the order, with the exception of the elements that the order must include in accordance with the law, are replaced by the “X” sign.

Example: data on the individual “Petar Petrovski”, birth registry number, or data on the legal entity “Skopje DDOEL” that is targeted by the measure, or data on the facility, space or item that is targeted by the measure, are replaced by the “X” sign.

After the anonymization by the judge who issued the order, the anonymized copy of the order for OTA contains only the data established by the LIC as follows:

- Number of the order;
- Duration of the measure; and
- Type of telecommunications system, telephone number or other identification data, and the identification number for each of them individually.

8.6.2. Anonymization of the order for oversight and control

The anonymization of the order for oversight and control is carried out by the judge in a way that all elements in the order, with the exception of the elements that the order must include in accordance with the law, are replaced by the “X” sign.

Example: data on the individual “Petar Petrovski”, birth registry number, or data on the legal entity “Skopje DDOEL” that is targeted by the measure, or data on the facility, space or item that is targeted by the measure, are replaced by the “X” sign.

After the anonymization by the judge who issued the order, the anonymized copy of the order for oversight and control contains only the data established by the LIC as follows:

- Number of the order;
- The duration of measure; and
- Identification number.

The Rulebook on the method of order anonymization does not provide the manner of anonymization of the order’s reasoning, as stipulated for the anonymization of other decisions, rulings or judgments. The reasoning also includes data by which the subject could be directly or indirectly identified, and this data in the section of the order’s reasoning should therefore be replaced by “X”.

8.6.3. Recording in the Order Register

Anonymized copies of the orders are recorded in the Order Register by number and date.

For the purpose of oversight and control, the judge who issued the order and the authorized person in OTA record the date and number of the anonymized copy in two separate registers in the court and OTA.

The recording in the Order Register is carried out by:

- The judge, at the time of the issuance of the anonymized order to the authorized person in OTA and the anonymized order for oversight and control; and
- The authorized person in OTA upon reception of the anonymized copy.

The provisions of the Anonymization Rulebook are applied accordingly for issued temporary written orders for implementation of the measure for interception of communications, when proceeding in urgent cases as referred in Article 30 of LIC.

8.7. Duration and extension of the measure for interception of communications

The measure of interception of communications should be as short as possible. In this context, Article 24 of the Law defines the general framework. Paragraph 1 of the same article initially uses the wording “the necessary time” but limiting it to “no longer than six months“. The wording “the necessary time” in Article 26 of the LIC gives the judge a possibility to order the extension of the measure for interception of communications, but for not longer than six months, with the option of further six-month extensions up to two years, including the period covered by the first order for the measure.

Article 26 of the Law in Interception of Communications regulates the procedure for extension of the measure of interception of communications. Regarding the specific procedures it is especially important that each of the authorized institutions proceeds towards establishing the real necessity for its extension. The public prosecutor must first establish the necessity of the measure’s extension when assessing the proposal of the authorized institution implementing the measure, considering the reasons for such an extension through an analysis of the achieved results presented in the report by the authorized institution in line with Article 27 of the LIC, which should provide the expedience of its extension.

When deciding on the request by the Chief Public Prosecutor of RNM for the measure’s extension, the Supreme Court Justice first decides on the necessity of its extension and can extend it based on the reasoning provided by the public prosecutor in the request for extension of the measure of interception of communications and the reports from the authorized institutions. The judge should always be guided by the wording “the necessary time” as the main principle, and based on the expected effects within the determined timeframe, again observing the limitation that the measure should not last for more than six months (Article 26 Paragraph 3 of the Law on Interception of Communications). Here, the legislator also provides the option, in case of expressed disapproval by the judge, upon objection, the decision to be made by a chamber of three Supreme Court judges, in line with Article 21 Paragraph 3 of the Law on Interception of Communications.

It is questionable whether the law ensures sufficient quality in the sense of predictability, because it allows for expansion “when necessary”, which is a vague term, and because it is not explicitly defined whether the extension is allowed only once or on numerous occasions (*Szabo and Vissy v. Hungary of 12 January 2016*).

Therefore, the court should use caution when carrying out its jurisdiction in deciding on the extension of the intrusive measure. Namely, it is recommended that the general criterion for the extension incorporate the following:

- a. Existence of a reasonable expectation that additional information would be obtained by extending the measure that is necessary for protection of the democratic institutions;
- b. Existence of justified reasons that had prevented the collection of the required intelligence information during the previous period of the intrusive measure's duration;
- c. The practice of extending the intrusive measure to be approved for a shorter period than the one requested (for example: by one month instead of a longer period);
- d. Compulsory submission of a report on the achieved objectives from the prior use of the intrusive measures as an attachment to the request for their extension;
- e. Conducting continual or unannounced control with direct access to the transcripts from the intercepted communications.

8.8. Reports

The authorized institution prepares and submits a report on the implementation of the measure for interception of communications once in three months from the start of the measure's implementation to the Chief Public Prosecutor of the Republic of North Macedonia.

Besides the compulsory reports submitted once in three months, the authorized institution also submits a report when the Chief Public Prosecutor of the RNM requires this, and also after the expiry of the period allowed for implementation of the measure for interception of communications. The Chief Public Prosecutor of RNM submits the reports from the authorized institution to the Supreme Court of RNM.

8.9. Termination of the measure for interception of communications

The measure is terminated after the expiry of the period for which it had been issued.

Considering the aims and reasons for the measures for interception of communications, the legislator established the reasons and situations when the measure is to be terminated. Hence, it shall be terminated when the aims for which it was issued are achieved or when the grounds for its issuance cease to exist.

In addition, Article 25 of LIC regulates the procedure of terminating the measure and the specific competences of the three stakeholders involved in the procedure. According to this Article, as soon as such a request is submitted, the judge should immediately order the public prosecutor to terminate the measures and the public prosecutor forwards the order to the authorized person who then delivers it to the authorized person in OTA. The authorized person in OTA must immediately proceed upon the order for termination of the measure, in line with Article 64 Paragraph 1 Line 2 of the LIC.

9. Urgent procedures

By exception, in urgent cases, when there are threats of delays, the Supreme Court Justice can immediately issue a temporary written order for implementation of the measure of Article 18 Item 1 of LIC, for a period of 48 hours.

In this context, in Article 30 of the LIC the legislator stipulates the term acting in emergencies as a situation involving a threat of delay, without defining specifically what a threat of delay means. However, in this case and considering the previous positions regarding "acting in urgent cases", judges

are guided by certain rules (analogy) that are already established in other legislative branches and relate to the assessment of the state of urgency. In cases when measures are undertaken for the protection of national security, the aims of the measures can be used as an additional element when assessing the urgency.

Thus, considering the aims of this measure and the institutions implementing these measures, the judge can recognize them in practice as activities directed at prevention of a possible threatening act on the vital security segments on one hand, or when intercepting perpetrators of crimes, i.e. preventive action in relation to activities regarding crimes from the Criminal Code such as terrorist organization (Article 394a), terrorism (Article 394b) and terrorism financing (Article 394c), when urgency is necessary in a specific situation.

The feature of the urgency is that the measure can be issued immediately and is limited in time to 48 hours. It needs to be highlighted that the Supreme Court Justice issues such temporary orders in writing, based on a written request by the Chief Public Prosecutor of RNM, who is proceeding upon a reasoned and written proposal submitted by any of the authorized persons.

Article 30 of the LIC regulates the detailed procedure for the issuance of this measure and the procedures to be followed by the authorized institutions, including OTA, as well as the content of the order, the data anonymization and the recording in the order register.

The judge submits the temporary written order and the anonymized copies of the issued written order for OTA and for oversight and control to the Chief Public Prosecutor of the Republic of North Macedonia, who forwards them to the authorized person in the authorized institution, who then delivers them to OTA. The authorized person in OTA must proceed upon the order immediately.

The Justice of the Supreme Court issues the temporary written order based on a written request by the Chief Public Prosecutor of RNM, who is proceeding upon a reasoned written proposal, submitted by the authorized person of the authorized institution.

The temporary written order referred to in Paragraph 1 of this Article contains the same data as in any other order issued in a regular procedure. The judge carries out the anonymization of the temporary written order in the same manner and form like for any other order issued in regular procedure. This includes:

- An anonymized copy of the order for OTA; and
- An anonymized copy for oversight and control.

The data anonymization in the temporary written order is done by the judge who issued the order.

If it is assessed there is a need to extend the period for implementation of the measure for interception of communications, a procedure is carried out prior to the expiry of the deadline in the same manner and form as for the requests for extension of the measures for interception of communications issued by an order in a regular procedure.

10.Storage and disposal of data collected using measures for interception of communications

Article 29 of the Law on Interception of Communications regulates the storage and disposal of data collected through the implementation of the measure for interception of communications in the procedure of implementing measures for interception of communications for the purpose of protecting the state interests. According to the provisions of this Article, any data collected and processed through the execution of an order for implementation of measures for interception of communications, and when the data is believed to be significant for the implemented measure, it is stored at

the authorized institutions for the measures' implementation in accordance with the regulations for protection of personal data and classified information, for a period of three years from the expiry of the period defined in the order.

However, if it is established that there is new information directly related to the specific data for which the storage period has still not expired, the period of 3 (three) years can be extended. In such an event, the law provides for a periodical assessment of the necessity to store specific data, once a year, which establishes whether the collected data is significant for the aims of the implemented measure for interception of communications. If the results of the assessment show that the collected data is not significant, it is destroyed, while the method of establishing the relevance of data and the method of their destruction is regulated by special Rulebooks prescribed by the Defense Minister and the Minister of Interior. Moreover, such a Rulebook should also be adopted by the new National Security Agency.

The following should be considered as data collected and processed through the execution of an order for implementation of measures for interception of communications for the purpose of protecting the interests of state security and defense, in the sense of the abovementioned rulebooks:

- contents of the intercepted communication and data related to the communication in an unambiguous way;
- only contents of the intercepted communication;
- only data related to the intercepted communication;
- transcript of the contents of the intercepted communication in full (word for word) or summarized (with a description of the contents of the communication). Transcripts can be either in hardcopy or in electronic form.

Electronic data obtained from interception of communications can be found in the Law Enforcement Monitoring Facility (LEMF) or transferred at any storage medium (CD, DVD etc.) or transferred and stored in any other electronic system (document management system) located in an institution authorized for interception of communications and managed by the institution authorized for interception of communications.

The relevance of data obtained through interception of communications is assessed and determined by an employee of the Military Service for Security and Intelligence within the Ministry of Defense (hereinafter Service) who is working on the case and initiated the proposal for an order for implementation of the measure for interception of communications, for which he drafts a report, or by an employee in the Mol who is working on the case and initiated the proposal for an order for implementation of the measure for interception of communications, for which he also drafts a report.

If assessed that the data is significant for the implemented measure, it is stored until the end of the period defined by the order for implementation of the measure for interception of communications, in compliance with the regulations for protection of personal data and classified information.

According to both rulebooks, the Mol and the MoD set up Committees to establish whether data collected by implementing SIMs are of significance for the measure, so that it is stored for three years after the expiry of the period determined by the order for implementation of the measure for interception of communications.

A Committee assesses the possible extension of the deadline for storage of data collected by the measure for interception of communications for a period of one year, with a possibility of a further extension for the following year, with the deadline extended by a period of three years in total at most (Article 21 of both rulebooks).

After the expiry of the deadline for storage of data collected by implementing the measure for interception of communications, the data and all materials related to the enforcement of the order for implementation of the measures for interception of communications are destroyed by the Committee in the MoI or MoD. The Committee carries out the destruction of data and all materials related to the enforcement of the order for implementation of the measures for interception of communications under the supervision of a Justice from the Supreme Court of the Republic of North Macedonia, designated by the court's internal schedule for order issuance, in a manner and under conditions as regulated by law. Any electronic data stored in electronic equipment is destroyed by erasing their physical and logical locations by using a proper interface and programming support installed in the equipment by the manufacturer. The destruction can be carried out from a work station or other terminal connected to the equipment or installed in the equipment by the manufacturer.

The committee tasked with the destruction cannot have or ask for other direct or indirect access to the physical or logical location of data in the electronic equipment.

An electronic record (log) remains in the electronic equipment about the data that has been erased, when they were erased, who carried out the erasing and what was the basis for the erasing. The electronic record also stores the record number of the data that has been erased, if the technical capacities provide such an option. Electronic data in portable media is destroyed through physical destruction of the data holder within the portable medium.

Depending on the structural complexity, the medium can be disassembled to its components (hard disc or USB) in order to destroy the component where the data is stored in a way that would prevent reassembling of the medium or leave a possibility for restoration and use of the destroyed data.

Hardcopy data is destroyed by paper cutting machines or shredders in a way that prevents the pieces to be fully reassembled to make data readable.

The Committee makes a record of the destruction, which registers only the number of the court order. The record is drafted in two copies (one copy each for the court and the petitioner of the request for monitoring of communications) and is kept for 10 years.

11. Obligation for keeping official secrets

Article 31 of the LIC regulates the obligation for keeping official secrets for persons from the authorized institutions for implementation of the measures for interception of communications, persons from OTA or persons from the operators, who get familiarized with data related or arising from the implementation of measures for interception of communications.

According to the provisions of this Law, the person is obligated to keep as an official secret i.e. as classified information all data arising from the measure of interception of communications, unless it has been illegally collected. In that case, the person must immediately inform the authorized public prosecutor. The person is obligated to keep the official secret related to the data he/she obtained during the implementation of the measure for interception of communications for the duration of his/her tenure or employment, as well as for a period of 5 (five) years after their termination.

The obligation of keeping official secrets refers to the type of data as referred to in Article 29 of the LIC, i.e. data collected and processed through the enforcement of the order for implementation of measures for interception of communications, when assessed as having significance for the implemented measure. They are stored in the authorized institutions for the measures' implementation in accordance with the regulations for protection of personal data and classified information, for a period of three years from the expiry of the deadline determined by the order for interception of communications, and in case of the deadline's extension.

ANEXES TO PART 3

CHECKLIST FOR IMPLEMENTING MEASURES FOR INTERCEPTION OF COMMUNICATIONS FOR THE PURPOSE OF PROTECTING THE STATE'S INTERESTS OF SECURITY AND DEFENSE

DRAFTING A REQUEST

- **The Chief Public Prosecutor of the Republic of North Macedonia, at the proposal of the NSA Director or a person authorized by him/her, or at the proposal of the Minister of defense or a person authorized by him/her, drafts a request.**
- **The written request contains:**
 - Type of measure for interception of communications for which the request is submitted;
 - Data on the individual or the legal entity that is subject of the measure;
 - Data on the object, space or item that is subject of the measure;
 - The authority responsible for the implementation of the order;
 - Reasoning why the measure is proposed;
 - Duration of the measure; and
 - Type of telecommunications system, telephone number or other identification data, and the identification number for each of them individually.

REQUEST DELIVERY

- **The Chief Public Prosecutor of the Republic of North Macedonia delivers the request to the Supreme Court of the Republic of North Macedonia.**

DECISION-MAKING

- **A Justice of the Supreme Court of the Republic of North Macedonia, designated through the internal schedule of the Court, makes a decision immediately and within 24 hours after the delivery of the request at the latest.**
- **By exception, upon the request of the Chief Public Prosecutor of the Republic of North Macedonia, in urgent cases and when there is a threat of delay, the Justice of the Supreme Court of the Republic of North Macedonia can immediately issue a temporary written order for implementation of the measure for a period of 48 hours (Article 30 Paragraph 1 of the LIC).**

ORDER ISSUANCE

- **The Supreme Court Justice drafts an order.**
- **The order contains:**
 - Type of measure for interception of communications for which the request is submitted;
 - Data on the individual or the legal entity that is subject of the measure;
 - Data on the object, space or item that is subject of the measure;
 - The authority responsible for the implementation of the order;
 - Reasoning why the measure is proposed;
 - Duration of the measure; and
 - Type of telecommunications system, telephone number or other identification data, and the identification number for each of them individually.

ANONYMIZATION

- **The anonymization of the order is prescribed in the Rulebook on the manner of anonymization for implementation of measures for interception of communications for the purpose of protecting the state's interests of security and defense, and the manner of recording in the register of anonymized orders (Official Gazette of RM no.200 of 1 November 2018).**
- **The judge issuing the order for implementation of the measure for interception of communications in accordance with LIC is anonymizing it immediately after its issuance:**
 - One copy of the anonymized order for OTA; and
 - Two copies of the anonymized order for oversight and control, one of which for OTA and the other for the authorized institutions.

ORDER DELIVERY

- **The order is delivered to the Chief Public Prosecutor of the Republic of North Macedonia.**
- **The Chief Public Prosecutor of the Republic of North Macedonia delivers the order to an authorized person in the institution, at whose proposal he/she submitted the request to the Supreme Court Justice.**
- **The authorized person delivers the anonymized copies of the order to the authorized person in OTA.**

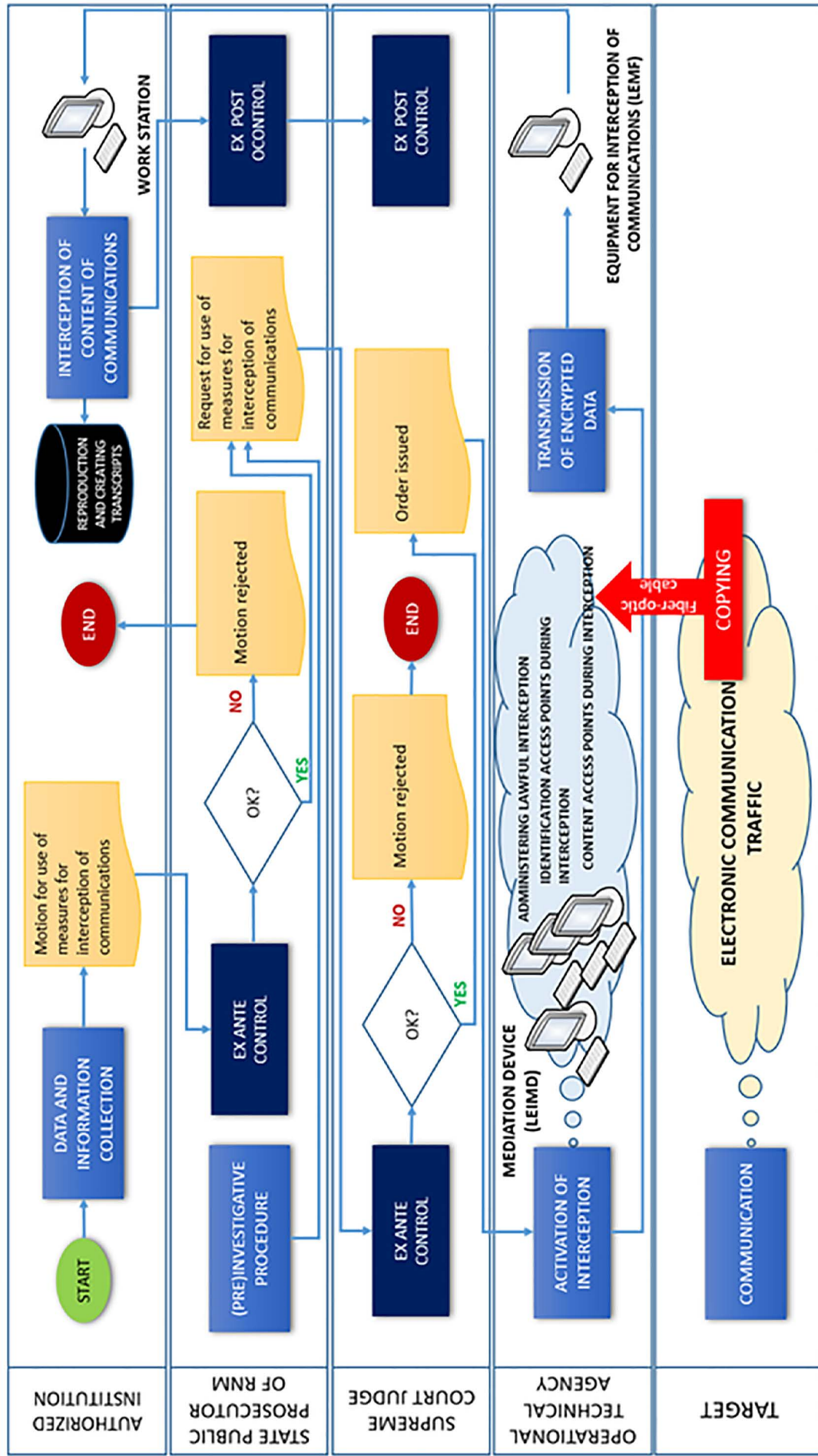
REPORTS

- **The authorized institution drafts and submits a report on the measure's implementation once in three months from the start of the measure's implementation to the Chief Public Prosecutor of the Republic of North Macedonia.**
- **Besides the mandatory reports submitted every three months, the authorized institution also submits a report upon request by the Chief Public Prosecutor of the RNM and also after the expiry of the period allowed for implementation of the measure for interception of communications.**

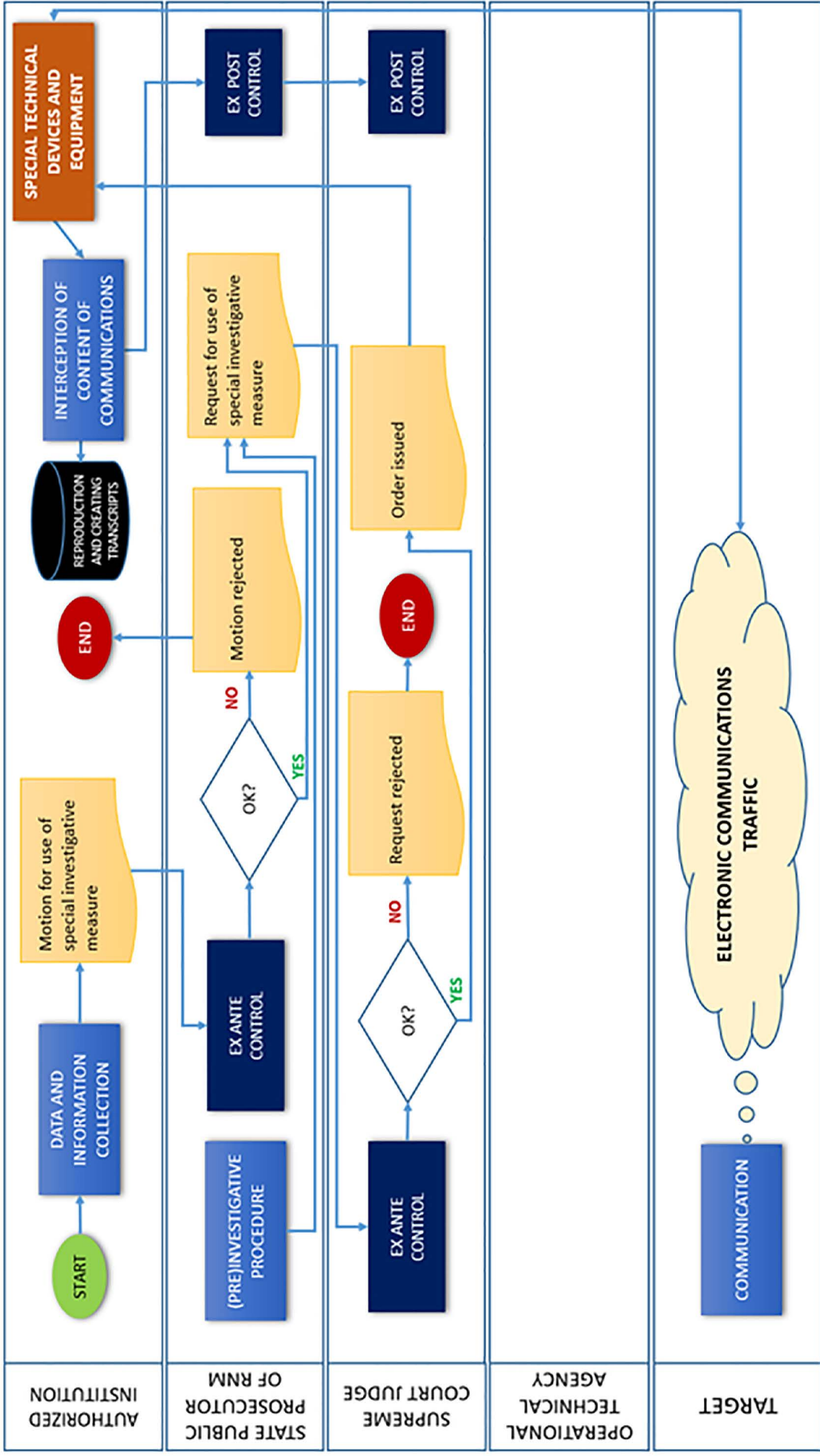
DELIVERY OF REPORTS

- **The Chief Public Prosecutor of RNM submits the reports from the authorized institution to the Supreme Court of RNM.**

INTERCEPTION OF COMMUNICATIONS FOR THE PURPOSE OF PROTECTING THE STATE'S SECURITY AND DEFENSE INTERESTS WITH OTA AS AN INTERMEDIARY



INTERCEPTION OF COMMUNICATIONS FOR THE PURPOSE OF PROTECTING THE STATE'S SECURITY AND DEFENSE INTERESTS WITHOUT OTA AS AN INTERMEDIARY



PART 4

CONTROL AND OVERSIGHT ON THE USE OF SPECIAL INVESTIGATIVE MEASURES



1. Introduction

In the case of *Klass v. Germany*, the ECtHR specified that “Special investigative measures in contemporary democratic societies represent a necessary instrument for the law enforcement authorities as an adequate means for prevention and detection of crime. However, if the use of these invasive measures is not legally regulated, there is a threat of undermining or even destroying democracy under the justification of its defense. The state should provide clear evidence on the necessity of the measures and assemble a legal framework that ensures proper and efficient protection from abuse through order by coincidence and giving proper attention. This also includes the existence of methods of responsibility for the authorization of intrusive measures and efficient control and oversight. In this regard, parliamentary oversight and judicial control are sufficient to meet the criteria of Article 8 Paragraph 2 of the ECHR, where judicial control offers the best guarantees of independence, impartiality and a proper procedure”.

The inability of achieving full accountability, transparency, oversight and control of the work of the security-intelligence services is a serious problem that is prevalent in almost all countries across the globe. The reasons and factors for this situation are numerous, such as:

- inexistence or insufficiently built efficient system for oversight and control of the work of the security-intelligence services;
- the “natural” introversion of services, originating from the special regime of secrecy in the work of the security-intelligence services and often restricts access and inspection of all relevant documents, activities and information;
- existence of discretion competencies of the services, which gives them an enormous and autochthonous freedom in the assessment of the type and level of danger from the threats on national security, and the type of undertaken measures and activities;
- lack of procedural safeguards for control and oversight in the procedure of proposing the use of the measures and undertaking of other operational activities;
- politicization, i.e. prevailing of political over security criteria in the work of the services, especially in the classification and assessment of the type of threats and the risks they pose;
- covering up of the non-transparent, unaccountable and unlawful work under the front of “top secret” or other types of restrictions of the access of the controlling and oversight bodies or the public, with the justification that such secrecy is necessary to prevent the occurrence of irreparable damage to national security etc.

By rule, a distinction is made between the terms of oversight and control.

The **term oversight usually means** (full or partial) planned (inspection) monitoring over a certain institution, accompanied by systematic (examination) research and review of the state of affairs that are subject of the oversight, ascertaining and evaluating an established state of affairs.

The **oversight** is a relatively new and efficient tool (end of the 20th century) of a democratic society, aimed to achieve and promote the accountability of the security-intelligence services, which compared to other state institutions, have restrictions to their openness and transparency to the public due to their work’s confidential nature. The citizens’ right to be informed about the operations and activities of the security-intelligence services, arises from the fact that they use public funds. Therefore,

the public has a full right to know if those means are used in a proper, lawful, effective and efficient way. Oversight (especially the parliamentary one) is an efficient instrument for the prevention and restriction of abuse tendencies in and by the security-intelligence system in a democratic society. Timely detection, ascertaining and signaling of certain inconsistencies by representatives of the Parliament (and other institutions with the right to oversight) enables timely reaction for the purpose of protecting the fundamental values of the democratic community.

The weaknesses of the parliamentary oversight arise from the nature and structure of the members of the parliamentary oversight:

- As political figures, they do not have the sufficient expertise in the area that is the subject of the oversight;
- Due to their affiliation to a certain political party, they are usually (considered to be) susceptible to political influence; and
- Due to the priority of their political office, members of parliaments pay much less attention to the significance of the oversight.

Unlike oversight, **control** is a legally modeled instrument of power for direct influence and guidance in all segments of the institution's operations that is subject of control, i.e. influence and guidance of its operating strategy, management and activities. Therefore, control is a prerogative of the executive and begins with the internal control that is applied hierarchically in the service itself.

The control is an important element not only for the performance (efficiency and effectiveness) in implementing the policies of the executive, but also (same as oversight) a significant instrument that guarantees and ensures the rule of law, i.e. the principle of lawful operations of the security-intelligence services. Unlike oversight, the control is aimed not only at ascertaining the state of affairs, but is always accompanied by specific compulsory guidelines, measures, obligations, and even establishing responsibility on the established illicit operations of the institution that is subject to control.

Control is also carried out by other authorities beyond the executive. In this context, the most important control is the one carried out by the judiciary and the public prosecutor's office.

*The aim of the oversight and control on the use of the special investigative measures is: **legality** (rule of law), **efficiency** (expedience and thriftiness in planning the realization of the projected competences and aims) and **effectiveness** (success in realization of the aims) in the application of the measures. Efficient oversight and control on the use of the measures is the best defense from overstepping or abuse of competences by the implementing authorities. The executive, through procedural safeguards, usually manages to establish and sustain a permanent and efficient oversight and control of the activities by the security and intelligence services. However, is it of essential significance for a democracy in a society to have an efficient oversight established by parliamentary bodies and non-parliamentary expert bodies that are independent from the current government administration.*

Parliamentary oversight is usually established in the form of separate bodies (most commonly commissions or committees) with a broad scope of oversight (oversight of the entire operations of services) or in the form of specialized committees (with a narrow scope), whose oversight competence is aimed only at one segment of the operations of the security-intelligence services (for example: *ex ante* or *ex post* oversight of certain complex operations by the services, oversight of measures for interception of communications etc.).

A significant and efficient oversight and control instrument is the financial audit of the work of the security-intelligence services (deciding on the size of the budget, its enlargement or additions, analysis of the annual financial reports etc.). The factual and efficient inspection of the financial

operations of the services can provide information on possible abuse or irregularities in their work. Suspicious financial activities are most commonly covered up as “special technical or operational costs” that are not available for public inspection. The financial operations are the most sensitive segment for which services are almost never “in a good mood” to give a full and transparent account and presentation to the public, explaining that this would cause “unforeseeable damage” to the state’s security interests.

Non-parliamentary expert bodies (inspections) for oversight are established and operate independently of the executive, parliamentary structures and the security-intelligence services they conduct the oversight of. They are elected and report to the Parliament and are considered more effective than parliamentary committees because of their expertise and full commitment to the oversight (most commonly these are professionals who had been engaged by and/or worked in the security-intelligence services).

Efficiency of oversight and control can be achieved only through precise standardization of the mechanisms for control and oversight and by creating conditions for adequate and objective application of the established control and oversight mechanisms.

Otherwise, the competent authorities can turn into a generator of crises and instead of enjoying the trust among citizens as a guarantee of public and national security, the public will look at them with doubt and mistrust.

The efficiency of control and oversight mechanisms is determined by a series of interrelated factors, as well as by the overall social, political and security environment in a country.

The integrity and independence of the institutions for oversight and control, and their cooperation with the other relevant institutions are of exceptional importance. A significant prerequisite for efficient oversight and control is the elimination of any partisan-political influence on persons managing these institutions.

By doing so, oversight and control will become the true watchdog of bodies authorized to use intrusive measures. This is especially important for oversight and control of the interception of communications, considering the complex structure of the system for interception of communications.

2. Oversight of the measures for interception of communications pursuant to the domestic legislation

According to the provisions (Articles 35, 40 and 47) of the LIC, the oversight of measures for interception of communications implemented by the competent authorities for interception of communications, the operators and the Operational Technical Agency (OTA) can be carried out by:

- **Parliament of RN Macedonia;**
- **Directorate for Security of Classified Information;**
- **Directorate for Personal Data Protection;**
- **Ombudsman;**
- **Citizens’ Control Council;**
- **Other entities (media, NGOs, the general public etc.).**

Unlike control, the aim of the oversight is, by rule, restricted to the legality of the operations of the security-intelligence services (or a portion of their operations), and indirectly of their effectiveness, without the possibility of incorporating the efficiency of their work.

Parliamentary oversight of the security-intelligence services in the security-intelligence system of RN Macedonia is conducted by:

- **Committee on Defense and Security** – conducting (indirect) oversight of the security-intelligence services in the Defense Ministry;
- **Committee for Supervising the Work of the Security and Counterintelligence Administration and the Intelligence Agency** – conducting oversight of the National Security Agency (the former Security and Counterintelligence Administration-UBK) and the Intelligence Agency;
- **Committee on Oversight of the Implementation of Measures for Interception of Communications.**

This third specialized Parliament committee comprised of incumbent MPs is authorized to conduct oversight of the legality and effectiveness in the implementation of the measures for interception of communications in all institutions involved in the process of implementing measures for interception of communications (Article 40 Paragraph 1 of the LIC), except in the Intelligence Agency.

In order to conduct a successful oversight (Article 39 of the LIC), the Committee on Oversight of the Implementation of Measures for Interception of Communications (hereinafter Committee) can hire national and international technical experts possessing the required expertise, who can take part in the Committee's work based on their accreditation. The technical oversight conducted by the Committee with the support of the technical experts does not include oversight on the content of the communications or any data related to the identity of the person or the communication that is subject of the measures for interception of communications.

The technical oversight in OTA and the operators is restricted only to the inspection of the anonymized court order and a check-up of the (logs) automatically created and stored electronic data in the mediating technical devices at the operators and OTA (Articles 41 and 42 of the LIC) that refer to the start and end of the measures, the number of anonymized court orders and the total number of implemented measures within a certain period of time, while technical oversight in the competent authorities is restricted (Article 43 of the LIC) only to an inspection of the anonymized court order and documents related to the start and end of the measure's implementation.

The oversight is always *ex post* and restricted only to establishment of the legality of proceedings when implementing the measures. Thus, besides data on the start and end of the measures, the Committee can obtain data on the number of issued court orders and total number of intercepted communications, and can conduct inspection of any anonymized order for oversight and control, but cannot obtain data on the real identity of the person whose communication is under surveillance.

Namely, unlike control, the Committee checks the similarity of the communication intercepted by the operators, OTA and the competent authorities for the measures' implementation, through a comparison of the identification numbers (they replace the real data on the identity of the communications' owner) listed in the anonymized court orders for oversight and control (Articles 41, 42 and 43 of the LIC).

In conducting the oversight, the Committee can make an inspection and establish whether the institutions involved in the process of implementing the measures for interception of communications have proper regulations for:

- the procedure of receipt, recording and forwarding court orders;
- procedure of internal control;
- procedure for rejection of orders by superiors that are against the law; and
- procedure of reporting irregularities and illicit activities in operations.

The Committee can conduct inspection and establish (Article 68 Paragraph 6 of the LIC) whether operators (OTA and competent authorities accordingly) have ensured the proper conditions for accu-

rate and unambiguous interception of communications, for the purpose of preventing the so-called mass surveillance of communications.

The Committee conducts the oversight of the effectiveness of the measures indirectly and by reviewing and analyzing the Annual Report of the Chief Public Prosecutor of the Republic of North Macedonia regarding the use of special investigative measures (Article 40 paragraph 3 of the LIC).

The Committee can conduct the oversight without prior announcement, as required, and at least once in three months, even in absence of a majority vote. The oversight can be a field one, i.e. direct presence of the Committee in the premises of the institution that is subject of the oversight, but the oversight can also be conducted in the premises of the Committee, by reviewing and analyzing the reports or through discussion with persons working in the institutions that are subject of the oversight.

The procedure of security check of the persons designated in the oversight bodies, as well as of the hired national and international technical experts in these bodies, is scheduled to last for a month instead of six months as it was before. The changes are aimed at creating prerequisites for an efficient oversight through elimination of certain difficulties, especially those that members of the parliamentary committees were faced with, even at times when there had been political will to conduct an efficient oversight.

3. Control of the measures for interception of communications in the domestic legislation

Unlike oversight, the judicial and prosecutorial control has no restrictions on the scope, width and type of activities and data it can control in the competent authorities for implementation of the special investigative measures, the operators and OTA (Articles 59 and 60 of the LIC).

Understandably, the only restriction arises from the subject matter jurisdiction of both institutions (Article 57 of the LIC), since each institution can control the issues that fall within its subject matter jurisdiction.

In other words, the Basic Court cannot control the measures ordered by the Supreme Court and the same refers to the control of the public prosecutors. Understandably, the law does not allow for control of the higher instances of the measures proposed and ordered by the lower instances, with one exception referring to the control of the special technical devices and equipment located at the Basic Public Prosecutor's Office for Organized Crime and Corruption (Article 60 Paragraph 5 of the LIC) and the National Security Agency.

Namely, only the Chief Public Prosecutor of the Republic of North Macedonia and the preliminary procedure judge, i.e. Supreme Court Justice who issued the order for the special investigative measure may conduct the control of the special technical devices and equipment, based on Article 60 of the LIC and Articles 55 and 58 of the LNSA. In addition, this is the only case when the Chief Public Prosecutor of the RN Macedonia can conduct a control (exception from the subject matter jurisdiction) of the official records that are maintained at the Basic Public Prosecutor's Office for Organized Crime and Corruption and the competent authorities.

Based on the legal provisions, the control is restricted to the legality of the measures' implementation (Articles 57-61 of the LIC) and is, by 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 ap-

proval 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 interception of communications and other official documents related to the use of the measures by the competent authorities, OTA and operators.

Due to the direct involvement of both institutions, the control inevitably includes the efficiency and effectiveness in the implementation of the measures for interception of communications, primarily among the competent authorities for implementation of the measures, and less among the operators and OTA.

According to Article 57 of the LIC, in cases when measures for interception of communications are used for criminal purposes, the public prosecutor in charge of the investigation and the preliminary procedure judge who issued the order for the special investigative measure are authorized to conduct the control of the legality of the special investigative measure conducted by the competent authorities for implementation of the special investigative measure, the operators and OTA.

In cases when the measures for interception of communications are used for the protection of the interests of security and defense of the state, the Chief Public Prosecutor of the Republic of North Macedonia and the Justice of the Supreme Court of the Republic of North Macedonia who issued the order for interception of communications are authorized to conduct the control of the legality in the implementation of the measure for interception of communications.

De legelata (Article 59 Paragraph 2), the law does not prescribe when the control is to be conducted, because this is a discretion right of both institutions, i.e. if required and unannounced. The subject of control is the legality of the special investigative measure (Article 57 Paragraph 1 and Article 59 Paragraph 1), i.e. proceeding in compliance with the provisions related to the implementation of the measures for interception of communications. The control incorporates all three institutions that are legally involved in the entire process of the measures' implementation: 1. the competent authorities for implementation of the special investigative measure, 2. the operators and 3. OTA.

Thus, pursuant to Article 59 of the LIC, the controlling authorities can *ex post*:

- conduct inspection at the location of the work stations used by the competent authorities, as well as the OTA premises that hold the equipment for interception of communications and the intermediary devices, but also at the location where operators store the devices for rerouting of the signal to OTA;
- ask or directly access the electronic register system;
- ask for inspection or a hardcopy of the register;
- ask or directly take on the anonymized order for interception of communications;
- read all logs that have been created, recorded or stored by the systems used by OTA and the operators, as well as the work stations used by the competent authorities, including data required from the operator, OTA or the competent authorities when conducting the oversight.

For the first time on record in the judicial and prosecutorial practice in the RN Macedonia, the Supreme Court of the RN Macedonia (in April 2019) and the Basic Public Prosecutor's Office for Organized Crime (in May 2019) conducted an unannounced, continual and *ex post* control of the legality, efficiency and effectiveness of the measures for interception of communications in OTA, the competent authorities and operators. This approach complies with the key role that the Court and the public prosecutor's office have in the field of control over the implementation of measures for interception of communications.

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 interception of communications in the work stations of the competent authorities for 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.

The Ministry of Interior of the RN Macedonia conducts a special type of control (Articles 2 and 62 of the LIC), which is not part of the aforementioned control, but refers to the production, offer for sale, sale, import, export, re-export or holding of means for interception of communications. This control is conducted *ex ante* by giving an approval to legal entities operating in the field, and *ex post* through continual control (inspections) of their work.

4. Public (independent) oversight of measures for interception of communications

4.1. Citizens' Control Council

The amendments to the LIC (Article 47) in 2018 led to the establishment of the Citizens' Control Council as a new, non-state, oversight body of the measures implemented by the competent authorities and OTA, but not the operators. The Council submits annual reports regarding its work and proceeds upon its own initiative or upon complaints filed by citizens.

The Council proceeds based on motions by citizens and legal entities over perceived illegal actions or irregularities in the implementation of the measures for interception of communications, and especially in cases of breaches to the constitutionally guaranteed human rights and fundamental freedoms. The Council notifies the Parliamentary Committee on Oversight of the Implementation of Measures for Interception of Communications, the competent public prosecutor and the Ombudsman about any observed irregularities. The sessions of the Council are held whenever required.

The Council conducts an announced oversight, except in cases when the nature of the complaint requires urgent action. It can ask the management of the competent authorities, OTA and the operators for information or data required to establish the validity of the claims in the complaint. The Council (and also the Committee), from the direct oversight, can only establish the existence of any abuse, but not whether the telephone number of the applicant had been intercepted or not.

The Council is elected by the Parliament for a period of three years. The Citizens' Control Council is comprised of a President and six members, of whom three are experts and the other three are representatives of NGOs in the field of human rights, security and defense. The Council is obliged to submit an annual report to the Parliament, which is discussed at a Parliament session.

4.2. Directorate for Personal Data Protection

The Directorate for Personal Data Protection has limited oversight of the competent authorities for the use of the measures, the operators and OTA. This oversight relates only to the legality of the

activities for processing personal data, as well as to the measures for their protection stipulated by the law (Article 54 of the LIC).

4.3. Directorate for Security of Classified Information

The Directorate for Security of Classified Information also has limited oversight of the competent authorities for use of the measures, the operators and OTA. This oversight relates to the legality when handling classified information regulated by law and the regulations adopted in compliance with that law. The subject of the oversight is: the method and procedure of security classification of information and documents, the method and procedure of their storage, the method and procedure of internal and external exchange of classified information and documents, the zoning of premises used for handling of classified information etc. (Article 55 of the LIC).

4.4. Ombudsman

The Ombudsman can also conduct oversight of the legality of the measures for interception of communications. As a body protecting the constitutional and legal rights of citizens when violated by acts, actions or absence of actions by the public authorities, the Ombudsman is authorized to undertake actions and measures and initiate proceedings upon complaints or by its own initiative. The Ombudsman is authorized to conduct external control of the Ministry of Interior. Article 24 of the Law on the Ombudsman regulates that for the purpose of assessing a complaint, the Ombudsman can ask for explanations, information and evidence, enter official premises, conduct direct inspections, call an official for a conversation, as well as undertake other measures provided for in a law or other regulation.

4.5. Annual report of the Chief Public Prosecutor of RN Macedonia

The Chief Public Prosecutor of the Republic of North Macedonia submits an annual report to the Parliament of RN Macedonia on the use of special investigative measures during the previous calendar year.

Although the law does not stipulate the Parliament's competences regarding this report, from the content of this Article, it might be concluded that the aim of this briefing to the Parliament is to obtain data statistically representing the dynamics of the measures, and not for the Parliament to be controlling the legality of the measures. Besides data on the number of procedures that involved the issuance of orders for intrusive measures and the crimes for which these measures were applied, in this report, the Chief Public Prosecutor should provide information on whether the use of special investigative measures produced results that are relevant to the procedure or there is a probability that they could be relevant for the procedure (Article 271 Paragraph 2 Item 6 of the LCP), but also elaborate the reasons for any lack of relevant results from the interceptions (Article 271 Paragraph 2 Item 7 of the LCP).

Until now, the annual reports by the Chief Public Prosecutor have not incorporated more detailed information on whether the interception of communications produced relevant results and the reasons for the lack of such results.

The prior annual reports on the use of the special investigative measures contain only statistical data on the number and type of the applied special investigative measures, the crimes due to which the measures were issued etc. On the other hand, the reports clearly show that in comparison with the other measures stipulated in the LCP, the special investigative measure of *Interception and recording of*

telephone and other electronic communications in a procedure established by a separate law was by far the most frequently used measure.

4.6. Other authorities

Besides the abovementioned authorities, the **media, NGOs and the public** are also watchdogs of the entities in charge of interception of communications. This control is significant if it is really objective and free of partisan-political influence and pressure. The prerequisite for this type of control is the development of investigative journalism, transparency and accountability of institutions.

BIBLIOGRAPHY

Books and articles

- Bloustein, E., Privacy as an aspect of Human Dignity, 39 New York University Law Review, 1964
- Flaerty, D., Protecting Privacy in Surveillance Society, The University of North Carolina press, 1989
- Gunderman, L., Law on personal data protection with comments, Directorate for personal data protection, Skopje, 2010
- Kambovski, V., Organized crime, Skopje, 2005
- Kilkelly, U., The right to respect for private and family life, A guide to the implementation of Article 8 of the European Convention on Human Rights, Council of Europe, Strasbourg, 2001
- Ruiz, B., Privacy in telecommunications, A European and American Approach, Kluwer Law International, The Hague, 1997
- Haris, D, O'Boyle, M, Warbrick, K., Law of the European Convention on Human Rights, second edition, Oxford University Press, 2009
- Westin, A.F., Privacy and Freedom, Bodley Head, 1970

Legal acts

- Constitution of the Republic of Macedonia, Official Gazette of the Republic of Macedonia no. 84/03
- Law on changes and amendments of the Law on Criminal Procedure, Official Gazette of the Republic of Macedonia no. 74/04
- Law on Criminal Procedure, Official Gazette of the Republic of Macedonia no. 150/10
- Law on Interception of Communications, Official Gazette of the Republic of Macedonia no. 71/18, 108/19
- Law on Operative Technical Agency, Official Gazette of the Republic of Macedonia no. 71/18
- Law on Electronic Communications, Official Gazette of the Republic of Macedonia no. 13/05, 14/07, 55/07, 83/10, 13/12, 123/12, 11/18
- Law on Internal Affairs, Official Gazette of the Republic of Macedonia no. 42/14, 116/14, 33/15, 5/16, 120/16, 127/16, 142/16, 190/16
- Law on Police, Official Gazette of the Republic of Macedonia no. 114/06, 6/09, 145/12, 41/14, 33/15, 31/16, 106/16, 120/16, 21/18, 64/18
- Law on Defense (consolidated text), Official Gazette of the Republic of Macedonia no. 185/11
- Law on Public Prosecutor' Office, Official Gazette of the Republic of Macedonia no. 150/07, 111/08
- Law on Customs Administration, Official Gazette of the Republic of Macedonia no. 46/04, 81/05, 107/07, 103/08, 64/09, 48/10, 158/10, 53/11, 113/12, 43/14, 167/14, 33/15, 129/15, 23/16, 120/18
- Law on National Security Agency, Official Gazette of the Republic of North Macedonia no. 108/19
- Law on Coordination of the Security Intelligence Community in the Republic of North Macedonia, Official Gazette of the Republic of North Macedonia no. 108/19
- Decree for Administrative Security of Classified Information, Official Gazette of the Republic of Macedonia no. 9/04
- Strategy for Defense of Republic of Macedonia, Official Gazette of the Republic of Macedonia no. 30/10
- Rulebook on the Method of Determining the Relevance of Data Collected and Processed by Implementing the Order to Implement Measures for Interception of Communications for the Protection of State Security and Defense Interests and Their Destruction, Official Gazette of the Republic of Macedonia no. 243/18

- European Commission for Democracy through Law (Venice Commission) Report on the Democratic Oversight of the Security Services, Strasbourg, 11 June 2007, no. 388/2006, [http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/3_cdl-ad\(2007\)016_/3_cdl-ad\(2007\)016_en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/3_cdl-ad(2007)016_/3_cdl-ad(2007)016_en.pdf)
- Resolution 2625 (XXV) of the United Nations General Assembly in 1970 (*The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States*, United Nations, A/RES/25/2625)
- Explanatory Memorandum to Rec (2005) 10
- Parliamentary oversight of the security sector: Principles, mechanisms and practices, <http://archive.ipu.org/PDF/publications/decaf-e.pdf>
- Recommendation (1996) 8 on Europe in a time of change: crime policy and criminal law, adopted by the Committee of Ministers on 5 September 1996
- Recommendation (2001) 11 of the Committee of Ministers to member states concerning guiding principles of the fight against organized crime, adopted by the Committee of Ministers on 19 September 2001
- Recommendation (2005) 10 of the Committee of Ministers to member states on „special investigation techniques“ in relation to serious crimes including acts of terrorism, adopted by the Committee of Ministers on 20 April 2005
- Recommendation 1713/2005, Parliamentary Assembly of Council of Europe, <http://www.assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17360&lang=en>
- Recommendation on Democratic Oversight of National Security Services, Commissioner for Human Rights of Council of Europe, 2015, [https://rm.coe.int/ref/CommDH/IssuePaper\(2015\)2](https://rm.coe.int/ref/CommDH/IssuePaper(2015)2)
- Explanatory Memorandum to the Recommendation Rec (2005) 10 of the Committee of Ministers to member states on “special investigation techniques” in relation to serious crimes including acts of terrorism, CM/DEL/DEC(2005)925/10.8, 10 May 2005
- UN Council for human rights 2009; UN 2010a, <https://fas.org/irp/eprint/unhrc.pdf>

Law cases

- Olsson v. Sweden, 24.05.1988 (No. 10465/83)
- Sunday Times v. UK, 1980, 2 EHRR 245
- James v. UK, 1986, 8 EHRR
- Sporrang v. Sweden, 1983, 5, EHRR
- Smith and Grady v. UK, 2000, 29 EHRR 493
- Kopp v. Switzerland, 1999, 27 EHRR 91
- Klass v. Germany, 1979/80, EHRR 213
- Campbell v. UK, 1992, 15 EHRR 137
- Craxi v. Italy, 17.07.2003 (No. 25337/94)
- Malone v. United Kingdom, 27.06.1986 (No. 8691/79)
- Silver v. United Kingdom (1983) 5 EHRR 347
- Taylor-Sabori v. United Kingdom (2002) 36 EHRR 17
- Doerga v. The Netherlands, 27.04.2004 (No. 50210/99)
- Khan v. United Kingdom [1997] AC558
- Ramanuskas v. Lithuania, 2008, Application No. 74420/01
- Shannon v. United Kingdom, 5.4.2004, No 120
- P.G. and J.H. v. the United Kingdom, no. 44787/98, ECHR 2001 IX
- Dragojević v. Croatia (no. 68955/11, §§ 52-61, 15 January 2015)
- Funke v. France (1993) 16 EHRR 297

ANEXES TO THE BENCHBOOK

SECRET

BASIC PUBLIC PROSECUTOR'S OFFICE

KOIM OSK no.

Skopje, ____ (date)

TO

BASIC COURT SKOPJE 1

- pre-trial judge -

SKOPJE

Based on Article 39 Paragraph 2 Line 2, in relation to Article 256, Article 252 Paragraph 1 Item 1 and Article 253 Item 2 of the CPC, I hereby submit this

REQUEST

FOR AN ORDER

FOR IMPLEMENTATION OF THE FOLLOWING SPECIAL INVESTIGATIVE MEASURE:

Interception and recording of telephone and other electronic communications of Article 252 Paragraph 1 Item 1 of the CPC.

AGAINST PERSON:

Name and surname, birth reg.no, residence address in xxx at str.xxx,

Macedonian tel.no. xxx, identification numbers

OSK_OSK1_XXXXXXXX_1_TM and

OSK_OSK1_XXXXXXXX_1_OV.

For whom there are grounds of suspicion of undertaking activities to commit crime *Receiving a bribe* of Article 357 of the Criminal Code and crime *Abuse of office* of Article 353 of the Criminal Code.

It is likely that data and evidence for successful criminal procedure shall be secured, but cannot be collected by other means.

The judicial police shall implement the special investigative measures, under the control of the public prosecutor.

The special investigative measure Interception and recording of telephone and other electronic communications incorporates interception of communications of the person at telephone line xxx.

Equipment owned by the Ministry of Interior of the RM is to be used in implementing the special investigative measures.

The order for the special investigative measure to be issued for a period of three month, starting at xxx h on xxx up to xxx h on xxx.

REASONING

Basic public prosecutor's office xxx has knowledge and evidence that the persons undertake activities for commit crime *Receiving a bribe* of Article 357 of the Criminal Code and crime *Abuse of office* of Article 353 of the Criminal Code.

This knowledge arise from the testimony of person xxx

In this context, the official note provides information that the persons that are subject of the special investigative measures, each in their own field of action and by affecting employees xxx who are directly responsible.

Considering the above, there is reasonable suspicion that the persons undertake activities to commit crime *Receiving a bribe* of Article 357 of the Criminal Code and crime *Abuse of office* of Article 353 of the Criminal Code.

In the specific case, data and evidence required for a successful criminal procedure cannot be collected by other means not only because of the type of the listed crimes, but also because these are crimes committed through strict conspiracy between the persons. Therefore, I submit a Request for use of the special investigative measure Interception and recording of telephone and other electronic communications incorporates interception of communications of Article 252 Paragraph 1 Item 1 of CPC against the persons.

Based on Article 258 Paragraphs 1 and 2 of the CPC, the judicial police shall draft a separate report after the measure's enforcement and submit it to the public prosecutor.

PUBLIC PROSECUTOR

SECRET

SECRET

BASIC PUBLIC PROSECUTOR'S OFFICE

KOIM no. /

Skopje, ____ (date)

TO

TO

BASIC COURT SKOPJE 1

- pre-trial judge -

SKOPJE

Based on Article 39 Paragraph 2 Line 2, in relation to Article 256, Article 252 Paragraph 1 Item 2 and Article 253 Item 2 of the CPC, I hereby submit this

REQUEST

FOR AN ORDER

FOR IMPLEMENTATION OF THE FOLLOWING SPECIAL INVESTIGATIVE MEASURE

Interception and recording in a home or enclosed space belonging to the home or office space designated as private or in a vehicle, and entry in such facilities in order to create the required conditions for interception of communications of Article 252 Paragraph 1 Item 2 of the CPC.

AGAINST PERSON:

xxx

For whom there are grounds for suspicion of undertaking activities for perpetration of crime *Receiving a bribe* of Article 357 of the Criminal Code, crime *Giving a bribe* of Article 358 of the Criminal Code, and crime *Abuse of Office* of Article 353 of the Criminal Code.

It is likely that data and evidence for successful criminal procedure shall be secured, but cannot be collected by other means.

Interception and recording in a home or enclosed space belonging to the home or office space designated as private or in a vehicle, and entry in such facilities in order to create the required conditions for interception of communications of Article 252 Paragraph 1 Item 2 of the CPC.

The judicial police of the Ministry of Interior of RM shall implement the special investigative measures, under the control of the public prosecutor.

The order for the special investigative measure to be issued for period of one month, starting at xxx h on xxx up to xxx h on xxx.

REASONING

The Ministry of Finance, Finance Police Office, submitted Report no.xxx of xxx to this prosecutor's office, stating there is reasonable suspicion that xxx.

Considering the abovementioned reasons for one of the persons xxx, two orders for special investigative measures have been issued: xxx.

Having in mind the special investigative measures undertaken until now, the public prosecutor's office finds that the incriminating activities are prepared in the working premises of person xxx, especially if considered that the person is working in an isolated office in xxx.

In the specific case, the data and evidence required for a successful criminal procedure cannot be collected by other means not only because of the type of the listed crimes, but also because these are crimes committed through strict conspiracy between the persons. Therefore, I submit a Request for an order for the special investigative measure *Interception and recording in a home or enclosed space belonging to the home or office space designated as private or in a vehicle, and entry in such facilities in order to create the required conditions for interception of communications* of Article 252 Paragraph 1 Item 2 of the CPC, against person xxx, encompassing the following premises xxx.

PUBLIC PROSECUTOR

SECRET

SECRET

BASIC PUBLIC PROSECUTOR'S OFFICE

KOIM no.

Skopje, _____ (date)

TO

TO

BASIC COURT SKOPJE 1

- pre-trial judge -

SKOPJE

Based on Article 39 Paragraph 2 Line 2, in relation to Article 256, Article 252 Paragraph 1 Item 3 and Article 253 Item 2 of the CPC, I hereby submit this

**REQUEST
FOR AN ORDER**

FOR IMPLEMENTATION OF THE FOLLOWING SPECIAL INVESTIGATIVE MEASURE

Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private of Article 252 Paragraph 1 Item 3 of the CPC,

AGAINST PERSON:

THE PERSON, no telephone numbers...

For whom there are grounds for suspicion of undertaking activities for perpetration of crime -

It is likely that data and evidence for successful criminal procedure shall be secured, but cannot be collected by other means.

The judicial police shall implement the special investigative measures, under the control of the public prosecutor.

Equipment owned by the Ministry of Interior of the Republic of Macedonia is to be used in implementing the special investigative measures.

The order for the special investigative measure to be issued for a period starting at xxx h on xxx up to xxx h on xxx.

REASONING

The Basic Public Prosecutor's Office Skopje possesses information and evidence that person.....

Considering all of the above, there is a reasonable suspicion that person xxx, who had contacts with the assistant on xxx at xxx, and on certain occasions handed over a package-envelope with unknown contents, undertook activities for perpetration of crime xxx.

In the specific case, the data and evidence required for a successful criminal procedure cannot be collected by other means not only because of the type of the listed crimes, but also because these are crimes committed through strict conspiracy between the persons. Therefore, I submit a Request for an order for the special investigative measure *Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private* of Article 252 Paragraph 1 Item 3 of the CPC, against person xxx.

Based on Article 258 Paragraph 2 of the CPC, the judicial police shall draft a report after the measure's enforcement and submit it to the public prosecutor.

PUBLIC PROSECUTOR

SECRET

SECRET

BASIC PUBLIC PROSECUTOR'S OFFICE

KOIM no.

Skopje, _____ (date)

TO
BASIC COURT SKOPJE 1
- pre-trial judge -
SKOPJE

Based on Article 39 Paragraph 2 Line 2, in relation to Article 256 and Article 252 Paragraph 1 Item 4 of the CPC, I hereby submit this

REQUEST
FOR AN ORDER

FOR IMPLEMENTATION OF THE FOLLOWING SPECIAL INVESTIGATIVE MEASURE
Secret inspection and search of computer systems of Article 252 Paragraph 1 Item 4 of the CPC.

AGAINST PERSON:

XXX

For whom there are grounds for suspicion of undertaking activities for perpetration of crime *Abuse of Office* of Article 353 of the Criminal Code.

It is likely that data and evidence for successful criminal procedure shall be secured, but cannot be collected by other means.

The judicial police shall implement the special investigative measures, under the control of the public prosecutor.

Equipment owned by the Ministry of Interior of the RM is to be used in implementing the special investigative measures.

The order for the special investigative measure to be issued for a period of four months, starting at xxx h on xxx up to xxx h on xxx.

REASONING

Having in mind that the Financial Police Office reported of having information of crimes committed in the field of financial crime, i.e. *Abuse of Office* of Article 353 of the Criminal Code, perpetrated by responsible persons in the first group of legal entities, in a way that xxx.

For the purpose of securing data and evidence that cannot be obtained by other means or their obtaining would be difficult, while the persons involved in the illicit activities acquired and will acquire unlawful property by committing crimes *Abuse of Office* of Article 353 of the Criminal Code, in the interest of efficient detection of the perpetrators, we hereby propose to the pre-trial judge to issue an order for use of special investigative measure *Secret inspection and search of computer systems* of Article 252 Paragraph 1 Item 4 of the CPC, against person xxx.

PUBLIC PROSECUTOR

SECRET



SECRET

A PRE-TRIAL JUDGE in BASIC COURT - Pre-trial Department XXX, proceeding upon a request by the Basic Public Prosecutor's Office KOIM-OSK no. of XXX, for an order for implementation of special investigative measure Interception and recording of telephone and other electronic communications, in accordance with Article 252 Paragraph 1 Item 1 of the CPC and Article 256 of the CPC in relation to Article 9 in relation to Article 8 and Article 15 of the Law on Interception of Communications, on xxx issues the following:

ORDER

The following special investigative measure is to be implemented for the purpose of securing data and evidence for successful criminal procedure that cannot be collected by other means:

Interception and recording of telephone and other electronic communications in a procedure laid down by law of Article 252 Paragraph 1 Item 1 of the CPC.

AGAINST PERSONS:

1. X with X telephone number X, identification numbers XXXXXXXXX
2. X with X telephone number X, identification numbers XXXXXXXXX
3. X with X telephone number X, identification numbers XXXXXXXXX
4. X with X telephone number X, identification numbers XXXXXXXXX
5. X with X telephone number X, identification numbers XXXXXXXXX
6. X with X telephone number X, identification numbers XXXXXXXXX
7. X with X telephone number X, identification numbers XXXXXXXXX

For whom there are grounds for suspicion of undertaking activities for perpetration of crimes - XXX of the CPC, crime - XXX of the Criminal Code and crime - XXX of the Criminal Code.

It is likely that data and evidence for successful criminal procedure shall be secured, but cannot be collected by other means.

Special investigative measure Interception and recording of telephone and other electronic communications in a procedure laid down by law of Article 252 Paragraph 1 Item 1 of the CPC incorporates the interception of communications of persons:

1. X with X telephone number X, identification numbers XXXXXXXXX
2. X with X telephone number X, identification numbers XXXXXXXXX
3. X with X telephone number X, identification numbers XXXXXXXXX
4. X with X telephone number X, identification numbers XXXXXXXXX
5. X with X telephone number X, identification numbers XXXXXXXXX
6. X with X telephone number X, identification numbers XXXXXXXXX
7. X with X telephone number X, identification numbers XXXXXXXXX

The special investigative measure is to be implemented through the technical means owned by the Operational Technical Agency and the Ministry of Interior.

The order is to be enforced by the Ministry of Interior of RM, with OTA as intermediary, under the control of the public prosecutor.

According to Article 258 Paragraphs 1 and 2 of the CPC, the Ministry of Interior of RM drafts a report at the request of the public prosecutor every 30 days and drafts a separate report for the public prosecutor after the measure's enforcement.

The order is issued for a period of four months, starting at 15:00h on xxx up to 15:00h on xxx.

REASONING

The basic public prosecutor's office submitted to the pre-trial judge of this court on XXX under KOIM-OSK no.X a Request for an order for implementation of special investigative measure Interception and recording of telephone and other electronic communications, in accordance with Article 252 Paragraph 1 Item 1 of the CPC against persons X with X telephone number X, identification numbers XXXXXXXXX; X with X telephone number X, identification numbers XXXXXXXXX; X with X telephone number X, identification numbers XXXXXXXXX; X with X telephone number X, identification numbers XXXXXXXXX; X with X telephone number X, identification numbers XXXXXXXXX; X with X telephone number X, identification numbers XXXXXXXXX; X with X telephone number X, identification numbers XXXXXXXXX, because of existing grounds for suspicion of undertaking activities for perpetration of crime - X of the Criminal Code, crime - X of the Criminal Code and crime - X of the Criminal Code. The Request is accompanied by Notification SD no.X of X drafted by the Ministry of Finance, Financial Police Office, Republic of North Macedonia.

Considering the reasoning of the request for implementation of the special investigative measure and in relation to Notification SD no.X of X, the pre-trial judge finds it is grounded.

For the purpose of securing data and evidence required for a successful criminal procedure that cannot be collected by other means or their obtaining would be difficult, especially due to the fact that obtained data and information cannot successfully prove the involvement and relationship of the persons taking part in the illicit activities and the acquisition of unlawful property, and in the interest of efficient detection of the perpetrators and finding other perpetrators of crime, the pre-trial judge hereby issues the order for use of special investigative measure Interception and recording of telephone and other electronic communications in a procedure laid down by law of Article 252 Paragraph 1 Item 1 of the CPC.

BASIC COURT X
X UOSK no.X of X

Pre-trial judge

SECRET

THE BASIC COURT, proceeding upon a request by the Basic Public Prosecutor's Office KOIM no. of X, for an order for extension of the implementation of a special investigative measure, in accordance with Article 256 and Article 260 of the CPC, on xxx issues the following:

ORDER

Extension of the following special investigative measure is to be implemented for the purpose of securing data and evidence for successful criminal procedure that cannot be collected by other means:

Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private of Article 252 Paragraph 1 Item 3 of the CPC,

AGAINST PERSONS:

1. X with birth reg.no, residing at X
2. X with birth reg.no, residing at X

For whom there are grounds for suspicion of undertaking activities for perpetration of crime - X of the Criminal Code.

The special investigative measure of Article 252 Paragraph 1 Item 3 of the CPC incorporates secret surveillance and recording of persons X and objects by using technical devices outside the home or office space designated as private, because there are grounds for suspicion over their involvement in the perpetration of crime - X of the Criminal Code.

Equipment owned by the Ministry of Interior of the RM is to be used in implementing the special investigative measures.

The order is issued for a period of four months, starting at 15:00h on xxx up to 15:00h on xxx.

Implementation of the special investigative measure is to be stopped before the expiration date as soon as the grounds for approval cease to exist or when their objectives have been met.

The judicial police shall implement the special investigative measures, under the control of the public prosecutor, drafting a report that is submitted to the public prosecutor upon his request.

REASONING

The basic public prosecutor's office submitted to the pre-trial judge of this court on XXX under KO-IM-OSK no.X a Request for an order for extension of the implementation of special investigative measure *Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private* of Article 252 Paragraph 1 Item 3 of the CPC, against persons X because of existing grounds for suspicion of undertaking activities for perpetration of crime X of the Criminal Code. Attached is a notification from the Ministry of Finance, Financial Police Office no. X of X.

The motion by the basic public prosecutor's office states that the Financial Police Office has knowledge of XXXXXXXX.

Considering the reasoning of the request for extension of the implementation of the special investigative measure, the pre-trial judge finds it is grounded.

For the purpose of proving the involvement of persons XXX in the perpetration of crime XXX of the Criminal Code and for the purpose of securing data and evidence required for a successful criminal procedure that cannot be collected by other means or their obtaining would be difficult, the pre-trial judge hereby issues the order for extension of the special investigative measure.

BASIC COURT X
KPPm no.X of X

Pre-trial judge

SECRET

SECRET

THE BASIC COURT, proceeding upon a request by the Basic Public Prosecutor's Office KOIM no.X of X, for an order for implementation of a special investigative measure, in accordance with Article 256 and Article 260 of the CPC, on xxx issues the following:

ORDER

The following special investigative measure is to be implemented for the purpose of securing data and evidence for successful criminal procedure that cannot be collected by other means:

Secret inspection and search of computer systems of Article 252 Paragraph 1 Item 4 of the CPC.

AGAINST PERSONS:

1. X with birth reg.no, residing at X
2. X with birth reg.no, residing at X

For whom there are grounds for suspicion of undertaking activities for perpetration of crime - X of the Criminal Code.

The special investigative measure of Article 252 Paragraph 1 Item 4 of the CPC incorporates secret surveillance and recording of persons X and objects by using technical devices outside the home or office space designated as private, because there are grounds for suspicion over their involvement in the perpetration of crime - X of the Criminal Code.

Equipment owned by the Ministry of Interior of the RM is to be used in implementing the special investigative measures.

The order is issued for a period of four months, starting at 15:00h on xxx up to 15:00h on xxx.

Implementation of the special investigative measure is to be stopped before the expiration date as soon as the grounds for approval cease to exist or when their objectives have been met.

The judicial police shall implement the special investigative measures, under the control of the public prosecutor, drafting a report that is submitted to the public prosecutor upon his request.

REASONING

The basic public prosecutor's office submitted to the pre-trial judge of this court on XXX under KOIM-OSK no.X a Request for an order for extension of the implementation of special investigative measure *Secret inspection and search of computer systems* of Article 252 Paragraph 1 Item 4 of the CPC, against persons X because of existing grounds for suspicion of undertaking activities for perpetration of crime X of the Criminal Code. Attached is a notification from the Ministry of Finance, Financial Police Office no. X of X.

The motion by the basic public prosecutor's office states that the Financial Police Office has knowledge of XXXXXXXX.

Considering the reasoning of the request for extension of the implementation of the special investigative measure, the pre-trial judge finds it is grounded.

For the purpose of proving the involvement of persons X in the perpetration of crime X of the Criminal Code and for the purpose of securing data and evidence required for a successful criminal procedure that cannot be collected by other means or their obtaining would be difficult, the pre-trial judge hereby issues the order for extension of the special investigative measure.

BASIC COURT X
KPPm no.X of X

Pre-trial judge

SECRET

SECRET

BASIC PUBLIC PROSECUTOR'S OFFICE

KOIM no.

Skopje, ____ (date)

Based on Article 39 Paragraph 2 Line 2, in relation to Article 256, Article 252 Paragraph 1 Item 6 and Article 253 Item 2 of the CPC, hereby issues this

ORDER

FOR IMPLEMENTATION of special investigative measure

Inspection in telephone and other electronic communications of Article 252 Paragraph 1 Item 6 of the CPC,

AGAINST PERSONS:

XXX

XXX

There is reasonable suspicion that the suspect xxx undertook actions to commit crime *Receiving a bribe* of Article 357 Paragraph 1 of the Criminal Code and crime *Abuse of office* of Article 353 Paragraph 1 of the Criminal Code, while suspect xxx is under reasonable suspicion of perpetrating crime *Giving a bribe* of Article 358 Paragraph 1 of the Criminal Code and crime *Abuse of office* of Article 353 Paragraph 1 in relation to Article 23 of the Criminal Code.

It is likely that data and evidence for successful criminal procedure shall be secured, but cannot be collected by other means. An order for implementation of investigative procedure KO no.xxx of xxx (date) was also issued.

The special investigative measure *Inspection in telephone or other electronic communications* of Article 252 Paragraph 1 Item 6 of the CPC encompasses the determination of the ownership of a mobile phone type xxx model xxx IMEI xxx and area code xxx, and whether the telephone number had been used for phone communication with the telephone number of suspect xxx, and other facts that can serve as evidence from the aspect of the abovementioned crimes and the suspects as perpetrators.

The judicial police and the Department for prevention of organized and serious crime within the Public Security Bureau shall implement the special investigative measures, under the control of the public prosecutor.

The following technical equipment is to be used when implementing the special investigative measure:

- computer equipment owned by Mol.

The order for the special investigative measure to be issued for a period of ten days, starting at xxx h on xxx up to xxx h on xxx.

REASONING

The Basic Public Prosecutor's Office Skopje has the following information and evidence: xxx, which produce the grounds for suspicion that the suspect xxx undertook activities to commit crime *Receiv-*

ing a bribe of Article 357 Paragraph 1 of the Criminal Code and crime *Abuse of office* of Article 353 Paragraph 1 of the Criminal Code, while suspect xxx of undertaking activities to commit crime *Giving a bribe* of Article 358 Paragraph 1 of the Criminal Code and crime *Abuse of office* of Article 353 Paragraph 1 in relation to Article 23 of the Criminal Code.

Namely, it arises from the information and evidence that on day xxx.

In the specific case, data and evidence necessary for a successful criminal procedure cannot be collected by other means, not only because of the type of the listed crimes, but also because these are crimes committed through strict conspiracy between the persons.

Considering the above, I hereby issue this order.

PUBLIC PROSECUTOR

SECRET

SECRET

BASIC PUBLIC PROSECUTOR'S OFFICE

KOIM no.

Skopje, ____ (date)

Based on Article 39 Paragraph 2 Line 2, in relation to Article 256 Paragraphs 1-7 and Article 253 Item 2 of the CPC, the public prosecutor in the Basic Public Prosecutor's Office Skopje issues this

ORDER

FOR IMPLEMENTATION of special investigative measure

Simulated purchase of items of Article 252 Paragraph 1 Item 7 of the CPC,

AGAINST PERSONS:

XXX

XXX

For whom there are grounds for suspicion of undertaking activities for perpetration of crime *Unlawful production and distribution of narcotics, psychotropic substances and precursors* of Article 215 of the Criminal Code.

It is likely that data and evidence for successful criminal procedure shall be secured, but cannot be collected by other means. Special investigative measure *Simulated purchase of items* of Article 252 Paragraph 1 Item 7 of the CPC would secure evidence of the specific crime and activities undertaken by persons xxx for its perpetration, but also detect other persons involved in the perpetration of the crime.

Special investigative measure *Simulated purchase of items* of Article 252 Paragraph 1 Item 7 of the CPC incorporates infiltration of an undercover agent that would conduct a simulated purchase of narcotics.

The judicial police of the MoI of the Republic of North Macedonia shall implement the special investigative measures, under the control of the public prosecutor.

Equipment owned by the Ministry of Interior of the RM is to be used in implementing the special investigative measures.

The order for the special investigative measure to be issued for a period of two months, starting at xxx h on xxx up to xxx h on xxx.

REASONING

The MoI Skopje department, Sector for illicit drug trafficking has submitted a report to the Basic Public Prosecutor's Office Skopje SD no.xxx of xxx (date), stating that persons xxx are undertaking activities related to the purchase of narcotics xxx in larger quantities, thus committing the crime *Unlawful production and distribution of narcotics, psychotropic substances and precursors* of Article 215 Paragraph 1 of the Criminal Code.

In the specific case, the order for special investigative measure *Simulated purchase of items* of Article 252 Paragraph 1 Item 7 of the CPC shall enable a simulated purchase of narcotics from the

abovementioned persons, ensuring data and evidence necessary for a successful criminal procedure, which cannot be collected by other means, not only because of the type of the listed crimes, but also because these are crimes committed through strict conspiracy between the persons.

Considering the above, I hereby issue this order.

PUBLIC PROSECUTOR

SECRET

SECRET

BASIC PUBLIC PROSECUTOR'S OFFICE

KOIM no.

Skopje, _____ (date)

Based on Article 39 Paragraph 2 Line 2, in relation to Article 256, Article 252 Paragraph 1 Item 8 and Article 253 Item 2 of the CPC, the public prosecutor in the Basic Public Prosecutor's Office Skopje issues this

ORDER

FOR IMPLEMENTATION of special investigative measure

Simulated offering and receiving bribes of Article 252 Paragraph 1 Item 8 of the CPC,

AGAINST PERSONS:

XXX

XXX

For whom there are grounds for suspicion of undertaking activities for perpetration of crime *Receiving a bribe* of Article 357 Paragraph 1 of the Criminal Code and crime *Abuse of office* of Article 353 of the Criminal Code.

It is likely that data and evidence for successful criminal procedure shall be secured, but cannot be collected by other means.

Special investigative measure *Simulated offering and receiving bribes* of Article 252 Paragraph 1 Item 8 of the CPC incorporates simulated offering of cash as bribe and intermediary activities among persons xxx, through persons xxx and against persons xxx.

The judicial police of the MoI of the Republic of North Macedonia shall implement the special investigative measures, under the control of the public prosecutor.

Equipment owned by the Ministry of Interior of the RM is to be used in implementing the special investigative measures.

The order for the special investigative measure to be issued for a period starting at xxx h on xxx up to xxx h on xxx.

REASONING

The Basic Public Prosecutor's Office has information and evidence that xxx.

Person xxx was reported at the xxx and the Department for prevention of organized and serious crime at xxx h on xxx (date).

Order for special investigative measure *Simulated offering and receiving bribes* of Article 252 Paragraph 1 Item 8 of the CPC against person xxxx under KOIM OSK no. xxx of xxx (date) was issued by the Basic Public Prosecutor's Office Skopje and a pre-trial judge within Basic Court Skopje I Skopje issued order KPP no.xxx of xxx (date) for special investigative measure *Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private* of Article 252 Paragraph 1 Item 3 of the CPC, against xxx.

In addition, the MoI Department for prevention of organized and serious crime submitted a report no. xxx of xxx (date), stating that xxx.

All of the above produces a reasonable suspicion that person xxx is undertaking activities for perpetration of crime *Receiving a bribe* of Article 357 Paragraph 1 of the Criminal Code and crime *Abuse of office* of Article 353 of the Criminal Code and that xxx.

Regarding the abovementioned activities, a public prosecutor issued order KOIM OSK no. xxx of xxx (date) against person xxx for special investigative measure *Simulated offering and receiving bribes* of Article 252 Paragraph 1 Item 8 of the CPC.

In the specific case, data and evidence necessary for a successful criminal procedure cannot be collected by other means, not only because of the type of the listed crimes, but also because these are crimes committed through strict conspiracy between the persons.

Considering the above, I hereby issue this order.

PUBLIC PROSECUTOR

SECRET

SECRET

BASIC PUBLIC PROSECUTOR'S OFFICE

KOIM no.

Skopje, ____ (date)

Based on Article 39 Paragraph 2 Line 2, in relation to Article 256 Paragraph 1 Item 10 and Article 253 Paragraph 2 of the CPC, the public prosecutor in the Basic Public Prosecutor's Office Skopje issues this

ORDER

FOR IMPLEMENTATION of special investigative measure

Use of persons with secret identity for surveillance and collection of information or data of Article 252 Paragraph 1 Item 10 of the CPC,

AGAINST PERSONS:

XXX

XXX

For whom there are grounds for suspicion of undertaking activities for perpetration of crime *Unlawful production and distribution of narcotics, psychotropic substances and precursors* of Article 215 of the Criminal Code.

It is likely that data and evidence for successful criminal procedure shall be secured, but cannot be collected by other means. Special investigative measure *Use of persons with secret identity for surveillance and collection of information or data* of Article 252 Paragraph 1 Item 10 of the CPC would secure evidence of the specific crime and activities undertaken by persons xxx for its perpetration, but also detect other persons involved in the perpetration of the crime.

Special investigative measure *Use of persons with secret identity for surveillance and collection of information or data* of Article 252 Paragraph 1 Item 10 of the CPC incorporates infiltration of an undercover agent that would conduct a simulated purchase of narcotics.

The judicial police of the Mol of the Republic of North Macedonia shall implement the special investigative measures, under the control of the public prosecutor.

Equipment owned by the Ministry of Interior of the RM is to be used in implementing the special investigative measures.

The order for the special investigative measure to be issued for a period of four months, starting at xxx h on xxx up to xxx h on xxx.

REASONING

The Mol Skopje department, Sector for illicit drug trafficking has submitted a report to the Basic Public Prosecutor's Office Skopje SD no.xxx of xxx (date), and at the request of the Basic Public Prosecutor's Office Skopje of xxx (date) KOIM no. xxx of xxx (date) and upon order K-PP no.xxx of xxx (date), issued by a pre-trial judge of the Basic Court xxx, stating that persons xxx are undertaking activities related to the purchase of narcotics xxx in larger quantities, thus committing the crime

Unlawful production and distribution of narcotics, psychotropic substances and precursors of Article 215 Paragraph 1 of the Criminal Code.

Regarding the above, there is reasonable suspicion that persons xxx are undertaking activities for perpetration of crime *Unlawful production and distribution of narcotics, psychotropic substances and precursors* of Article 215 Paragraph 1 of the Criminal Code.

In the specific case, the order for special investigative measure *Use of persons with secret identity for surveillance and collection of information or data* of Article 252 Paragraph 1 Item 10 of the CPC, incorporating the infiltration of an undercover agent in the specific incriminating environment, is to ensure data and evidence necessary for a successful criminal procedure, which cannot be collected by other means, not only because of the type of the listed crimes, but also because these are crimes committed through strict conspiracy between the persons.

Considering the above, I hereby issue this order.

PUBLIC PROSECUTOR

SECRET

SECRET

BASIC PUBLIC PROSECUTOR'S OFFICE

KOIM-OSK NO. /

Skopje, _____ (date)

TO

BASIC COURT SKOPJE 1

- pre-trial judge -

SKOPJE

Based on Article 7, Article 8, Article 11 and Article 15 of the Law on Interception of Communications, in relation to Article 39 Paragraph 2 Line 2, in relation to Article 256, in relation to Article 260 Paragraph 2, in relation to Article 252 Paragraph 1 Item 1 of the CPC, I hereby submit this

**REQUEST
FOR AN ORDER FOR EXTENSION
OF SPECIAL INVESTIGATIVE MEASURE**

Interception and recording of telephone and other electronic communications in a procedure laid down by law of Article 252 Paragraph 1 Item 1 of the CPC.

AGAINST:

- 1., user of telephone number .
- 2., user of telephone number .

The special investigative measure *Interception and recording of telephone and other electronic communications in a procedure laid down by law* of Article 252 Paragraph 1 Item 1 of the CPC incorporates the interception of communications of persons xxx using telephone number ---, xxx using telephone number ---, xxx using telephone number --- and telephone number ---, xxx using telephone number ---, and xxx using telephone number ---, by which they are expected to engage into conversations related to crime *Abuse of office* of Article 353 of the Criminal Code, crime *Receiving a bribe* of Article 357 of the Criminal Code, and crime *Receiving a reward for unlawful influence* of Article 359 of the Criminal Code.

The special investigative measure shall be implemented by using the technical means owned by the Operational Technical Agency and the Ministry of Interior.

The order is to be enforced by the Ministry of Interior of RM, with the Operational Technical Agency as intermediary, under the control of the public prosecutor.

The order is to be issued for a period of one month, starting from xxx h on xxx up to xxx h on xxx.

REASONING

On xxx (date), the Mol of RM, Public Security Bureau, Department for prevention of organized and serious crime within the Bureau submitted to this public prosecutor's office a report under SD no.xxx stating that from the use of the special investigative measure and other operational information, it has been established that the abovementioned persons are continuing to undertake actions towards committing crime *Abuse of office* of Article 353 of the Criminal Code, crime *Receiving a bribe* of Article

357 of the Criminal Code, crime *Receiving a reward for unlawful influence* of Article 359 of the Criminal Code, for which there were previous orders issued for a special investigative measure. The report noted it was additionally discovered that person xxx uses another telephone line xxx, proposing a special investigative measure for that number too.

Considering the above, along with the likelihood of securing data and evidence that is required for a successful criminal procedure, and which cannot be obtained by other means, I hereby submit a request for extension of the special investigative measure *Interception and recording of telephone and other electronic communications in a procedure laid down by law* of Article 252 Paragraph 1 Item 1 of the CPC, against persons xxx, and in view of the abovementioned crimes, a request for a special investigative measure for the new telephone number of the person.

Special investigative measure *Interception and recording of telephone and other electronic communications in a procedure laid down by law* of Article 252 Paragraph 1 Item 1 of the CPC incorporates the interception of communications of persons xxx using telephone number ---, xxx using telephone number ---, and xxx using telephone number ---, by which they are expected to engage into conversations related to the commitment of the crimes.

A pre-trial judge has issued order UOSK no. /14 of xxx (date).

The Mol of RM, Public Security Bureau, Department for prevention of organized and serious crime, Corruption sector has submitted to this public prosecutor's office a report under SD no.xxx of xxx (date), stating that the abovementioned persons are continuing to undertake actions towards committing crime *Abuse of office* of Article 353 of the Criminal Code, crime *Receiving a bribe* of Article 357 of the Criminal Code, crime *Receiving a reward for unlawful influence* of Article 359 of the Criminal Code. Considering the prior use of the special investigative measure and the likelihood of securing data and evidence that is required for a successful criminal procedure, and which cannot be obtained by other means, a request is submitted for extension of the special investigative measure.

The special investigative measure *Interception and recording of telephone and other electronic communications in a procedure laid down by law* of Article 252 Paragraph 1 Item 1 of the CPC incorporates the interception of communications of persons xxx using telephone number ---, xxx using telephone number ---, by which they are expected to engage into conversations related to the perpetration of the crimes.

The order is to be enforced by the Ministry of Interior of RM, with the Operational Technical Agency as intermediary, under the control of the public prosecutor.

PUBLIC PROSECUTOR

SECRET

SECRET

BASIC PUBLIC PROSECUTOR'S OFFICE

KOIM no. /

Skopje, _____ (date)

TO

BASIC COURT SKOPJE 1

- pre-trial judge -

SKOPJE

Based on Article 39 Paragraph 2 Line 2, in relation to Article 256, Article 252 Paragraph 1 Item 3 and Article 253 Item 2 of the CPC, I hereby submit this

REQUEST

**FOR AN ORDER FOR EXTENSION OF THE IMPLEMENTATION OF THE
SPECIAL INVESTIGATIVE MEASURE**

Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private of Article 252 Paragraph 1 Item 3 of the CPC,

AGAINST PERSONS:

The special investigative measure *Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private* of Article 252 Paragraph 1 Item 3 of the CPC incorporates secret surveillance and recording of persons xxx and objects by using technical devices outside the home or office space designated as private, because there are grounds for suspicion over their involvement in the perpetration of crime *Abuse of office* of Article 353 of the Criminal Code, crime *Receiving a bribe* of Article 357 of the Criminal Code and crime *Receiving a reward for unlawful influence* of Article 359 of the Criminal Code.

It is likely that data and evidence for successful criminal procedure shall be secured, but cannot be collected by other means.

The judicial police shall implement the special investigative measures, under the control of the public prosecutor.

Equipment owned by the Ministry of Interior of the RM is to be used in implementing the special investigative measures.

The order is issued for a period of one month, starting at xxx h on xxx up to xxx h on xxx.

REASONING

On xxx (date), the Mol of RM, Public Security Bureau, Department for prevention of organized and serious crime within the Bureau submitted to this public prosecutor's office a report under no.xxx stating that from the use of the special investigative measure and other operational information, it has been established that the abovementioned persons are continuing to undertake actions towards committing crime *Abuse of office* of Article 353 of the Criminal Code, crime *Receiving a bribe* of Article

357 of the Criminal Code, crime *Receiving a reward for unlawful influence* of Article 359 of the Criminal Code, for which there were previous orders issued for a special investigative measure.

The pre-trial judge within Basic Court Skopje 1 issued an order KPP no. xxx of xxx for extension of the special investigative measure *Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private* of Article 252 Paragraph 1 Item 3 of the CPC.

Considering the above, along with the likelihood of securing data and evidence that is required for a successful criminal procedure, and which cannot be obtained by other means, I hereby submit a request for extension of the special investigative measure *Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private* of Article 252 Paragraph 1 Item 3 of the CPC, against persons xxx, and in view of the abovementioned crimes.

Special investigative measure *Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private* of Article 252 Paragraph 1 Item 3 of the CPC considers that data and evidence required for a successful criminal procedure cannot be obtained by other means, but also because these are crimes committed through strict conspiracy between the persons. Therefore I hereby submit a Request for extension of the special investigative measure for persons xxx.

In accordance with Article 258 Paragraph 2 of the CPC, the judicial police shall draft a separate report upon the measure's implementation and submit it to the public prosecutor.

PUBLIC PROSECUTOR

SECRET

SECRET

THE BASIC COURT, proceeding upon a request by the Basic Public Prosecutor's Office KOIM no. of X, for an order for termination of the implementation of a special investigative measure, in accordance with Article 256 and Article 260 of the CPC, on xxx issues the following:

**ORDER
TO TERMINATE THE IMPLEMENTATION
OF THE SPECIAL INVESTIGATIVE MEASURE:**

Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private of Article 252 Paragraph 1 Item 3 of the CPC,

AGAINST PERSON:

X birth reg.no. X employed as XXX
applied by order KPP no. XXX (date).
because the grounds for its approval have ceased to exist.

REASONING

The Basic Public Prosecutor's Office Skopje submitted a Request for an order for termination of special investigative measure *Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private* of Article 252 Paragraph 1 Item 3 of the CPC to a pre-trial judge of this court under KOIM no.XXX, against person XXX for crime XXX of the Criminal Code.

The proposal by the Basic Public Prosecutor's Office states that information and evidence required for a successful criminal procedure, which could not be collected by other means, were obtained in the course of the enforcement of the special investigative measure against person XXX for crime XXX of the Criminal Code. The measure was applied until X (date) through documented meetings and events, when person X was detained at X h due to a reasonable suspicion of committing crime X of the Criminal Code, and therefore the grounds for the application of the special investigative measure cease to exist in full.

This order terminates the implementation of special investigative measure *Secret surveillance and recording of persons and items by technical devices outside the home or office space designated as private* of Article 252 Paragraph 1 Item 3 of the CPC against person X upon whom the special investigative measure was applied by an order of a pre-trial judge of the Basic Court for crime X of the Criminal Code.

Taking into consideration the findings in the request for termination of the implementation of the special investigative measures, the pre-trial judge found it as being substantiated and decided as in the wording of the decision.

BASIC COURT X,
KPPm no. of X (date)

Pre-trial judge

SECRET



PUBLIC PROSECUTOR'S OFFICE OF REPUBLIC OF NORTH MACEDONIA

OSK no.-/2019

Skopje, _____ (date)

**To
SUPREME COURT OF THE REPUBLIC
OF NORTH MACEDONIA
SKOPJE**

Based on Article 20 in relation to Articles 18, 19 and 21 of the Law on Interception of Communications (Official Gazette of Republic of Macedonia no.71 of 19 April 2018), I hereby submit this

**REQUEST
FOR AN ORDER FOR INTERCEPTION OF COMMUNICATIONS**

1. Interception and recording of telephone and other electronic communications of Article 18 Paragraph 1 Item 1 of the Law on Interception of Communications

AGAINST PERSON:

- **N.N.**, of father N and mother N, born on ----- in -----, residing at st. ----- no. ----- in C., Birth Registry Number _____
- user of telephone number _____
- identification number JOM _____
- identification number JOM _____

Due to the existence of grounds for suspicion that perpetration of a crime against the state "*Terrorist endangerment of the constitutional order and security*" of **Article 313** of the Criminal Code of the Republic of Macedonia is in preparation.

The grounds for suspicion arise from the operational information of the National Security Agency, listed in the proposal DT no.____ of ----- and report DT no.____ of -----.

The order for interception of communications for the purpose of protecting the interests of state security and defense incorporates interception and recording of telephone and other electronic communications of person N.N., user of telephone number _____, identification number JOM, _____, identification number JOM _____.

The order for implementation of the measure for interception of communications for the protection of the interests of state security and defense is to be enforced by the authorized institution, in accordance with Article 4, Paragraph 1, Item 7 of the Law on Interception of Communications, using the equipment for that purpose in the work station, in compliance with Article 4 Paragraph 1 Item 21 of the Law on Interception of Communications, with the Operational Technical Agency as intermediary by providing the technical link between the operator and the authorized institution for the measure's enforcement, in compliance with Article 64 of the Law on Interception of Communications, and Articles 2 and 3 of the Law on the Operational Technical Agency (Official Gazette of RM no.71 of 19 April 2018).

The order for interception of communications to be issued from 13:00h on ???.?.2019 up to 13:00h on ???.?.2019.

REASONING

The National Security Agency has submitted a proposal to the Public Prosecutor's Office of the Republic of Macedonia for an order for implementation of the measure for interception of communications, in accordance with Article 20 Paragraph 1 of the Law on Interception of Communications (Official Gazette of the Republic of Macedonia no.71 of 19 April 2018) DT no. _____ of ---- 2018.

The proposal states that an informal group of followers of the extreme Salafism is operating in the Republic of Macedonia, making attempts to infiltrate in closed communities through the observance of Sharia way of life and complete distancing from the democratic norms and freedoms of citizens, which has resulted in the isolation of the group members as a form of parallel society. Namely:

After serving prison sentences, Islamic militants and former Jihadists started to incite previously selected followers into organizing activities that would lead to terrorist endangerment of the state, i.e. establishment of Sharia isolated environments where the Sharia law would be fully applied. According to obtained information, they urged for the Sharia law to be promptly implemented, otherwise they would start to use force, violence and Jihad.

The abovementioned individuals are in direct communication with the Salafi imams and others, who besides regular religious teachings, secretly meet with selected individuals for private religious and physical training. The selected individuals include Islamic State fighters returning from Syria, who have formed Salafi groups upon their return, where members receive religious and physical training.

N.N. has been recruited by the religious authorities for a higher level of physical training. Mutual closed visits of selected individuals have been registered in the recent period, for the purpose of organizing religious teachings and drills in nature, including elements of military training, the aim being the establishment of Sharia isolated environments with complete application of the Sharia law.

Data and information over the operations of this informal group of mutually related individuals cannot be collected by other means and we therefore believe that the measure for interception of communications *Interception and recording of telephone and other communications* should be applied, in accordance with Article 18 Paragraph 1 Item 1 of the Law on Interception of Communications.

The order for implementation of the measure for interception of communications for the purpose of protecting the interests of state security and defense is to be enforced by the authorized institution in accordance with Article 4, Paragraph 1, Item 7 of the Law on Interception of Communications, using the equipment for that purpose in the work station, in compliance with Article 4 Paragraph 1 Item 21 of the Law on Interception of Communications, with the Operational Technical Agency as intermediary by providing the technical link between the operator and the authorized institution for the measure's enforcement, in compliance with Article 64 of the Law on Interception of Communications, and Articles 2 and 3 of the Law on the Operational Technical Agency (Official Gazette of RM no.71 of 19 April 2018).

The order for interception of communications to be issued from 13:00h on ???.?.2019 up to 13:00h on ???.?.2019.

**PUBLIC PROSECUTOR
NN**

TOP SECRET

JUDGE OF THE SUPREME COURT OF THE REPUBLIC OF NORTH MACEDONIA N.N., proceeding at the request of the Public Prosecutor's Office of the Republic of North Macedonia OSK no. __/2019 of ____ (date) on an order for interception of communications, in accordance with Articles 21 and 22 of the Law on Interception of Communications ("Official Gazette of RM" no.71/2018 of 19 April 2018) and Articles 2 and 3 on the Law on the Operational Technical Agency, issued on ____ (date) the following:

ORDER

Due to grounds for suspicion that the perpetration of crime against the state *Terrorist endangerment of the constitutional order and security* of Article 313 of the Criminal Code, *Murder of representatives of highest state authorities* of Article 309 of the Criminal Code, and *Violence against representatives of the highest state authorities* of Article 311 of the Criminal Code are in preparation, **HEREBY ORDERS:**

AGAINST PERSONS:

1. **XXX.**,

- user of telephone number _____
- identification number PPO _____
- identification number PPO _____

2. **XXX.**,

- user of telephone number _____
- identification number PPO _____
- identification number PPO _____

3. **XXX.**,

- user of telephone number _____
- identification number PPO _____
- identification number PPO _____

INTERCEPTION AND RECORDING OF TELEPHONE AND OTHER ELECTRONIC COMMUNICATIONS

This order for implementation of the measure for interception of communications for the purpose of protecting the interests of state security and defense to be enforced by an authorized institution - National Security Agency, with the Operational Technical Agency as the intermediary, which provides the technical link between the operator and the authorized institution for the measure's implementation.

The order for the interception of communications to be issued for a period of six months, starting at 15:30h on ____ up to 15:30h on ____.

¹ The Supreme Court template of an order to the PPORNM - the order is not anonymized in accordance with the law and the internal rulebook and therefore data it contains is underscored and the template is printable. The Supreme Court template for an order to OTA is anonymized and contains XXXXXXXXXX in that section, and data on a template that is not printable is underscored.

The applicant must submit the reports obtained from the authorized institution, in line with Article 27 of the Law on Interception of Communications, within three days from their reception.

REASONING

The Public Prosecutor's Office of the Republic of North Macedonia submitted a Request for an order for interception of communications to the judge of this court on ____ based on Article 20 of the Law on Interception of Communications, asking for the issuance of an order for interception and recording of telephone and other electronic communications of persons N.N. due to suspicion that the execution of crime against the state *Terrorist endangerment of the constitutional order and security* of Article 313 of the Criminal Code, *Murder of representatives of highest state authorities* of Article 309 of the Criminal Code, and *Violence against representatives of the highest state authorities* of Article 311 of the Criminal Code are in preparation. The request was accompanied by a proposal DT no. _____ of ____ (date) and report DT no. _____ of ____ (date) of the National Security Agency.

This court assessed the merits of the request and established, based on the findings of the request and the proposal, that the criteria to issue an Order in line with Article 21 of the Law on Surveillance of Communications have been met. The order is to be implemented with the Operational Technical Agency as intermediary, ensuring the technical link between the operator and the authorized institution for implementation of the measure in accordance with Articles 2 and 3 of the Law on the Operational Technical Agency ("Official Gazette of RM" no.71/2018 of 19 April 2018).

SUPREME COURT OF THE REPUBLIC OF NORTH MACEDONIA

SSK.no. _/2019-PPORNM of ____ (date)

**Judge,
N.N.**

TOP SECRET

TOP SECRET

**PUBLIC PROSECUTOR'S OFFICE
OF THE REPUBLIC OF NORTH MACEDONIA
OSK no. --/2019
Skopje, _____ (date)**

**To
SUPREME COURT OF THE REPUBLIC OF
NORTH MACEDONIA
SKOPJE**

Based on Article 29 and Article 33 in relation to Article 30 Paragraph 3 of the Law on Interception of Communications, I hereby submit this:

**REQUEST
FOR AN ORDER FOR EXTENSION OF INTERCEPTION OF COMMUNICATIONS**

LIAISON: SSK no.---/20—of ---

AGAINST PERSONS:

1. **N.N.**, born on ----- (date) in ---, residing at str.----- no.--- in ---, birth reg.no._____
- user of telephone number -----
2. **N.N.**, born on ----- (date) in ---, residing at str.----- no.--- in ---, birth reg.no._____
- user of telephone number -----

Due to grounds for suspicion of preparing, inciting and organizing the perpetration of crime against the state *Terrorist endangerment of the constitutional order and security* of Article 313 of the Criminal Code.

The grounds for suspicion arise from the operational knowledge of the National Security Agency listed in proposal DT no. ____ of ____ (date) and report DT no. ____ of ____ (date).

The order for interception of communications encompasses the interception of all types of telephone communications of persons NN as user of telephone number ----- and NN as user of telephone number -----.

Equipment owned by --- is to be used in implementing the order for interception of communications.

The Operational Technical Agency carries out the order for interception of communications.

The order for interception of communications is to be issued for a period starting from 12:00h on xxx up to 12:00h on xxx.

REASONING

The National Security Agency has submitted a proposal to the Public Prosecutor's Office of the Republic of Macedonia for interception of communications DT no.____ of ----- , against persons NN and NN, for which Order SSK no.--/20—of ----- has been issued.

The request states that the National Security Agency had learned that the security situation in Syria/Iran, the current military engagement of the Syrian, Iraqi and other foreign armies against certain paramilitary formations that have lately been retreating from the previously conquered terri-

tories and surrendering to the Syrian and Iraqi armies, has not resulted in a drop of the support by individuals and groups in R.Macedonia to these paramilitary formations.

According to obtained information, several imams from R.Macedonia who promote the Salafi ideology have started to incite previously selected followers into organizing violent activities in R.Macedonia. Upon their instruction, NN and NN should select and recruit selected individuals to commit a terrorist act or occasional acts of violence in the state towards causing fear and panic among the population and demonstrating presence of "Sharia fighters in the region". In this regard, these persons hold secret meetings for the purpose of instructing individuals into preparation for terrorism acts and selecting their assistants.

It has been established from the application of the measure that NN, besides using the telephone number at which the measure has been directed, has also used telephone number -----, while NN besides using the telephone number at which the measure has been directed, has also used telephone number -----.

Considering the type and character of activities undertaken by the abovementioned individuals, there are grounds for suspicion that perpetration of crimes against the state is prepared, incited and organized - *Terrorist endangerment of the constitutional order and security* of Article 313 of the Criminal Code.

The interception of communications will ensure timely undertaking of measures for protection of the sovereignty, territorial integrity and security of the state, registration of points for spreading of the militant ideology and its neutralization, identification of members of militant groups for the purpose of timely prevention of their violent activities, identification of possible locations where physical training is carried out etc.

Data or evidence cannot be collected by other measures and I therefore believe the measure of interception of communications should be applied.

Considering the above, I find that an Order for interception of communications is reasonable due to the existence of grounds for suspicion of preparing, inciting and organizing the perpetration of crime against the state *Terrorist endangerment of the constitutional order and security* of Article 313 of the Criminal Code.

The grounds for suspicion arise from the operational knowledge of the National Security Agency listed in proposal DT no. ____ of ----- and report DT no. ____ of -----.

The order for interception of communications encompasses the interception of all types of telephone communications of persons NN as user of telephone number ----- and NN as user of telephone number -----.

Equipment owned by --- is to be used in implementing the order for interception of communications.

The Operational Technical Agency carries out the order for interception of communications.

The order for interception of communications is to be issued for a period starting from 12:00h on --- up to 12:00h on ---.

**PUBLIC PROSECUTOR
NN**

TOP SECRET

TOP SECRET

OSK no. --/18

Skopje ____ (date)

**To
SUPREME COURT OF THE REPUBLIC OF
NORTH MACEDONIA
SKOPJE**

LIAISON: SSK--/2018

Based on Article 25 in relation to Articles 20, 18, 19 and 21 of the Law on Interception of Communications (Official Gazette of RM no.71 of 19 April 2018), I hereby submit this:

**REQUEST
FOR AN ORDER FOR TERMINATION OF MEASURE FOR INTERCEPTION AND RECORDING OF
TELEPHONE AND OTHER ELECTRONIC COMMUNICATIONS**

AGAINST PERSONS:

1. XXX

- user of telephone number _____
- identification number JOM _____
- identification number JOM _____

2. XXX

- user of telephone number _____
- identification number JOM _____
- identification number JOM _____

due to **inactivity** of the abovementioned telephone numbers.

REASONING

The National Security Agency submitted a proposal to the Public Prosecutor's Office of the Republic of Macedonia for an order for termination of the measure for interception and recording of telephone and other electronic communications DT no. ____ of ----- (date), based on Article 25 Paragraph 1 of the Law on Interception of Communications (Official Gazette of RM no.71 of 19 April 2018).

The proposal states there is no activity at telephone numbers of persons XXX and XXX.

Since the grounds for approval of the measure of interception and recording of telephone and other electronic communications by an Order of the Supreme Court of the Republic of Macedonia SSK??/2018 of ???????? (date), for these telephone numbers, have ceased to exist, I hereby propose the termination of the measure of interception and recording of telephone and other electronic communications.

**PUBLIC PROSECUTOR
NN**

TOP SECRET



Geneva Centre for Security Sector Governance (DCAF) promotes good governance and reforms in the security sector. The Centre conducts research on good practices, promotes the development of national and international norms, drafts the recommendations on policies and ensures advisory and assistance programmes in the country. DCAF's partners include governments, parliaments, civil society, international organizations, and range of services in the security sector, including military, police, judicial, intelligence agencies and border security services.

Visit us at www.dcaf.ch

Technical design:
Polyesterday

Print:
Polyesterday

Circulation:
500

