Promoting, Shaping and Upholding Internet Freedoms Project

ANALYSIS OF THE LEGAL FRAMEWORK FOR INTERCEPTION OF COMMUNICATIONS AND IMPLEMENTATION THEREOF

Author:
Aleksandar Nikolov


МЕТАМОРФОЗИС
Фондација за интернет и општество


APC
ASSOCIATION FOR
PROGRESSIVE
COMMUNICATIONS

INTRODUCTION

This analysis aims to provide an overview of the situations with the legal frameworks related to media in the Republic of Macedonia in the past and current period as well. It is developed as part of the activities of the Promoting, Shaping and Upholding Internet Freedoms Project implemented by Foundation for Internet and Society, Metamorphosis, and supported by the Association for Progressive Communications (APC).

Main objectives of the Promoting, Shaping and Upholding Internet Freedoms Project are: promoting knowledge and understanding of situation related to protection of the fundamental human rights online in the Republic of Macedonia, CSO and media capacity building, facilitating the process of sharing knowledge and good practices among citizens, CSOs and media.

The content of the paper is the sole responsibility of the authors and in no way reflects the views of the Foundation for Internet and Society, Metamorphosis, and Association for Progressive Communications (APC).

ANALYSIS OF THE LEGAL FRAMEWORK FOR INTERCEPTION OF COMMUNICATIONS AND IMPLEMENTATION THEREOF

The reforms of the 2018 system for interception of communications paved the way for passing the new **Law on Interception of Communications** [1]and for amending the **Law on Electronic Communications (LEC)**[2] with which the Administration for Security and Counterintelligence (UBK) was deprived of its direct access to citizens' telecommunication traffic and its role as a mediator in the interception of communications - a request that was part of European Commission's 2015 Urgent Reform Priorities[3]. The Law on Interception of Communications allows interception of communications for the purpose of detecting and prosecuting perpetrators of crimes as well as for protection of the country's interests in defense and security - both purposes are in keeping with the Constitution and the Urgent Reform Priorities.

The **Law on Operational-Technical Agency** [4] allowed the creation of a new body (OTA), which since November 2018 has had the role of a mediator between the authorized bodies for interception of communications and the telecom operators, with the aim to avoid concentration of power in one authority and to ensure interception of communications based only on laws and relevant court decisions. The Law governs the remit and managing of OTA, expert oversight and its funding. According to the law, some UBK staff should have joined the OTA, but it was unclear how persons who had been previously involved in the abuse of the system for the interception of communications will be prevented from forming part of that staff.

In February 2019, the **Bill on National Security Service** (NSS) was introduced in the legislature, which projects ceasing of UBK's operations. As of June

1 Law on Interception of Communications, Official Gazette of the Republic of Macedonia no. 71/2018.
2 Law on Electronic Communications, Official Gazette of the Republic of Macedonia no. 39/2014, 188/2014, 44/2015, 193/2015, 11/2018 and 21/2018.
3 Available at: https://eeas.europa.eu/sites/eeas/files/urgent_reform_priorities_en.pdf
4 Official Gazette of the Republic of Macedonia no. 71/2018.

2019, the National Security Service is supposed to replace the UBK, which will not form part of Ministry of Interior's organogram. The Service should collect, process, analyze, assess, exchange, keep and protect data and information with the aim to detect and prevent activities related to safety threats and risks to national security. The Service shall permanently monitor the telecommunication lines, electronic communications, audio recordings in rooms, and audio, video and photographing at open spaces, inquiry in the communication metadata of citizens as well as collect data and information from natural and legal entities and other relevant parties. Some UBK staff is supposed to join the NSS, but it is unclear how persons who had been previously involved in the abuse of the system for the interception of communications will be prevented from forming part of that staff.

The amendments of 2018 and 2019 are not aligned with the EU acquis, more specifically the Police and Criminal Justice Data Protection Directive[5], the verdict of the European Court of Justice that annulled the Data Retention Directive 2006/24/EC, as well as the relevant case law of the European Court of Justice and the European Court of Human Rights. These sources of the EU acquis were neither identified in the regulatory impact assessments nor in the rationales on the legislative initiatives that the Government delivered to the Parliament. Our legislation doesn't prescribe all personal data protection mechanisms comprised in the Directive 2016/680, doesn't set an adequate limit of data collection to what's directly needed and relevant for a specific purpose[6], doesn't prescribe a right to nonprofits operating in the interest of individuals to lodge complaints and represent the concerned persons[7], doesn't introduce an obligation for notifying persons in the event of violation of collected personal data.[8]

...5

Below is a brief description of other domestic acts that are relevant to the interception of communications.

The Constitution of the Republic of Macedonia guarantees the freedom and inviolability of correspondence and other forms of communication.

5 Directive 2016/680
6 So-called data minimization principle
7 Articles 52-55 of the Directive.
8 Article 31 of the Directive.

Only a court decision, under conditions and in a law-stipulated proceeding, may authorize non-application of the principle of the inviolability of the correspondence and other forms of communication, in cases where it is indispensable to a criminal investigation or required in the interests of the defense of the Republic.[9] The security and confidentiality of personal information are guaranteed. Citizens are guaranteed protection from any violation of their personal integrity deriving from the registration of personal information through data processing.[10]

The interception of communications is laid down as a special investigation measure in the **Law on Criminal Procedure**.[11] These measures are regulated in Chapter XIX, wherein the law stipulates the special investigation measures - among which is monitoring and recording of the telephone and other electronic communications - when it is necessary to obtain data and evidence the criminal procedure, **which cannot be obtained by other means.** According to the Law on Criminal Procedure, in one of the special investigation measures[12], the recording shall be stopped, if, during the recording, there are indications that it might be possible for statements to be recorded, which belong in the basic sphere of private and family life. Any documentation on such statements shall be destroyed immediately. [13]

Similarly, **the Law on Personal Data Protection**[14] envisages special categories of personal data which must not be processed, i.e. can be processed but under special conditions. This part of the law should be applicable to the data processing during the interception of communications, which includes: personal data revealing the racial or ethnic origin, the political views, religious or philosophical or other beliefs, membership in a trade union and data relating to the health condition of the people, including genetic data,

9 Amendment XIX which replaces article 17.
10 Article 18 of the Constitution.
11 Official Gazette of the Republic of Macedonia no. 150/2010, 100/2012, 142/2016 and 198/2018.
12 Surveillance and recording in homes, closed up or fenced space that belongs to the home or office space designated as private or in a vehicle and the entrance of such facilities in order to create the required conditions for monitoring of communications.
13 Article 268 of the Law on Criminal Procedure.
14 Official Gazette of the Republic of Macedonia no. 7/2005, 103/2008, 124/2010 and 135/2011, 43/2014, 153/2015, 99/2016 and 64/2018.

biometric data or data referring to the sexual life.

The Law on Electronic Communications (LEC)[15] regulates the confidentiality of communications, as regards their content, but also of the data on communication traffic and location data. Confidentiality exemptions refer to the application of the Law on Interception of Communications, retention of user metadata, technical keeping of data necessary for transfer of communications as well as recording of communications and relevant data on communication traffic due to obtaining evidence of commercial transactions. The Law already obliges the operators to undertake technical and organizational measures for appropriate risk management of networks and services safety, particularly to prevent and minimize the effect on users.[16]

KEY SOURCES OF RELEVANT INTERNATIONAL LAW

- Universal Declaration of Human Rights of the United Nations;
- International Covenant on Civil and Political Rights of the United Nations;
- European Convention on Human Rights;
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe;
- Directive 2016/680 on Protection of Police and Criminal Justice Data;
- The case law of the European Court of Human Rights and the European Court of Justice in cases of interception of communications, privacy protection, and personal data.
- Праксата на Европскиот суд за човекови права и Европскиот суд на правдата во случаите со следење на комуникациите, заштита на приватноста и личните податоци.

15 Law on Electronic Communications, Official Gazette of the Republic of Macedonia no. 39/2014, 188/2014, 44/2015, 193/2015, 11/2018 and 21/2018.

16 Article 166 of the Law on Electronic Communications.

1

TYPES OF INTERCEPTION OF COMMUNICATIONS ALLOWED BY LAW

TYPES OF INTERCEPTION OF COMMUNICATIONS ALLOWED BY LAW

The Law on Interception of Communications covers all types of telephone and other electronic communications such as internet protocol, speech through internet protocol, website, and e-mail.[17] Defined like this, the interception of communications covers communications via internet apps for transfer of voice, video and other content (for example: *Skype, Viber, Snapchat, WhatsApp, FaceTime*). The Law on Interception of Communications envisages possibilities for interception of non-telecom communications, including recording of communications inside objects or on open spaces as well as photographing and video recording on open spaces.

The Law on Electronic Communications already obliges all telecom and internet providers to retain the so-called "metadata" for all of their users for one year i.e. data on time, persons we communicate with, type of communication, types of devices we use, the location as well as geo-tracking of the telephone devices.[18] Metadata is generated regardless of whether the people are engaging in any communication activity. For example, the e-mail apps on smartphones communicate with the so-called cell towers of the mobile operators in very short time intervals, thus constantly generate and retain data on mobile phone's location and the direction of moving of its user. Although the Public Prosecutor, the Administration for Security and Counterintelligence and other authorities[19] have the right to an inquiry in our communication metadata that is collected by the operators, this is not

17 Article 4 of the Law on Interception of Communications.
18 Law on Electronic Communications, articles 176, 178 and 181.
19 The Military Security and Intelligence Administration and the Army Centre for Electronic Reconnaissance.

covered by the definition of interception of communications in the Law on Interception of Communications.[20]

This last fact does not comply with the Venice Commission Rule of Law Checklist[21], which clearly states that even covert collection of metadata on electronic communications is interception of communications. The introduction of the provisions on mass retention of communication metadata in our Law on Electronic Communications (LEC) was justified as transposing of the Directive 2006/24/EC.[22] However, soon after the new LEC was enacted in 2014, the European Court of Justice declared the Directive invalid. The Court ruled that the *mass* retention of communication metadata violates the right to private life and right to individuals' personal data protection, guaranteed by articles 7 and 8 of the EU Charter of Fundamental Rights. [23] Despite the fact that amendments to the relevant laws were initiated and adopted in 2018 and 2019, the state still hasn't taken measures to align the metadata retention with the EU acquis.

RECOMMENDATIONS - HOW TO ALIGN THE TYPES OF ALLOWED INTERCEPTION OF COMMUNICATIONS WITH THE CONSTITUTION AND THE EU ACQUIS?

- To repeal articles 176 and 178 of the Law on Electronic Communications, which stipulate mass retention of communication metadata regarding **all** citizens, due to the abolishment of the Directive 2006/27/EC by the European Court of Justice that is transposed in this law.
- The interception of and inquiry in metadata on electronic communications of **specific** persons and objects to be covered by the definition of interception of communications in the Law on Interception of Communications.

20 Ironically, the Law on Interception of Communications does not include the inquiry in the communication metadata in the definition of interception of communications, however, it regulates the right and manner of exercise of such inquiry.

21 Available at: http://www.venice.coe.int/images/SITE%20IMAGES/Publications/Rule_of_Law_Check_List.pdf

22 Data Retention Directive 2006/24/EC.

23 Joined cases C-293/12 and 594/12.

2

INITIATING COURT APPROVAL FOR THE INTERCEPTION OF COMMUNICATIONS TOO

INITIATING COURT APPROVAL FOR THE INTERCEPTION OF COMMUNICATIONS TOO

According to the Law on Interception of Communications, the court may order interception of communications due to detection and prosecution of perpetrators of crimes or due to the interests of the defense of the country. The table below provides an overview of the main similarities and differences between the provisions for interception of communications based on the following two bases.

...15

	Interception of communications due to detection and prosecution of perpetrators of crimes	Interception of communications due to security and defense
Basis	Detection and prosecution of perpetrators of crimes	Preparation of crime against the state, armed forces or against humanity and international law; preparation, instigation, organization or participation in an armed attack against the state or disabling the security system; prevention of terrorist organization, terrorism and financing terrorism

	Interception of communications due to detection and prosecution of perpetrators of crimes	Interception of communications due to security and defense
Applicant of a request for interception of communications	The competent public prosecutor upon their own initiative or upon the motion of the judicial police	The public prosecutor upon the motion of the Minister of interior, the Minister of defense or a person authorized by any of them For access to communication metadata of citizens collected by the telecom operators: the Administration for Security and Counterintelligence, the Military Security and Intelligence Administration orthe Army Centre for Electronic Reconnaissance
Duration of the interception	Up to 4 months, with a possibility for severalfold extension of up to 4-6 months for each extension, upon the request of the public prosecutor, but not more than 14 months in total	Up to 6 months, with a possibility for extension, but not more than 24 months in total
Judge that issues an order for interception of communications	Judge in the preliminary procedure For access to citizens' communication metadata, the laws do not require the court's approval of the request The Public Prosecutor submits the request directly to the telecommunications operator.	Designated Supreme Court judge For access to citizens' communication metadata, the laws do not require the court's approval of the request UBK and other authorities submit the request directly to the operator, while the Public Prosecutor confirms the justification within 48 hours.

	Interception of communications due to detection and prosecution of perpetrators of crimes	Interception of communications due to security and defense
Deadline for the judge to rule on the request for interception of communications	72 hours, while in emergency cases they can issue a temporary written order within 12 hours, which is valid for 48 hours	24 hours, while in emergency cases they can immediately issue a temporary written order, which is valid for 48 hours
Objection for the denied request is submitted to	Three-member council of judges of the competent Basic Court	Three-member council of judges of the Supreme Court

The impression that there is a broad scope of crimes for which interception of communications is allowed remains. According to a relevant recommendation of the Council of Europe, the special investigation measures should be used for the purpose of detecting and investigating serious crimes.[24] According to a UN Convention, serious crime is conduct constituting an offense punishable by a maximum deprivation of liberty of at least four years or a more serious penalty;[25] However, apart from crimes that require interception of communications for the purpose of prosecution or prevention thereof, interception of communication is also allowed for crimes punishable by a minimum of six months in prison.

The overview above reveals a serious problem with regard to the access to citizens' communication metadata which the telecomunication operators is obliged to retain 12 months for all users - it can be used by authorized bodies without a court order. That runs counter the Amendment XIX of the Constitution, which replaces article 17, according to which the inviolability of correspondence and other forms of communication can be violated only on the basis of a court order. According to the Venice Commission Rule of Law Checklist procedural control and oversight need to be in place, including issuing an authorization by a judge or an independent body, even in cases of interception of telecom traffic metadata of a specific person. The case law

24 Council of Europe Committee of Ministers, Recommendation Rec (2005) 10 of the Committee of Ministers to member states on "special investigative techniques" in relation to serious crimes including acts of terrorism.

25 The United Nations Convention Against Transnational Organized Crime, Article 2.

of the European Court of Human Rights[26] confirms that the absence of prior approval of access to citizens' communication metadata - of a court or an independent body - is a violation of the right to privacy pursuant to article 8 of the European Convention on Human Rights.

The legislative amendments from April 2018 replaced the oral order for emergency interception of communications - for instance if the criminal procedure might suffer consequences - with a temporary written order. However, the new Law on Interception of Communications does not prescribe more precise conditions that will demonstrate a need for an emergency. The law that was in force until 2012 justified emergency only in cases of danger of causing death or serious injury, causing material damage of vast property or escaping of a perpetrator of a crime that is not punishable by life imprisonment.

The number of authorized bodies for interception of communications has been increased in the new Law on Interception of Communications due to the protection of interests of defense and security, by adding the Military Security and Intelligence Administration. Additionally, the already brief deadline for court approval of requests for interception of communications on this basis is shortened from 24 to just 12 hours, as opposed to the increased time for court ruling when interception of communications for the purpose of criminal prosecution has been requested. The intercepted communications on the basis of protection of defense and security can be used as indications for criminal prosecution[27], which is unrelated to defense and security, according to the Law on Interception of Communications. That is problematic since it does not comply with the scope of the court order for interception of communications and the data is used for a purpose different than the one it has been collected for.

During the court's ruling on requests for interception of communications, the Law on Interception of Communications prescribes the "right to objection" only in cases when the request is denied by a competent judge, while there isn't such right when it comes to the protection of the rights and interests

26 Example: Big Brother Watch and Others v. the United Kingdom, nos. 58170/13, 62322/14, 24960/15, ECHR 2018, Judgment of 13 September 2018, paragraph 467.
27 Article 28.

of persons whose communications are proposed to be intercepted. The fact that there isn't any data of judges that have denied at least one request for interception of communications provides space for doubt that this one-sided "right to objection" pressures the judges to approve all requests.

RECOMMENDATIONS - HOW TO IMPROVE THE PROCEDURE FOR INITIATING COURT APPROVAL FOR INTERCEPTION OF COMMUNICATIONS?

- To re-examine the justification for the interception of communication for such a broad scope of crimes on the basis of the assessment whether the violation of privacy is proportional to the seriousness of the crime in question and the evidence that is expected to be collected with the special investigation measures i.e. interception of communications. According to a relevant recommendation of the Council of Europe, the special investigation measures should be used for the purpose of detecting and investigating serious crimes.[28] According to a UN Convention, serious crime is conduct constituting an offense punishable by a maximum deprivation of liberty of at least four years or a more serious penalty;[29]
- To amend the Law on Interception of Communications and the Law on Criminal Procedure as regards the interception, while the inquiry in metadata for electronic communications should be based on previously issued court order that will list **specific** persons or communication devices, in keeping with the Amendment XIX to the Constitution, instead of the current solution according to which metadata of all citizens is collected on a large scale, and the authorized bodies have access to it without a court decision.
- To introduce one more party in the procedure for approving interception of communications which will represent the interests of persons whose communications are proposed to be intercepted (for example a panel of experts, representative of the Directorate for Personal Data Protection or the Ombudsman). This party should be enabled to object to requests for interception of communications

28 Council of Europe Committee of Ministers, Recommendation Rec (2005) 10 of the Committee of Ministers to member states on "special investigative techniques" in relation to serious crimes including acts of terrorism.

29 The United Nations Convention Against Transnational Organized Crime:

as well as orders for interception of communications if it deems that citizens' privacy and personal data are unjustifiably violated.

- To introduce an obligation for performing security assessment before deciding whether interception of someone's communications due to the protection of country's interests of defense and security should be requested, and it should form part of the request delivered to a Supreme Court judge by the Public Prosecutor.
- To strengthen the expertize and ethics of public prosecutors and judges in the area of interception of communications, privacy and protection of personal data; to provide external support for the implementation of the European standards in this sphere, including training sessions and specialization for prosecutors and judges.

3

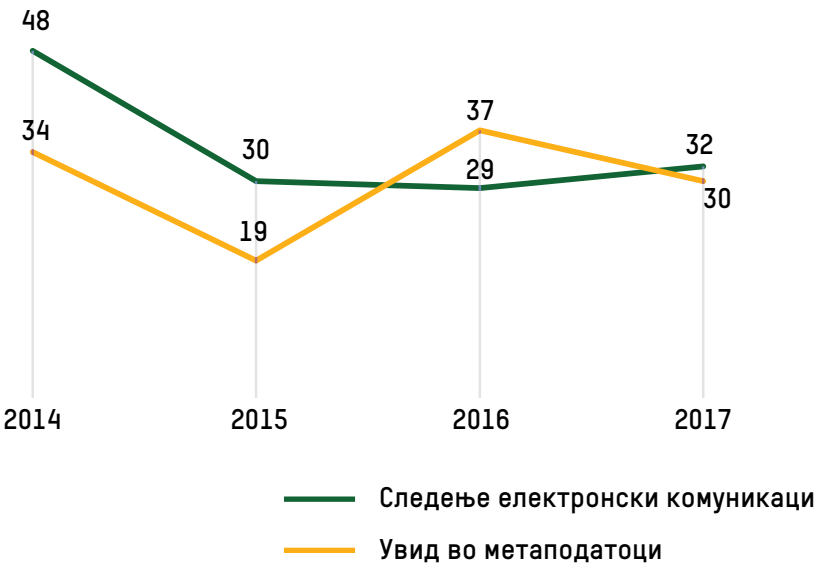
IMPLEMENTATION OF THE INTERCEPTION OF COMMUNICATIONS

IMPLEMENTATION OF THE INTERCEPTION OF COMMUNICATIONS

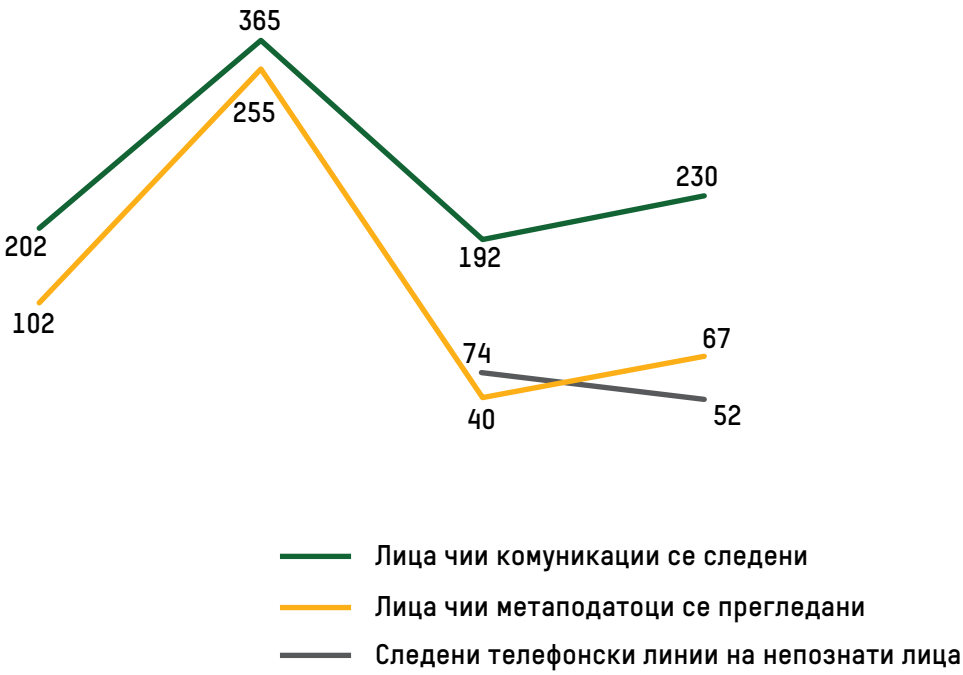
	Interception of communications due to detection and prosecution of perpetrators of crimes	Interception of communications due to security and defense
Implementation	1) With the mediation of the Operational-Technical Agency (OTA), or 2) With equipment kept in the Basic Public Prosecutor's Office for Prosecuting Organized Crime and Corruption (OTA is not the mediator in the interception of communications)	1) With the mediation of the Operational-Technical Agency (OTA), or 2) With equipment of the Administration for Security and Counterintelligence (OTA is not a mediator in the interception of communications)
Longest period of keeping the records	Until the investigation has been closed without the possibility for reopening, but if an indictment is issued - until the expiration of the statute of limitations of the criminal prosecution as regards the act for which interception of communications has been ordered or until the expiration of the statute of limitations of performing the criminal sanction.	Three years after the time determined by the order has expired, and this deadline may start running again in case of "obtaining new information".

...23

Графикон 1: Случаи на кривично гонење при кои биле следени електронски комуникации или метаподатоци



Графикон 2: Број на лица и телефонски линии кои биле следени поради кривично гонење



These graphs show the application of two special investigation measures in the period 2014-2017: monitoring and recording telephone and other electronic communications (monitoring electronic communications) and inquiry in engaged telephone and other electronic communications (inquiry in metadata).[30] Data on interception related to defense and security is unavailable. The average duration of the measure interception of electronic communications shows a negative trend, which is 4 months in 2017. As regards the measure inquiry in metadata, the 2017 average is 1.5 months.

The Law on Interception of Communications, passed in 2018, allows interception of communication without the mediation of the new Operational-Technical Agency (OTA) and the telecommunication operators, which renders the oversight easier since it creates more points for obtaining and comparing data.

However, the Law allows interception of communication without the mediation of OTA and the operators,[31] with special unspecified equipment, therefore it is unclear whether this formulation includes all hardware and software for interception of communications that the authorized bodies have on their disposal.[32] The Law on Interception of Communications does not set any conditions whatsoever that have to be met so communications can be intercepted without OTA. This Law and the Bill on National Security Service do not provide effective oversight of whose communications are intercepted without OTA's mediation since they do not envision creating invariable electronic records, such as the case when the interception is done through OTA. In such case, the two pieces of legislation envision invariable electronic records with details on the implemented activities, the persons who have implemented them, the phone number or IP address in question, the time of commencement and end of the interception. Unlike the detailed description

30 The data is obtained from the annual reports of the Public Prosecutor's Office for application of the special investigation measures.

31 Articles 17 and 34 of the Law.

32 According to media reports, it can be related to IMSI catchers i.e. equipment mounted on vehicles that imitates cell towers of mobile operators. The equipment may intercept communications of mobile telephony, but also the locations of mobile phone users. The said provision can pertain to other controversial tracking technologies, such as FinFisher, which, according to media reports, is allegedly present in the country and which allows access to data and communications from mobile phones, computers, computer networks, telecom operators' equipment etc.

of these records as regards the interception with OTA's mediation, the Law on Interception of Communications and the Bill on National Security Service prescribe only an equipment sign out sheet, in cases when the equipment is removed from the premises of the Public Prosecutor's Office or UBK's[33] premises, and the number of court order, while the Bill on National Security Service stipulates that the authorized persons must not delete any data from this equipment. Since this equipment is mounted on vehicles too[34], the possibility for effective control and oversight of its use if kept in the UBK (i.e. the future Service) and if only the UBK/Service maintains records of its use is brought into question.

It is concerning that the Law on Interception of Communications and the proposed law on National Security Service does not prescribe the series of measures for the protection of collected data as per the Directive 2016/680 on Protection of Police and Criminal Justice Data. In addition, the Directive[35] and our Law on Personal Data Protection envisage special categories of personal data[36] which must not be processed, i.e. can be processed but under special conditions. Such data is generally regulated by the Law on Criminal Procedure and does not apply to the measures for interception of electronic communication as well as the interception of communication for defense and security purposes.

The Law on Interception of Communications prescribes retaining of the collected communications until the statute of limitations of the criminal prosecution has expired, even in cases when acquittal or rejection verdict has been reached. When it comes to interception of communications for Republic's defense and security purposes, data is retained for 3 years, and this deadline may start running again in case of "obtaining new information". The formulation "this deadline may start running again in case of "'obtaining new information'" provides space for irrationally long and even unlimited

33 According to the legal regulations, the equipment for interception on the basis of security is kept in the UBK, while the one for interception on the basis of criminal prosecution is kept in the Public Prosecutor's Office.

34 According to media statements of former and incumbent officials.

35 And also the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe.

36 For instance ethnic origin, political views, data relating to the health condition of the people, data referring to sexual life.

data retention - which from the viewpoint of data protection principles is unacceptable and increases the risk of inadequate use of personal data.[37]

RECOMMENDATIONS - HOW TO IMPROVE THE OPERATIONAL IMPLEMENTATION OF THE INTERCEPTION OF COMMUNICATIONS?

- A bylaw containing specifications and technical features of the equipment for interception of communications without the mediation of OTA and operators, as well as the manner of maintaining and operating with this equipment to be determined by an approval by the Committee for Overseeing the Work of UBK/Service and the Intelligence Agency.
- To be prescribed by a law that the equipment of the soon-to-be National Security Service, that enables interception of communications without the mediation of the OTA, shall be kept in the premises of another institution, so there would be another entity that would keep track of the use of the equipment by the Agency.
- To provide training on data protection, basic rights, professional ethics and integrity for the OTA employees and authorized bodies for interception of communications, in accordance with the Urgent Reform Priorities.

- The Law on Interception of Communications and the Bill on National Security Service ought to prescribe more detailed technical and organizational security measures as regards the data processing in accordance with the Directive 2016/680 on Protection of Police and Criminal Justice Data. In addition, the data minimization principle as regards the interception of communications ought to be prescribed by law, meaning that data collection should be legally restricted to only what's directly needed and relevant to the specific purpose, and such data should be retained as long as needed for the specific purpose only.
- To prescribe precaution as per the special categories of personal data (stipulated by the Law on Personal Data Protection) i.e. statements regarding such data should be excluded or deleted during the process of interception of communications.

37 Article 29 of the Law.

- To limit the deadline for further retention of data, which has been collected by interception of communications for defense and security purposes.
- To be prescribed by law that when data collected by interception of communications is destroyed, the original records and all copies in all involved institutions and entities shall be destroyed as well. Data should be destroyed in the presence of representatives of the Directorate for Personal Data Protection and the Ombudsman.

4

OVERSIGHT AND CONTROL

OVERSIGHT AND CONTROL

The reforms in 2018 increased the number of bodies, besides the Parliament, that oversee the interception of communications.[38] See their oversight spheres in the table below.

Oversight body	Legality	Legality[39]	Efficiency
Parliament	✓	✓	
Council for Civil Oversight	✓		
Directorate for Security of Classified Information	✓		
Directorate for Personal Data Protection	✓		
Ombudsman	✓		

The Law on Interception of Communications elucidated the manner of conducting oversight of the legality and effectiveness of the interception of communication measures on the part of the competent parliamentary committee, prescribed expert support and reduced the risk for hindrances by the political parties in power. The Law's text, that was published for public consultation, enabled the Committee to summon the directors of the authorized bodies for interception of communications, OTA and the operators, with the aim to establish the legality of their activities. This

38 The oversight bodies oversee the authorized bodies, OTA and the telecommunications operators, with the exception of the Council for Civil Control, which does not conduct oversight of the operators. OTA, on the other hand, conducts expert oversight of the operators.

39 The oversight bodies oversee the authorized bodies, OTA and the telecommunications operators, with the exception of the Council for Civil Control, which does not conduct oversight of the operators. OTA, on the other hand, conducts expert oversight of the operators.

provision was supposed to prevent a repetition of previous cases when officials refused to attend a session of the Committee they had been invited to, however, the version that the Government delivered to the Parliament and enacted later on didn't contain the said provision - despite the fact that the strengthening of the Committee's ability to provide testimonies was prescribed by the Urgent Reform Priorities. In 2018, the Committee focused mainly on participation in activities for strengthening of oversight capacities and meeting with representatives of competent authorities for interception of communications.[40] Although there was an ad, the expert support for its operations wasn't provided in February 2019.[41] It's unbeknown whether the Committee has ruled on the published case of 2018 when devices for interception of communications were found in the Public Prosecutor's Office and the Basic Court Skopje 1.

Although there were plenty of candidates from the ranks of the experts and representatives of civil society organizations, the Parliament didn't appoint all members of the Council for Civil Oversight - due to the demands of some of the parties in the Parliament for republishing the ad and reaching fair representation in the Council itself. Due to these circumstances, this Council is still inoperative.

On the other hand, control authorities as regards the legality of the implementation of the special investigation measure - interception of communications - on the part of the authorized bodies, the operators and OTA, are the public prosecutor and the judge who has issued the order for interception of communications. They are entitled to an unannounced inquiry in the authorized bodies, OTA and the operators, and access to all the data, and can also hire technical experts to help them conduct the control.

The Bill on National Security Service prescribes the same oversight bodies as in the case with the interception of communications, but in this case, competent authorities are the State Audit Office and the parliamentary Committee for Supervising the Work of the Security and Counter-Intelligence

40 Annual work report of the Committee on Oversight of the Implementation of Measures for Interception of Communications for 2018.

41 https://sobranie.mk/javen-povik-za-angaziranje-na-dvajca-tehnicki-eksperti-za-postojana-poddrshka-vo-komisijata-za-nadzor-nad-sproveduvanje-na-merkite-za-sledenje-na-komunikaciite.nspx

Directorate and the Intelligence Agency. The Bill provides more details on the oversight and manner of conducting the oversight by the Parliament only, not by the other oversight authorities, while the data that the Service will have to deliver to them is insufficiently defined. It is of significant importance that the parliamentary supervising committee can summon the Service's director and that internal control of the Service is introduced. The Bill obligates the director to submit an annual report to the competent parliamentary supervising committee as well as to publish a public report on the work, but the content of these reports hasn't been specified yet.

Pursuant to the Law on Criminal Procedure,[42] the Public Prosecutor submits an annual report to the Parliament on the use of the special investigation measures, including the interception of communications. The analysis of the reports 2014-2017 has shown that the Public Prosecutor's Office submits them to the Parliament 7-9 months after the year has passed, which is a rather long period for preparing a 10-16 pages report. The reports are not uploaded to the website of the Public Prosecutor's Office. With that said, the level of transparency is concerning. In addition, the reports do not contain the following elements prescribed by the Law on Criminal Procedure, which are crucial for the Parliament in order to be able to conduct oversight of the legality, effectiveness, and efficiency:

- elaboration on the reasons why the interception of communications didn't yield results relevant to the procedure, i.e. didn't provide evidence for the procedure;
- costs arising from the use of the special investigation measure.

There are inconsistencies as regards the data in the reports. For instance, the 2017 report states that the interception of electronic communications measure has been used in 32 cases, but after the measure had terminated a review has found that it has been used in 33 cases. Such discrepancies appear in the 2016 report as well. Another inconsistency as regards the reports is that data on the outcome of the application of the measure in the reports for 2014 and 2016 is presented in the form of cases, while in the report for 2015 data is presented per person and there is no data on the outcomes

42 Article 271 of the Law.

per case. As per the report for 2017, there is a number of cases and persons that are under investigation, while the rest of the outcomes are available in per person review, not per case. Regarding the measure inquiry in metadata, there is no data on the outcome for one case this measure has been applied and on the duration of use of this measure. Such inconsistencies render the comparison of data from different years and the assessment of the effectiveness of measures for interception of communications and metadata difficult.

It is surprising that the application of one of the two analyzed measures, which has resulted in gathering evidence for 7 verdicts, is mentioned only once in the analyzed reports for the four years. However, it is not stated whether and how many of these verdicts are conviction verdicts and whether they are final and valid. It is unclear whether in other years verdicts had been reached on the basis of evidence collected with the two analyzed special investigation measures or such indicator hadn't been monitored at all. There are also no examples of serious crimes that have been detected and prevented thanks to the application of the special investigation measures and, more specifically, the interception of communications.

The reports contain no data on the number of motions for interception of communications that had been delivered to the public prosecutor, how many of them had been agreed by the prosecutor, how many own initiatives had the prosecutor had, and how many orders following motions had been issued by judges. Also, the reports do not contain statistics on whether and how many requests for providing metadata to foreign internet service providers, such as *Twitter, Facebook, Gmail* etc. there had been.

RECOMMENDATIONS – HOW TO IMPROVE THE OVERSIGHT AND CONTROL OF THE INTERCEPTION OF COMMUNICATIONS?

- To prescribe more detailed provisions on the manner of monitoring the legality, effectiveness, and efficiency of the interception of communications in all of its stages: selection of measures, collection of data, analysis thereof and ruling thereon, and financing as well.
- The data, which the soon-to-be National Security Service shall be obligated to deliver upon the request of the oversight bodies, including successfulness indicators, to be legally stipulated, while

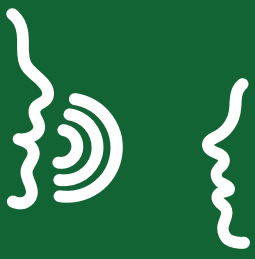
the remit and rights of the oversight bodies to be defined.

- For the purposes of building accountability, transparency, and trust in the work, all information that has to be encompassed in the annual report of the National Security Service should be stipulated by law, and that includes data on how many persons and communication devices have access, how many requests for issuing a court order have been submitted, rejected or reversed, statistics on eventual disciplinary measures against employees of the Service regarding omissions or abuse during implementation of measures for covert data collection, statistics on the amount of costs for the state and other relevant information. The annual report for the public to contain the same data, but presented in an easy to understand form. These categories of data to be encompassed in the Public Prosecutor's annual report on the application of the special investigation measures.
- Regular controls of the operators as regards the access and processing of communication traffic data and users' location data to be conducted by the competent authorities.

...35

5

NOTIFYING THE CITIZENS WHOSE COMMUNICATIONS HAVE BEEN INTERCEPTED AND LEGAL REMEDIES



NOTIFYING THE CITIZENS WHOSE COMMUNICATIONS HAVE BEEN INTERCEPTED AND LEGAL REMEDIES

If a court verdict says that the communication had been intercepted contrary to the provisions of the Law on Interception of Communications, as well as in case of publishing data collected by intercepting communications, the person is entitled to compensation from the state budget.[43] The Law gives the right to submit a request to the Council for Civil Control for checking whether their phone number is or has been illegally intercepted in the past three months. However, it's problematic that this right is limited to a phone number only, and it does not include the inquiry in metadata or internet traffic, including internet conversations and messages. There are no reasons whatsoever why this right is limited to the past three months only. Furthermore, the provision saying that following a decision on initiating an investigation the citizen is supposed to be familiarized with the report on the interception of communications does not exist in the Law on Interception of Communications. The Law on Criminal Procedure stipulates that after the termination of the special investigation measures, and if that is not harmful to the procedure, upon request by the concerned person, the public prosecutor shall deliver the written order to him or her. As in the previous case, the concerned persons should have prior knowledge that their communications had been intercepted so they could submit such request, and the law does not prescribe a clear mechanism for that to occur. The European Convention on Human Rights prescribes that the individual for whom data is being collected has the right to be informed, such as the case

43 Article 28 of the Law on Interception of Communications.

with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe. Additionally, contrary to the Directive 2016/680, our law does not prescribe the right of nonprofits to lodge complaints and represent the concerned persons[44] as well as the right of authorized bodies for interception of communications to notify the citizens in the event of a violation of their collected personal data.[45]

RECOMMENDATIONS – HOW TO IMPROVE THE NOTIFYING OF PERSONS WHOSE COMMUNICATIONS HAD BEEN INTERCEPTED AND THE LEGAL REMEDIES ON THEIR DISPOSAL?

- To introduce an obligation to notify the concerned persons about the special investigation measures after they have been terminated, except when it can be proven that it contains hindrances or prejudice relative to the criminal prosecution.
- To introduce effective *legal remedies* that can be used when a person believes that the interception of communications carried out by the competent authorities has violated their rights. Relevant nonprofits to be legally entitled to lodge objections and represent concerned persons in cases related to the interception of communications.

44 Article 55 of the Directive.
45 Article 31 of the Directive.