SLIPPERY SLOPES IN THE REFORM OF SERBIAN SECURITY SERVICES

Predrag Petrovic

Katarina Djokic
SLIPPERY SLOPES IN THE REFORM OF SERBIAN SECURITY SERVICES

Publisher
Belgrade Centre for Security Policy
Djure Jaksica 6/5, Belgrade, Serbia
Telephone: +381 11 3287 226
E-mail: office@bezbednost.org
Web: www.bezbednost.org

Authors
Predrag Petrovic
Katarina Djokic

Translation from Serbian
Vera Gojkovic

Design and layout
Marko Marinkovic

Printed by
Unagraf

Copies
100

ISBN
978-86-6237-144-7

BELGRADE, June 2017

Publication of this study was kindly supported by the Embassy of the Kingdom of the Netherlands in Belgrade, in the framework of the project "LEGASI - Towards Legislative Reform of Security Intelligence System". The opinions expressed in the publication are solely those of the authors and do not necessarily reflect the positions of the Kingdom of the Netherlands.
## Table of Contents

- **Introduction** 6
- **NATIONAL SECURITY COUNCIL – TAILOR-MADE FOR THE MOST POWERFUL PARTY LEADERS** 7
  - Incomplete composition of the Council 7
  - NSC secretary: political power has been turned into security power 8
  - Recommendations 9
- **POLICE COMPETENCES OF SECURITY SERVICES – SPECIFICITY OF THE SECRET POLICE** 9
  - Jeopardized secrecy of operation 10
  - Unnecessary duplication of activities 11
  - Towards greater intelligence and analytical competences 11
  - Recommendation 12
- **COMMUNICATIONS SURVEILLANCE MEASURES** 12
  - Rules regulating electronic surveillance: one step forward, three steps back 13
  - Regular – albeit very limited – oversight of access to retained data has been established 14
  - Security services still have the possibility of unlimited interception of communications 15
  - Monitoring center remains at Security and Information Agency premises 16
  - Access to retained data is chaotic and escapes oversight 18
  - Security services and the police are not the only ones that "lawfully" monitor communications 18
  - Number of persons whose communications are monitored remains a secret 19
  - Recommendations 20
- **INTERNAL CONTROL – INSUFFICIENT AUTONOMY OF OPERATION** 20
  - Recommendations 22
- **EXTERNAL OVERSIGHT OF SECURITY SERVICES** 22
  - Parliamentary supervision: regular, but superficial 22
  - Despite challenges, independent state authorities remain leaders in the oversight of security services 24
  - Recommendations 26
- **Legal framework** 27
Introduction

After having restored its statehood in 2006, Serbia had the opportunity to tailor the security sector to its own needs and possibilities, unburdened by complex political and other relations that are specific for a (con)federal state. However, contrary to the expectations of the professional and general public, a comprehensive reform of the security sector, including security services, has never been carried out. Similarly to what happened after the October 5, 2000 changes, a partial reform of the security services and the security-intelligence sector was guided by the desire and ambition of the most powerful political leaders to control the operation of security services, while some legal modifications had to be made as a result of Serbian Constitutional Court decisions. Consequentially, security services have still not become a part of a single security-intelligence system, the legal framework regulating their operation has not been harmonized and abounds in loopholes, it is not clear what BIA's role in criminal investigations is as opposed to the police, and the oversight and control of security services is ineffective and is not conducive to accountability for their management and the management of their operation. In other words, they are tailored to the needs of politicians, rather than the security interests and needs of the Serbian society and citizens. On the following pages, we will describe the outlined issues in greater detail and explain the negative consequences they might have in practice for the democratic order and human rights as well as for the operation of the security-intelligence sector. We will offer solutions for each of the problematic issues. In the course of 2017 and 2018, Serbia's Constitution is to be modified and one of the important steps in overcoming the issues analyzed herein is to regulate them in the Constitution.

1 Petrović, P. „Party interests are more important than national security“, 29.1.2014. Belgrade: BCBP. <https://goo.gl/KNwEKg>
A successful state response to modern-day security risks and threats, which are very complex, intertwined, and transnational by nature, calls for a coordinated and integrated response not only of security services and police, but also of other state institutions. To that end, modern states establish bodies for the coordination of activities of importance for national security, which are most frequently called national security councils (NSC). After several failed attempts, Serbia finally established its National Security Council as late as in 2007, when the Law on the Bases Regulating Security Services of Serbia was adopted. However, instead of ensuring that the main impetus for the establishment of the NSC be Serbia’s coordinated and integrated response to modern security challenges, risks and threats, the NSC was shaped to suit the needs and ambitions of political leaders who had the greatest political power at the time. Therefore, the Council has numerous shortcomings that stand in the way of the harmonious operation of the security sector.

**Incomplete composition of the Council**

One of the major shortcomings of the Council is that the minister of foreign affairs is not among its permanent members. This is opposed to the practice of most countries, since foreign policy is one of the most important elements in the realization of the national security policy, which is also stressed in Serbia’s National Security Strategy. Foreign policy has (or should have) special importance for the countries that pursue neutral (military) policies. The foreign affairs minister’s absence from the NSC membership is even more important if we take into account the fact that the intelligence component of the Security Information Agency (BIA) and the Military Security Agency (MSA) are underdeveloped and that the Serbian diplomatic capacity is insufficiently used for this purpose. This unusual solution is not supported by the comparative practices of other countries and is not a result of Serbia’s security needs; it is, rather, a consequence of personal relations which existed between two politicians while the Law on the Bases Regulating Security Services was drafted. Namely, the then Serbian president Boris Tadić did not want to have in the Council his party colleague Vuk Jeremić, whom he perceived as strong political competition.

Another major shortcoming is the absence of the Serbian National Assembly speaker from the Council membership, which means that the NSC is not required to file reports on its operation to the National Assembly and its working bodies. The principles of democratic control have

---

5 Statements of several survey participants, March 2016- May 2017. The underdevelopment of the intelligence component seems to be a common feature of security services in post-Socialist states. For example, it has been estimated that the Croatian Security and Intelligence Agency uses just 5-10% of its capacity for intelligence activities. For more, see: Tuđman, M. O iskustvima parlamentarnog nadzora i funkcionalnosti izvjestajnog sustava Republike Hrvatske, July 2013, Večernji list, 10.2.2016. https://goo.gl/mnsZIn
6 Statements of several survey participants, March-December 2016.
thus been considerably undermined. Also, if the legislator has already opted for mixed NSC membership, that is, for politicians and professionals as its members, it remains unclear why, in addition to the Serbian Army chief of General Staff and directors of security services, the NSC members do not also include the police director or the organized crime prosecutor.7 The role of the police in the prevention of modern security risks and threats, primarily (illegal) migrations, extremism and terrorism as well as organized crime, is becoming more and more important, and greater effectiveness of the police in this field is Serbia’s commitment to the path towards the EU.

**NSC secretary: political power has been turned into security power**

So far, the NSC practice has shown that the NSC secretary shows the biggest drawbacks in the coordination of security services. The secretary should ensure the implementation of NSC decisions and harmonized operation of security services; rather than that, politicians use this position to control the Serbian security services. Namely, under the 2007 Law on the Bases Regulating Security Services, the Serbian president’s chief of staff is also the secretary of the National Security Council. The NSC secretary is the *de facto* head of the Bureau for the Coordination of Security Services’ operation on the ground, although the Law never says this explicitly. This solution made it possible for the then Serbian president Boris Tadić to exert considerable security power through his chief of staff Miodrag Rakić. Some claim that Miodrag Rakić was the real director of the security services and the police.8

That politicians see this as an important position can also be seen from the following facts: after winning the 2012 elections and removing the Democratic Party from power, the Serbian Progressive Party (SNS) modified the Law on the Bases Regulating Security Services, stipulating that the Serbian president should appoint the Council secretary. However, the reasons for this were completely different from those declared in the explanation of the Bill - in order to ensure the deconcentration of power and to observe the principles of democratic control.9 The amendments to the Law removed the obstacles that had prevented SNS leader Aleksandar Vučić from assuming the office of the secretary and simultaneously being the first prime minister in charge of defense, security and fight against corruption, as well as the defense minister. He used this position for increasing his political power and popularity both in the society and within the party. He used the NSC secretary position to announce the arrests of crime and corruption suspects and held news conferences following the arrests. At one of the news conferences, he even disclosed the methods which the BIA had used for locating and arresting Darko Šarić, which is against the law, because these measures had been regulated by secondary legislation which had a classification marking.10

On the basis of media reports, we can conclude that the meetings of the Council and the Bureau were the most intensive in the first two years after the SNS had taken power (in 2012

---

7 During the survey, some interlocutors, quoting some solutions from developed democracies (e.g. Great Britain, Australia), indicated the need that only politicians or ministers be permanent NSC members. Professionals, i.e. directors of security services and police, as well as the chief of General Staff would be permanent members of the body in charge of operative coordination and realization of NSC decisions and would participate in the NSC operation as needed.


and 2013), only to become less frequent and less regular later. „Unfortunately, this body (the
Bureau, author’s comment) is not in service, operatively speaking. Its job is to ensure dai-
ly leadership and guidance in the security sector; distribution of activities and competences,
analyses, assessments, estimates and everything that belongs to security-intelligence activities.
However, the Bureau meets only occasionally.”

It appears that the NSC and the Bureau have merged lately, and thus the Bureau held a session
on the occasion of the Macedonian crisis in April 2017, attended by the prime minister, interior
minister, Minister of Defense and justice minister, chief of the General Staff and security
service directors.

These facts show how bad and dangerous it is for the democratic order and for a balanced
operation of the security sector to have politicians shape security institutions in accordance with
their ambitions and to have them personally coordinate the operative work of security services.
In order to avoid this bad practice, the Constitution will need to include the most important
provisions on the NSC, while the statutory conditions for becoming the Council secretary will
have to be several years of experience in the field of security-intelligence, and no political
party membership in the previous several years.

Recommendations

• It needs to be regulated that, in addition to the current members of the National Security
Council, permanent members should also include the National Assembly speaker, Minister
of Foreign Affairs and Police Director.
• Regulation must require from the National Security Council secretary to have nine years of
experience in the security-intelligence sector and not to have been a political party member
for the past 5 years.

POLICE COMPETENCES OF SECURITY SERVICES – SPECIFICITY OF THE SECRET POLICE

The right of security-intelligence services to collect evidence for criminal court proceedings,
and to be authorized to use weapons, apply coercion, and take in and arrest (hereinafter re-
ferred to as police competences) are not specific for security-intelligence services of the old
and new democratic regimes. This is because a merger between police and security-intelligence
activities results in a big concentration of security powers in a single organization, which
jeopardizes the division of power principle, as one of the cornerstones of modern democracies.
The concentration of counter-intelligence, security-intelligence and police activities within
one service is in the service of the authoritarian rule of a society, and such services are called
the „secret police“. This is why most developed democracies have deliberately divided the se-

11 Statement of Momir Stojanović, former head of the Security Service Control Committee and former MSA director. Glavonjić, Z.
Reforma tajnih službi: Krv, znoj, suze i politička volja, Radio slobodna Evropa, 9th December 2014. https://goo.gl/1O02ws
curity-intelligence and police activities into separate organizations while they were shaping their security sectors. Truth be told, there are some developed democracies (e.g. Denmark and Sweden) that have security-intelligence services with police competences, but they are under the diversified and effective democratic control.  

Starting from these principles, one of the main tasks of most post-socialist countries in the transformation of secret police services into security-intelligence services was to separate the security services from the interior ministry and strip them of the right to police competences. However, Serbia has not completed this process and, thus, BIA has kept all police competences, while the MSA has kept some of them. The BIA Law also makes it possible for the Agency to undertake and directly perform activities within the competence of the Ministry of Interior (MoI), where this is required by special security reasons. As a result, BIA is largely involved in different criminal investigations (of organized, financial and economic crime), as well as in combating drug trafficking, of which the Agency managers and Serbian presidents and prime ministers have boasted. One should also note that Serbian police use the technical capacities of BIA for the interception of communications and that BIA thus has an insight into police investigations.

There are several reasons for retaining police competences. First of all, in the transition societies, large cash flows, which are generated and transferred through criminal channels, enter the legal flows. Police competences of security services make it easier for politicians to affect these flows. “You see, the BIA director is a close friend of the prime minister, who is also the coordinator of all security services, while the organized crime prosecutor is a friend of the BIA director.” Furthermore, police competences “facilitate” the operative work of security services, because they can thus forcibly bring in a person from whom information is requested, and secure the cooperation of and receive information from the targets of security-intelligence operations, threatening them with criminal reports and prosecution. “You see, many pre-investigative activities under the CPC do not end up with criminal prosecution and conviction.” So, a combination of secret operations and law enforcement activities gives security services room for maneuver, but also paves the way to big risks from human rights violations and abuse.

Jeopardized secrecy of operation

The experience of developed democratic states also indicates that the security services’ participation in criminal investigations may jeopardize the secrecy of their work, which represents the inherent nature of their operation. Namely, the requirement of a fair trial, guaranteed under Article 6 of the European Convention on Human Rights and the relevant jurisprudence of the European Court of Human Rights, established on its basis, requires that all data collected during a criminal investigation be available to the defendant during the court proceedings. Although this is not an absolute right, the court is the last instance that

13 Council of Europe - European Commission for Democracy Through Law. Report on the Democratic Oversight of the Security Services, adopted by the Venice Commission at its 71st Plenary Session, Venice, 1-2 June 2007, Strasbourg, 11 June 2007. Otherwise, over the past ten years, Denmark and Sweden have made big efforts to ensure that their security services distance themselves from the police. The security services of these countries have thus been transferred from the police to the ministry of justice.


15 An interview with the interlocutor No. 3, who requested to remain anonymous, November 2016.

16 An interview with the interlocutor No. 2 who requested to remain anonymous, October 2016.
decides on the (non-)accessibility of data. Whenever the court decides that, for example, classified information is relevant for the defense, a clash most frequently occurs between security services and the prosecutor, who would sooner make sensitive information public than allow the investigation to fail.\textsuperscript{17}

Furthermore, it has turned out that, in order to determine the validity of security service data, all serious prosecutors want to be informed about the sources and method of data collection. The problem is that prosecutors, especially younger ones, sometimes change careers and go to private practice where they frequently defend organized crime suspects.\textsuperscript{18}

It is equally important that employees at security services are trained for secret operation and that they do not tend to appear at court as witnesses. „People who appear at court must be specially prepared, because this is a big shock for them in comparison with what they do.”\textsuperscript{19}

**Unnecessary duplication of activities**

In Serbia, the Service for Combatting Organized Crime and Service for Combatting Terrorism and Extremism at the Criminal Police of the MoI are nominally in charge of preventing and detecting organized crime and terrorism offenses. In the past, the police competences of security services had been justified by the fact that police were not trained and capable enough of conducting complex (organized crime) investigations. However, the situation has significantly changed over the past 10 years, and police resources have been significantly improved in that respect. Inter alia, a set of measures contained in the action plans for Chapters 23 and 24 envision additional improvement of police capacity in the fight against organized crime and terrorism. Therefore, the security services’ right to participate in criminal investigations only additionally complicates and hampers the fight against organized crime and results in a needless waste of resources, because the boundaries between the competences of security services and the police become blurred.\textsuperscript{20}

**Towards greater intelligence and analytical competences**

Not only that police competences are a challenge to democracy, but they are in contravention with the very logic of security-intelligence activities. The point of operation of security-intelligence services in modern democratic societies is to ensure accurate and timely data, information and assessmentsto the holders of state authority, in order to enable them to make the right foreign and internal policy decisions. The stress is on the observation of trends and activities of importance for the security of the state and citizens in the widest sense. In criminal investigations, however, the point is to collect data that may serve as evidence at court in the relevant case.\textsuperscript{21}

\textsuperscript{17} For more information, see: Vitkauskas D. The Role of a Security Intelligence Service in a Democracy. (Brussels: NATO, 1999): 37-41.


\textsuperscript{19} An interview with the interlocutor No. 1 who requested to remain anonymous, February 2016.

\textsuperscript{20} Petrović, P. Politizacija je velika prepreka za izgradnju integriteta u srpskim službama, an interview with Matthé van den Bersselaar. (Beograd: BCBP, 2016) https://goo.gl/mLq2xs

\textsuperscript{21} On the value of intelligence for criminal investigations, see: Lukić, T. Informacije (obaveštenja) službi bezbednosti kao dokaz u krivičnom postupku, Zbornik Radova 289, Novi Sad: Law School of the University of Novi Sad, 2011: 289-308.
The experience of security services that do not have police competences has shown that they develop knowledge and capabilities for security prevention and observation of the „big picture”, rather than for repression and investigations exhausted on a single, specific case. These security services have better human resources because they employ people of different profiles that are not usually hired by the police, such as historians, linguists, economists, psychologists, etc. This enables them to have staff that can comprehensively and creatively work on the observation, analysis and resolution of security issues. In the context of prevention of modern security threats, primarily terrorism, the Federal Bureau of Investigation has been strongly criticized for weak intelligence capacities that cannot be improved through the development (of a separate organizational entity) within the FBI, because police competences and the police culture of the FBI do not represent a stimulating environment.

**Recommendation**

- Security services should be stripped of police competences and of the right to collect evidence for criminal court proceedings.

**COMMUNICATIONS SURVEILLANCE MEASURES**

Special measures for secret data gathering (hereinafter referred to as: special measures) deserve particular attention as an unavoidable method and an especially sensitive area of operation of security service, since their implementation invades citizens’ privacy and temporarily derogates from some constitutional or legal provisions. The communications surveillance will be in the focus of this Chapter. The communications surveillance refers both to the measures for interception of communications as well as measures for the collection of data on communications without finding out their content (so-called retained data). The communications surveillance poses the greatest invasion of citizens’ privacy and its implementation limits the validity of constitutional provisions that guarantee the secrecy of letters and other means of communication and personal data protection.

---


26 Constitution of the Republic of Serbia, Article 42.
BRIEF OVERVIEW

THE COMMUNICATIONS SURVEILLANCE MEASURES IMPLEMENTED BY SECURITY SERVICES: LEGAL FRAMEWORK

The Security Information Agency and the Military Security Agency may implement communications surveillance measures:

- in order to carry out their primary competences, which are defined in the relevant laws. In that case, the implementation of the communications surveillance is regulated by the relevant laws27;
- for the purpose of collecting evidence in criminal proceedings, in accordance with the Criminal Procedure Code28.

The obligations of the operators of telecommunications services towards state authorities implementing the communications surveillance are contained in the Law on Electronic Communications (LEC).29

In continuation, we will present the steps forward achieved in the past few years in this field and main risks that remain in place despite the critique of experts, civil society organisations and the European Commission.

Rules regulating electronic surveillance: one step forward, three steps back

The secondary legislation (rulebook) that regulates in greater detail the technical conditions for the interception of electronic communications and data retention was adopted in October 2015, five years after the adoption of the Law on Electronic Communications.30 The Rulebook contains some commendable solutions that should address the shortcomings which have so far existed in practice. It requires that devices and program support for the interception of communications and data retention enable recording an indelible trace of each case of interception of communications and any access to the retained data. The fulfillment of this requirement creates technical opportunities for subsequent checks on whether the measures of interception of electronic communications and access to retained data have been implemented in accordance with the law. Also, the Rulebook requires from operators’ employees who work on the interception of communications and who access retained data to have the appropriate certificate for accessing classified data. This does not only protect the operative work of security services and the police, but also partly reduces the risk from the abuse of citizens’ personal data (e.g. through data „leakage”), because one has to be subjected to a security check in order to get the certificate.

28 Criminal Procedure Code, Articles 166-170 and 161-165.
29 Law on Electronic Communications, Articles 126-130a.
Nevertheless, the fact that personal data protection is regulated by a piece of secondary legislation is problematic.\(^3\) What was especially criticized was that the Rulebook, as a piece of secondary legislation which should specify the provisions of the existing law (LEC), “establishes” a new body, the monitoring center for the interception of communications.\(^3\) Although the Rulebook never says explicitly that this is an independent body, this is suggested by saying that the monitoring center will be located at the BIA premises until the fulfillment of conditions for the implementation of the provision on the monitoring center.\(^3\) This represents a separate issue that will be discussed later.

The Monitoring Center has been defined as a location housing devices and program support for the interception of communications.

Regular – albeit very limited – oversight of access to retained data has been established

The Commissioner has established the regular oversight of the access to retained data, in accordance with amendments to the Law on Electronic Communications of 2014.\(^3\) Operators and “competent authorities” who access data are required to keep records on the requests for access to retained data they (operators) have received or (state authorities) issued and to present the records to the Commissioner at the annual level. The BIA, MSA and MoI have regularly presented the records within the time frame provided for in the Law.\(^3\)

It is positive that the number of operators who send records to the Commissioner has increased significantly until 2017. Only two operators presented the 2014 records within the statutory time frame, the 2015 records were presented by 34 operators, while the 2016 records by 178 operators.\(^3\)

If we look at the presented records, we can observe that the quality of data has been improving from one year to another, which indicates that operators understand the LEC better and better.\(^3\)

However, under the LEC, the Commissioner is authorized to receive very limited data, on the basis of which the legality of operation of state authorities cannot be determined. The only thing he can check is whether the time elapsed between the date of data retention and the date when the access thereto has been requested observes the statutory time frame of 12 months.

Records received by the Commissioner contains data on the: 1) number of requests for accessing retained data; 2) number of granted requests for accessing retained data; 3) time elapsed from the date of data retention to the date when the access thereto was requested (LEC: Article 130a).

\(^3\) Commissioner for information of public importance and personal data protection. Opinion on the proposed rulebook on requirements for devices and program support for the lawful interception of electronic communications and technical requirements for fulfilling the obligation of retaining data on electronic communications. Belgrade, 4.05.2015. http://www.poverenik.rs/images/stories/dokumentacija-nova/razno/011304pravilnikel.komunik.doc

\(^3\) SHARE Foundation. Comments to the proposed rulebook on requirements for devices and program support for the lawful interception of electronic communications and retention of data on electronic communications. Novi Sad, 4.03.2015. Taken from: http://mtt.gov.rs/vesti/javne-konsultacije-o-predlogu-pravilnika/

\(^3\) Rulebook: Article 26.

\(^3\) This refers to Article 130a of the LEC.

\(^3\) Interview with Zlatko Petrović, Assistant Secretary-General of the Commissioner Service, Oversight Sector. Belgrade, 25.04.2017.

\(^3\) Ibid.

\(^3\) Copies of annual records presented by operators who had received requests for access to retained data, for the period between 2014 and 2016, presented to the Belgrade Center for Security Policy by the Commissioner Service upon our request for access to information of public importance. No. 072-09-1643, May 2017.
It is also important to stress that the operators’ records contain only data on the access made by state authorities following requests to the operator. The BIA, MSA and MoI, however, can access the retained data independently, without making any requests to the operators, and this is much more frequently the case in practice. Going through the reports which some operators have presented to the Commissioner and which are more detailed than the LEC requires, we can observe that no requests for accessing retained data have been sent by security services. Since the BIA and MSA attach classification markings to the reports they present to the Commissioner, the public cannot find out how often they access retained data at the annual level. On the other hand, MoI reports do not have classification markings, so it is possible to compare the records presented to the Commissioner directly by the MoI and some operators’ records on the MoI requests for accessing retained data. Comparing the records for 2016, we could see that in this year, the MoI accessed retained data 97,040 times, but that police units sent just 1,124 requests to the operators. So, the MoI independently accessed retained data in 95,916 (99%) cases. However, only one operator currently has the necessary technology and enough staff to keep track of the number of independent accesses. This practically means that one cannot check whether the data on the number of accesses which are sent to the Commissioner by the security services and MoI are correct.

Security services still have the possibility of unlimited interception of communications

Under the Constitution, the derogation from the provisions guaranteeing the confidentiality of communications and personal data protection is possible only for a limited amount of time, only on the basis of a court decision, only for the purpose of criminal proceedings or for protecting the security of the Republic of Serbia, and only in the way provided for by law. The legal framework that regulates the operation of security services further elaborates these limitations. Thus, except in one case, the communications surveillance, from the legal point of view, is not possible without a court order, issued at the explained motion of the service director or prosecutor. Also, the communications surveillance cannot last for more than a year.

At the same time, the LEC provisions which require from the operators to enable the lawful interception of communications have been interpreted in practice in such a way that the operators are required to obtain the equipment necessary for the activation of interception and access to retained data, and to unconditionally place it at the disposal of security authorities. The equipment is currently situated at the BIA premises. Such unlimited disposal of equipment and program support for interception is problematic for two reasons.

Firstly, there are no additional instances that can check before the beginning of interception whether a court order in the relevant case really exists. Acting under the recommendations of the Ombudsman and the Commissioner, the Security and Information Agency in 2012 announced that it was introducing a “dual key” system, which would prevent some BIA mem-

---

38 See the Constitution of the Republic of Serbia: Articles 41 and 42.
39 BIA director may first order the expansion of the special measure and only then, within 48 hours, to request the court approval. (Law on Security Information Agency: Article 15b).
40 As confirmed in the Rulebook: Article 26.
bers from initiating wiretapping on their own. Nevertheless, it seems that both keys have remained at the same Agency, which means that additional, independent control is lacking.

Secondly, since the operators themselves do not have the opportunity to keep records on when and how their equipment is used, there are no alternative sources on the basis of which external oversight bodies (competent committee of the National Assembly, the Commissioner, the Ombudsman, inspectors of the ministry in charge of telecommunications) could find out whether the data received from security services are correct. A step forward to this end was made in the Rulebook, which requires that the devices and program support which operators provide must leave an indelible trace of each lawful interception of electronic communications. Still, it is questionable whether this requirement can really be implemented in practice, since according to insiders’ claims „any trace can be deleted.” Having the technical infrastructure for the interception of communications at the premises of a single security service represents an even greater risk.

Monitoring center remains at Security and Information Agency premises

The Rulebook has officially confirmed that the monitoring center for the communications surveillance is at the BIA premises and even added that it will remain at the BIA premises until the conditions for the establishment of a separate monitoring center have been met, i.e.– until further notice. In practice, this means that the BIA physically controls the equipment for the activation of interception, and that police and the MSA have to address the BIA to activate interception for them. This is problematic even at the general level, because it blurs the boundaries between the activities of the police and security services and increases the risk from abuse.

The European Commission (EC) regularly voices concern over the fact that the Police depends on security services for the implementation of certain special investigative measures. At the EC recommendation, Serbia has included in the Action Plan for Chapter 24 a provision saying that it will revise the role and practice of security services in the criminal investigation phase in order to ensure police independence in the implementation of special investigative measures. The measures contained in the Action Plan, however, are quite superficial and vague, and the contradictory information from the report on the implementation of Action Plan is additionally confusing. According to this information, one measure has been realized, although the other, which is a prerequisite for the realization of the first, has not. Therefore, one gains
the impression that the Serbian Government has responded to the EC recommendation just for the sake of responding, without any real ambition to undertake reforms in this area.

If the Government decided to initiate reforms, it is certain that there would be three possible solutions for the interception of communications. Firstly, each state authority implementing these measures (BIA, MSA, police) could develop its own monitoring center. Thus, the police and the MSA would not depend from the BIA in the implementation of special investigative measures, although this would not necessarily solve the issue of lack of control and oversight of the implementation of the measures. Moreover, the current legislation requires from the operators to cover the costs of purchase and delivery of equipment and devices for program support on their own. If the number of monitoring centers increased, an additional – not negligible – financial burden would be imposed on the operators.

The other solution would be for the monitoring center to remain at the BIA premises, despite critiques. The arguments in favor of this solution, which have been presented in the expert discussions so far, are that the transfer of the monitoring center to another, separate location would incur considerable costs, both for the operators and for the state. In addition to this, additional efforts would have to be made to choose the appropriate building, to secure the new space and to implement security checks for new employees at the monitoring center (who would not be BIA members).

The third solution would be the establishment of a separate monitoring center for the communications surveillance, which would be independent from the MoI or any security service. This solution has been urged for years by the Commissioner and the Ombudsman, as well as by the civil society. An independent monitoring center would represent a technical body that would provide the interception of communications services to other state authorities, but would not itself conduct investigations, and its employees would not be able to inspect the content of communications. It would also ensure an additional control instance, if each state authority requesting the activation of interception were required to present a relevant court order to the monitoring center.

In addition to the three above-mentioned solutions, there is a possibility which has neither been reviewed in the public nor in the expert circles so far. The monitoring center might be established within the Regulatory Agency for Electronic Communications and Postal Services (RATEL). The argument in favor of this solution would be that RATEL already has within its competence the National Centre for the Prevention of Security Risks in ICT Systems. In addition to this, the selection procedure for the election of RATEL Managing Board members and the director is regulated in a way that should ensure the professionalism and independence of this body in vis-à-vis security services.

An opportunity to reform the measure of interception of communications should be provided through the preparation of a separate law on the interception of communications and access to retained data, which has been announced in the draft new law on electronic communications.

47 Law on Electronic Communications: Article 127 paragraph 4 and Article 130 paragraph 2.
48 Minutes from the expert consultations on the legislative reform of security services with security sector representatives, held in the organization of the BCBP, Belgrade, 30.03.2017.
50 Acronym, stands for information and communication technologies.
51 Ideas of BCBP researcher V. Erceg, presented in a discussion on 8.06.2017.
Access to retained data is chaotic and escapes oversight

After the Commissioner’s oversight of telephone service providers conducted in 2012\textsuperscript{52} and, particularly that of internet service providers conducted in 2014\textsuperscript{53}, the public received a grim picture of the lawfulness and regularity of access to retained data. Thus, the oversight of internet service providers showed that nearly one half of them did not have procedures in place for granting access to retained data, while a vast majority did not know or did not observe the statutory time limit of 12 months for retaining data.\textsuperscript{54} This finding has been additionally supported by data provided by some operators to the Commissioner within the annual reports on requests for access to retained data.\textsuperscript{55} They show that state authorities can sometimes get retained data from the operators even when they do not state the legal basis for accessing the data in the request. Internet service providers frequently neither know how to interpret the law, nor have the relevant support of the Ministry of Trade, Tourism and Telecommunications (MTTT), which is in charge of the implementation of LEC.\textsuperscript{56} If we add to this the above-mentioned fact that the BIA, MSA and MoI have and use the opportunity of independent access to retained data, on which nearly none of the operators have records, this situation creates a high risk from the arbitrary and unlawful implementation of the measure of access to retained data.

SERBIA DOES NOT FOLLOW EUROPEAN TRENDS?

The European Court of Justice in Luxemburg in 2014 issued a decision declaring the Directive 2006/24/EC on Data Retention invalid, because, in its opinion, indiscriminate data retention is not in accordance with the principle of proportionality. In this context, one needs to take into account the fact that in the EU integration process, Serbia will certainly have to amend its legislation and harmonize it with the relevant decision of the European Court of Justice.

Security services and the police are not the only ones that “lawfully” monitor communications

Neither the LEC nor any other Serbian law makes it completely clear which “competent state authorities” are authorized to implement the measure of communications surveillance and, primarily, to access retained data. An especially problematic issue is that the Criminal Procedure Code (CPC) has failed to recognize the access to retained data as a special investigative measure, that is, a communications surveillance measure. The CPC clearly says that the special investigative measure of communications surveillance may be implemented by the police,


\textsuperscript{53} Commissioner for information of public importance and personal data protection. Report on the oversight over the implementation and enforcement of the Law on Personal Data Protection by the operators of electronic communications who provide internet access services and internet services. Belgrade, 30.06.2015.http://www.poverenik.rs/images/stories/dokumentacija-nova/razno/izvestajisp.doc

\textsuperscript{54} Ibid: 2.

\textsuperscript{55} Copies of the presented annual records of operators who had requests for the access to retained data, for the period between 2014 and 2016, sent to the Belgrade Center for Security Policy from the Commissioner Service, at the request for access to information of public importance. No. 072-09-1643, May 2017.

\textsuperscript{56} Interview with Zlatko Petrović, Assistant Secretary-General of the Commissioner Service, Oversight Sector. Belgrade, 25.04.2017.
BIA or the MSA, but its definition indicates that the measure refers only to the monitoring of the content of communications. Under a 2012 Serbian Constitutional Court decision, the term “means of communication” - whose secrecy is guaranteed by the Constitution - encompasses not only the direct content of communications, but also the data on who communicated with whom, etc., that is, retained data. Since the CPC has remained incomplete in this respect, in practice, operators grant requests for access to retained data to higher and basic courts, higher and basic public prosecutors’ offices and even court experts (natural persons) and law offices.

Another big cause for concern is that some parties that successfully access retained data because of their competence are not involved in criminal proceedings (e.g. commercial courts, departments of the Market Inspectorate Sector at the MTTT). This is directly opposed to the Constitution, which generally allows for the derogation from the inviolability of letters and other means of communication only in the case of criminal proceedings or protection of security of the Republic of Serbia.

Number of persons whose communications are monitored remains a secret

The practice of security services and, to an extent, also of higher courts, of refusing to disclose to the civil society collective statistics on the applied measure of communications surveillance or the number of wiretapped natural persons and legal entities continued in 2017, despite the Commissioner’s decisions and the 2013 decision of the European Court of Human Rights, which indicated that the collective data on the implementation of special investigative measures should be publicly available.

A previous BCBP research has shown that state authorities have not reached a consensus on the interpretation of the law concerning the secrecy of collective data on the implementation of the measures. For example, out of 25 higher courts to which the BCBP had sent a request for collective statistics on the approved special investigative measures in late 2014 (the total number of requested measures and approved requests), 13 courts presented the requested data, while 12 others refused to do this, providing different explanations. On the other hand, the publicly presented position of BIA is that, until further notice, it will not immediately (i.e. without the Commissioner’s decision) approve requests for collective statistics on the implementation of the measures, as long as the law does not explicitly state that the security services are required to disclose this type of data.

---

57 CPC: Articles 166 and 168.
59 Copies of annual records presented by operators who had requests for access to retained data for the period between 2014 and 2016, sent to the Belgrade Center for Security Policy from the Commissioner Service, at the request for accessing information of public importance. No. 072-09-1643, May 2017.
62 In the territory of Serbia, excluding Kosovo and Metohija.
64 Jeremić, V. BIA: Prisluškivali smo 168 fizičkih i dva pravna lica. Danas, 14.maj 2015 goo.gl/INAvT
**Recommendations**

- **A new law should be adopted, one that would comprehensively regulate the area of communications surveillance.**
  - A monitoring center for the communications surveillance, which would be structurally and functionally independent from some security services and ministries, should be established.
  - It should be defined clearly and in accordance with the Constitution which state authorities and under which conditions have the right to implement the measure of communications surveillance, including access to retained data.
  - Regulations on data retention and access to data on communications without finding out the content of the communications should be harmonized in accordance with the best European human rights protection standards.
  - State authorities which apply the measures of communications surveillance should be explicitly required to publish at the annual level data on the number of proposed and implemented measures and the number of persons placed under covert interception.
- **The Criminal Procedure Code should be amended.**
  - The access to retained data should be defined as a special investigative measure in the Criminal Procedure Code.
- **Operators should be provided with support in the implementation of the law.**
  - The ministry responsible for telecommunications should send a letter to operators, informing them about all important aspects of the lawful interception of communications and data retention. The ministry should also appoint a contact point who would respond to the operators' inquiries on the issue.

**INTERNAL CONTROL – INSUFFICIENT AUTONOMY OF OPERATION**

The internal control represents a system of regulations, rules, procedures and bodies that exist within an institution. Its main goal is to protect and improve the institution's integrity by preventing and removing unlawful behavior and irregularities that may occur therein. Internal control bodies should represent the first line of defense from unlawful behavior and irregularities. An effective internal control makes it possible to address the observed irregularities within the institution without disclosing confidential and sensitive data to the public. To make this possible, the internal control should primarily have the right to access all data, information and documents, even when they bear a classification marking. It should also have access to all premises, and the right to conduct interviews with all persons they regard as important for an investigation. An important internal control feature is that it has the operative and financial independence and autonomy in operation, as well as mechanisms through which it can force security services to remove irregularities in their work. Finally, it is also important to ensure that internal control bodies are made up of people who have knowledge in the fields of importance for the implementation of control – lawyers, former security service members, IT experts, political scientists, etc.
Internal control has been regulated and developed differently at Serbian security services. Thus, under the Law on the MSA and Military Information Agency (MIA), there are dual control mechanisms – the inspector-general for the MSA and MIA and the internal control unit in each of the military agencies. They have been granted good competences for controlling the lawfulness of the agencies’ operation. However, the issue here is that these mechanisms have insufficient resources, independence and integrity for the successful realization of tasks. Consequently, MSA and MIA members are forced to refer to the external mechanisms of oversight and control, primarily the Ombudsman. In the procedure of the MSA and MIA control, the Ombudsman found numerous shortcomings in the operation of the internal control. They indicate that the leadership is using internal control as a mechanism of pressure on agency employees who are pointing to or would like to point to unlawful behavior or irregularities in the operation of the MSA, rather than as a mechanism for their timely detection and removal. Some MSA members complained to the Ombudsman that they had found themselves “in the line of fire” of the internal control and were subjected to polygraph testing which was to determine if they had already contacted the Ombudsman.

Unlike the military agencies’ internal control, which is directly subordinated to the agency directors, the MSA and MIA inspector-general is accountable to the defense minister. However, this functional distance from the agency directors is insufficient to ensure the efficiency of operation of the inspector-general. Thus, for example, in one of the procedures, the inspector-general established that the rights of a MIA member had been violated, but the MIA never complied with the recommendations and conclusions from the inspector-general’s report.

The inspector-general’s actions in the procedure of control initiated by the Ombudsman on the occasion of an incident that occurred at the 2014 Gay Pride were also highly disputable. In this procedure, the inspector-general, acting at the order of the Minister of Defense, requested from the Ombudsman to send to the inspector-general data in his possession to enable the inspector-general to control the operation of security services. The information presented by the inspector-general was opposed to the information collected by the Ombudsman in the control procedure, which gave rise to suspicion that this was an attempt to conceal the unlawful operation of the MSA leadership.

The Internal and Budgetary Control of the BIA is not regulated by law, but by secondary legislation, which is issued by the Agency director and which bears a classification marking. This is why the legal uncertainty of the Agency’s internal control is extremely high. The head of the Agency’s organizational unit in charge of internal control is directly accountable only to the director, to whom he files regular and periodical reports on the unit’s operation. Although the public does not know how efficient the internal and budgetary control of the BIA has been, some publicly known cases involving potentially unlawful actions give rise to suspicion regarding its efficiency.

So, the internal control in the Serbian security services has good oversight and control competences, but its resources are insufficient. More importantly, it has insufficient independence and autonomy in relation to security service directors, and, in the case of military agencies, also of the Minister of Defense.
INTERNAL CONTROL – INSUFFICIENT AUTONOMY OF OPERATION

International practice

Internal control practice in other countries has indicated that internal control mechanisms do not attain good results if they are established as “self-control” mechanisms, i.e. if they are subordinated to directors of security services and do not have own budgets. Therefore consolidated democratic states have set up inspectorates and expert oversight bodies, which are primarily accountable to the executive 65, but also report to parliaments. In addition, parliaments are involved in selection of heads of inspectorates. These bodies have relatively few members, but they are also supported by secretariats. This is a mixture of internal and external oversight of security services. Serbia should consider such experiences and solutions in the course of reforming security-intelligence system, especially in view of the announced reforms to the Constitution.66

Recommendations

- The security service inspectorate-general should be established as a government service. It would be accountable to the government and the National Assembly of the Republic of Serbia.
- It needs to be regulated that the inspector-general should be appointed by the government to a term of five years, with the approval of the National Assembly.
- The inspector-general should be required to have nine years of professional experience, and not to have been a political party member in the past 5 years.

EXTERNAL OVERSIGHT OF SECURITY SERVICES

Parliamentary supervision: regular, but superficial

Between its establishment on July 9, 2016 and late May 2017, the National Assembly Security Services Control Committee held 8 sessions. The Committee reviewed regular reports of security services, reports of the inspector-general of military security services and citizens’ complaints. Furthermore, the Committee paid oversight visits to the directorates and centers of the BIA, MSA and MIA in Belgrade and Novi Sad. In connection with legislative reforms, the Committee stressed the need for the adoption of a normative framework for BIA in accordance with European standards, but did not undertake further steps to encourage its drafting.67

65 For example, since 1989 Inspector General of the CIA has not been appointed by the Agency’s Director, but by the President, with the Senate’s approval.
66 For example, a whole heading of the South African constitution is dedicated to the security sector and includes basic provisions on the inspector monitoring activities of the intelligence services. Constitution of the Republic of South Africa, No. 108 of 1996, Constitutional Assembly, https://goo.gl/  
67 Information on the Committee activities collected from reports available on the National Assembly webpage: http://www.parliament.gov.rs/aktivnosti/narodna-sкупства/радна-тела/одбори,-пододбори,-радне-групе.2385.html
The Committee has missed the opportunity of overseeing security services outside its „regular activities” and of being more active in discussing what types of reforms of the security-intelligence system need to be undertaken in order to improve efficiency, integrity and democratic accountability of the Serbian security-intelligence system. The Committee did not organize thematic sessions or public hearings (e.g. in its 2014 convocation, the Committee planned a public hearing on the possibility for setting up a monitoring centre for communications surveillance68, but this never happened). In addition to this, the Committee has so far not organized meetings with independent state authorities, although it has included this in its 2016 activity plan.69 Relations with the Ombudsman, which deteriorated during the 2014 convocation after the Ombudsman’s control and recommendations on the MSA, have not been improved.

In its current convocation, the Committee has worked in a slightly more transparent manner than in the previous, which frequently issued no information about its sessions, except merely stating that they had been held. Nevertheless, the information which the Committee publishes about its work and results of its oversight is still scant. It is therefore impossible to assess how the MPs did their job, all the more so because only the first session of the Committee in this convocation was open to public.

On the basis of available reports on the work of the Committee, one can observe that the members’ attendance at sessions has decreased. This represents a big contrast to the practice of the 2012 convocation of the Security Services Control Committee, which was viewed as a good example of engagement of MPs in the oversight of the security sector.70 For example, the last time when the Committee reviewed MSA and MIA reports, both sessions were attended by (the same) five MPs, four of whom belonged to the ruling Serbian Progressive Party.71 One reason that may explain absence of some MPs from the sessions where the reports of security services were reviewed is that only seven out of 18 Committee members and deputy members had obtained security certificates for access to classified data by June 1st, 2017. The practice that Committee members undergo security vetting process and obtain security certificates has been established even though the Law on Data Secrecy guarantees to the Security Services Control members the right to access and insight to secret data pertaining to the oversight and control without any additional requirements.72 Under the 2016 Committee decision, sessions where secret data are reviewed may be attended only by the members and deputy members of the Committee „who have the appropriate certificate for access to secret data or have initiated the procedure for getting the certificate.”73

---

73 Law on Data Secrecy: Article 39.
74 National Assembly – Security Services Control Committee. Decision on the way in which Security Services Control Committee sessions where secret data will be reviewed will be held. No. 02-2263/16. Belgrade, 30.09.2016.goo.gl/EIDYP6.
Despite challenges, independent state authorities remain leaders in the oversight of security services

The Ombudsman continues to play an important role in the oversight of security services, despite serious challenges. In 2016, the Ombudsman issued seven recommendations to security services and all seven were complied with. Acting in accordance with the Ombudsman’s recommendations in this period, the Military Security Agency improved the integrity of the internal control procedure by starting to request from its members who implement the internal control procedure, statements on the non-existence of obstacles to their participation in the relevant control procedure. An important achievement of this institution in the past years was clarifying implementation of the measure of secret search of premises in the operation of the Security Information Agency. This is a measure which seriously derogates from constitutional provisions and invades citizens’ privacy, and its implementation is regulated only by an internal, classified BIA document. It needs to be stressed that BIA cooperated with the Ombudsman in the control process and sent him the response on actions undertaken in connection with his recommendations within the time frame provided for by law.

On the other hand, the Ombudsman’s oversight of security services was brought into question in 2014-2015, when the MSA and the Ministry of Defense prevented the control procedure and refused to comply with the recommendations of the Ombudsman in a politically sensitive high-profile case. What is especially worrying is that, during the attempted control of the MSA, the Ombudsman became the ‘target’ of the Security Services Control Committee, whose session where irregularities in the operation of the MSA were to be reviewed had turned into a session where the Committee appeared to control the Ombudsman, rather than the security services. Since the Ombudsman is an individual authority, his operations were strongly impeded after some Serbian Progressive Party politicians, including members of the Security Services Control Committee, started attacking the then Ombudsman Saša Janković, whom they perceived as a political opponent.

The Commissioner’s oversight in the field of personal data protection enabled the Serbian public to get an important insight in the problems pertaining to data processing and exchange and implementation of special measures in the operation of security services and the police. The oversight of the internet service providers’ compliance with the Law on Personal Data Protection in 2014 and the collection of regular reports on requests for access to retained data starting from 2015 uncovered considerable risks from abuse and anti-Constitutional practices in the field of communications surveillance (this topic is explained in more detail in the relevant chapter).

75 Ibid.
In addition to this, the Commissioner implemented the procedure of MoI oversight, after a photograph from the biometric database of the Ministry of a deputy special prosecutor had leaked into the public. It turned out that, right before the publication, the photograph had been accessed from “another security structure”. The Commissioner’s oversight pointed to serious issues in regard to the exchange of data between the MoI and security services.

In addition to the oversight in the field of personal data protection, the Commissioner regularly reacted in connection with complaints of the associations of citizens which could not get information on the operation of security services which should not bear a classification marking. This primarily refers to the statistics on the requests and implementation of the special measure of the secret collection of data.

Nevertheless, the Commissioner’s oversight is limited by his competences, and „the Commissioner cannot represent the consciousness of the entire public administration.” As for the oversight of telecommunications, the Ministry of Trade, Tourism and Telecommunications should play a big role in the process, because it is in charge of overseeing the implementation of the Law on Electronic Communications. And yet, it is unknown whether this Ministry has engaged in the oversight of the provisions of the law regulating the interception of communications and access to retained data. The Commissioner’s big limitation is the lack of oversight capacity, since most employees at the Commissioner Service are lawyers by profession and there are no IT and telecommunications experts. In view of the salaries of IT experts in the private sector, it is difficult to keep IT experts in the state administration, which, in turn, reduces the opportunity of external oversight bodies to determine whether security services and the police have lawfully and appropriately implemented special measures.

The State Audit Institution (SAI) has so far carried out one audit of the annual financial report and regularity of operation of the BIA (2013). The MSA and MIA were audited by the SAI as the organizational units of the Ministry of Defense in 2011 and 2013. Authorized state auditors have security certificates for the access to secret data. Nevertheless, a large number of entities that should be audited (beneficiaries of the budget and funds, local governance units, public enterprises, etc.) and the currently limited capacities of the SAI prevent it from carrying out regular external audits of the security services.
**Recommendations**

- The Security Services Control Committee should organize a public hearing on further reforms that are necessary for the Serbian security services.
- The Security Services Control Committee should organize, in cooperation with the Committee on Spatial Planning, Transport, Infrastructure and Telecommunications, a special public hearing on the best way to resolve the issue of status and location of the monitoring center for communications surveillance.
- The Security Services Control Committee should initiate the clarification of Article 39 of the Law on Data Secrecy and determine whether Committee members have the right to access secret data without a security certificate. If a security certificate is required, the issuance procedure should be sped up, in order to ensure the participation of all Committee members in the oversight.
- The Security Services Control Committee should restore cooperation with independent state authorities, primarily the Ombudsman and Commissioner for information of public importance and personal data protection, which had been established during the 2012 convocation.
- Following closed sessions and oversight visits, the Security Services Control Committee should publish reports on the oversight, which would contain the Committee’s findings and recommendations for the improvement of operation and management of security services. The Committee could rely on the existing experience of independent state authorities in the reporting on the findings of the control procedures in order to find a way for informing the public about its findings and recommendations without disclosing secret data.
- The new Ombudsman should maintain the best practices, high standards and independence in the control of security services.
- The National Assembly should react to the Ombudsman’s recommendation that the obstruction of independent state authorities’ control procedures needs to be criminalized and included in the Criminal Code.
- The professional capacities of the Ministry of Trade, Tourism and Telecommunications and the Commissioner for overseeing implementation of communications surveillance measures need to be strengthened.
Legal framework


2. Pravilnik o zahtevima za uređaje i programsku podršku za zakonito presretanje elektronskih komunikacija i tehničkim zahtevima za ispunjavanje obaveza zadržavanja podataka o elektronskim komunikacijama. [Rulebook on requirements for devices and software support for lawful interception of electronic communications and technical requirements for fulfilling the obligation to retain data on electronic communications] "Sl. glasnik RS", br. 88/2015.


