CENTER FOR EURO-ATLANTIC STUDIES - CEAS

*progress, determination, influence*

# TOTAL MAKEOVER

***

## CEAS PLAN FOR THE IMPROVEMENT OF THE SECURITY SYSTEM IN SERBIA WITH A SPECIAL FOCUS ON PROTECTION OF CONSTITUTIONALLY GUARANTEED HUMAN RIGHTS, SUCH AS THE RIGHT TO PRIVACY AND PERSONAL DATA PROTECTION

**AN ANALYSIS BY THE CENTER FOR EURO-ATLANTIC STUDIES**

**MARCH 2014**

*This analysis is part of the project "Promotion of Comprehensive Security Sector Reform," which is supported by the National Endowment for Democracy from Washington*

National Endowment for Democracy

*Supporting freedom around the world*

*„**T**here is no need to wait for the (enactment of the) law and do nothing. One should not forget that apart from law adoption there are other things which are equally important and perhaps even more important. Even the most perfectly written law is not good enough if its consistent implementation has not been ensured. And probably the most important prerequisite of consistent, quality implementation of a law is full awareness about the importance of the subject matter regulated by the given law.“*

***Rodoljub Šabić***

*The Commissioner for Information of Public Importance and Personal Data Protection*

## INTRODUCTION

The issues of basic human rights, the right to privacy, the protection of data in electronic and other communications, and the transmission of messages through wired and/or wireless networks (landline and cell phones, satellite tele-links) and their surveillance were among the most current political topics of 2013. The information disclosed by Edward Snowden in the spring of 2013 regarding the surveillance of electronic communications conducted by the NSA (National Security Agency of the USA) throughout the world has raised the issue of personal data protection and the right to privacy among the international community. The NSA has allegedly spied on the leaders of Germany, Brazil, Mexico and at least 35 other nations, as well as the headquarters of the World Bank, the International Monetary Fund, the United Nations, the European Union, the European Parliament etc.

In a response to this scandal, US President Barack Obama appointed a five-person panel, i.e. a five-member Review Group on Intelligence and Communication Technologies, tasked with reexamining the US practice of surveilling electronic communication and collecting mass data on billions of telephone calls to and from the USA.

In a report published by the White House in late December 2013, the five-member panel proposed new measures of protection as well as possible limitations for various intelligence programs, including the recommendation that the storing of call data should be ceded to the private sector or to a completely new entity that would collect information from telephone companies or from operators themselves. The recommendations given in this report will be discussed during the course of the forthcoming year.

In the meantime in Serbia, in July 2012, almost a year before the Snowden affair, Ombudsman Saša Janković and the Commissioner for Information of Public Importance and Personal Data Protection Rodoljub Šabić pointed at an alarming discrepancy between constitutional rights regarding surveillance of electronic communication and data protection and actual practice, as well as to the problems such a situation may cause and is causing. They presented their 14 points, i.e. recommendations, to help address this situation.

Already in October 2012, the Commissioner for Information of Public Importance and Personal Data Protection filed an Initiative for the adoption of a Law on Security Vetting within the Government, highlighting the fact that although the matter of security vetting is regulated through several laws and other regulations, it is done in an inadequate manner. The reason for this is that security vetting is regulated only within the context of the matter directly governed by case law and other regulations. These are typically those laws, or other regulations, regulating matters of employment in state bodies, especially in the Police, the Armed Forces and the security services, as well as the matter of education in schools viable for future employment in these public bodies.

CEAS repeatedly and publicly pointed out the absence of a special Law on Security Vetting, and has previously advocated for the adoption of a special Law to regulate this field.

CEAS believes that it is in the interest of all citizens of Serbia, the country itself, and the private security sector industry to have such assessments and conclusions that would from the security vetting of individuals; such processes should be placed under democratic control in order to reliably prevent possible abuses. It is necessary to urgently define the procedure of lawful security vetting, as the Constitution of Serbia requires. Bearing in mind the uncertainty regarding who can and should carry out the aforementioned vetting procedures, we believe that it is best to have this issue resolved with a specific Law on Security Vetting.

However, a year and a half after the official presentation of the 14 points, there is not any sufficiently strong political will in Serbia to regulate this area. Despite numerous still unaccounted for scandals involving surveillance of electronic communication and eavesdropping, which affect even the very top state leadership, i.e. a year after the scandalous revelation that Serbian President Tomislav Nikolić as well as Vice Prime Minister Aleksandar Vučić had been eavesdropped on, and even though Nikolić claims that his eavesdropping has continued despite regular public appeals issued by the Ombudsman and the Commissioner, no political consensus or political will has emerged that would enable Serbia to handle this problem by legally regulating the area of tracking and accessing electronic communications.

## AIM AND METHODOLOGY OF THE ACTION PLAN

Within the project *„The Promotion of the Comprehensive Security Sector Reform"* supported by the National Endowment for Democracy in Washington D.C., USA, the Center for Euro-Atlantic Studies has conducted a detailed analysis of the proposed 14 points pertaining to protection of the right to privacy and the affiliated human rights. Extensive previous consultation with the Ombudsman Saša Janković and the Commissioner for Information of Public Importance and Personal Data Protection Rodoljub Šabićm as well as many of the officials working in their offices, assisted in the rendering of the analysis. This Action Plan is the result of the analysis.

## GENERAL POLITICAL AND SECURITY CONTEXT

In July 2012, the Ombudsman and the Commissioner pointed to an alarming discrepancy between constitutional rights in terms of tracking of electronic communication and data protection and actual practice. They presented 14 Points, i.e. recommendations, to address this situation:

1. The Government should draft and propose and the Parliament should adopt only those laws which observe constitutional guarantees pertaining to privacy of communication and other human rights. The opinion of state bodies set up to protect citizens' rights should not be ignored by the Parliament of Serbia.

2. Urgently amend the relevant laws in order to determine which particular courts are empowered to decide on the requests by the police, the Military Security Agency (VBA) and the Military Intelligence Agency (VOA) to access data on citizens' communication (under existing legislation competent courts have been identified only in connection with requests by the Security and Information Agency (BIA) and the Ministry of the Internal Affairs).
3. Institute efficient organizational measures and IT solutions that accelerate previous court control and rulings on requests to access communication and communication data.
4. Unify the existing overlapping technical capabilities of various agencies and the police into a single national agency providing technical services necessary for intercepting communication and other signals to authorized users.
5. Unify procedures and obligations applicable to providers of electronic communication.
6. Ensure undeletable recording of accesses to telecommunications, with all data necessary for consecutive control of legality and regularity of access.
7. Continue to legally regulate the work of the private security sector. The deadline for aligning by-laws associated with the Law on Private Security and Detective Activity enacted on December 6, 2013 is May 6, 2014.
8. Enable robust legal and physical protection of whistleblowers (especially in the security sector, but also in general) and cede the jurisdiction for their protection to the Ombudsman.
9. Incriminate the obstruction of investigations conducted by independently controlled state bodies (the Ombudsman, the Commissioner for Information of Public Importance and Personal Data Protection, the Agency for the Fight against Corruption, the State Audit Institution and the Commissioner for Equality Protection). Any disturbance, threat or other attempt to influence a plaintiff or a witness cooperating with control bodies should be incriminated as a criminal offense constituting „obstruction of justice" when given subjects are concerned.
10. Introduce obligatory internal supervisory mechanisms to inform the Ombudsman and the competent parliamentary committees about findings which concern observance of human rights, especially when these rights are violated by top officials in state bodies in which internal supervisory mechanisms operate or in cases which testify about grave alleged or confirmed human right violations.
11. Reexamine results of the implementation of the Law on Data Privacy (including adoption of necessary by-laws, declassification of older documents, conducting of investigations, issuance of security certificates...) and make serious amendments to this Law or adopt a new one.
12. Strengthen the capacity of supervisory institutions to handle and keep sensitive data secured.

13. Adopt a new Law on Security and Information Agency in order to ensure predictability of the use of special measures, among other things.
14. Reconsider the competences of the police and the intelligence/security services i.e. their participation in criminal investigations.

In Serbia there is a problem that opens a possibility of uncontrolled access to personal data and citizens' communication, which had remained unnoticed until November 2012, when it personally affected Serbian President Tomislav Nikolić and the then Minister of Defense and the Coordinator of the Work of All Security Services and Serbian Vice Prime Minister Aleksandar Vučić. Making a guest appearance on the show called „The Witness" on Radio Television Serbia, Serbian President Tomislav Nikolić said: „We have fallen into *a snake's nest* among people who use their senior positions in state services to play master of people's lives, people who dare eavesdrop on both me and Aleksandar Vučić. It will have to be fully investigated. One cannot live like that in Serbia anymore." This was carried as news by all media and was confirmed the following day by Aleksandar Vučić, who announced comprehensive investigation and system changes. The information on the eavesdropping network were given to Vučić by the Security and Information Agency, which informed him that three days earlier one part of the Ministry of Internal Affairs has issued a warrant for tracking his and Nikolić's phone, allegedly as a part of tracking „a group, upon the request of the Ministry of Internal Affairs."

The Center for Euro-Atlantic Studies has responded by issuing a press release calling on all genuine pro-European forces in Serbia to demand urgent adoption of necessary laws and other implementing regulations, which would make sure that the current Serbian authorities are not tolerated – in the name of other priorities such as the dialogue between Belgrade and Pristina. The government's increasingly manifest incompetence or lack of intention to uphold the previously accomplished levels of democratic standards and division of powers, let alone advance them, risks all.

The recent example of the eavesdropping of the President himself is not the only example of the activities of uncontrolled power centers. Some time ago it was revealed that there are over 430 antennas of unclear origin installed at 16 control objects belonging to the Serbian Weather Forecast Service. Nothing has been done in connection with this discovery and CEAS insists that system solutions must be found to identify and prevent the activity of uncontrolled centers of power – regardless of the persons who are potential „victims" of use or abuse of competences.

CEAS has also stated that media and expert discussion about the fact that, as stated by Interior Minister Dačić, „the Criminal Investigation Police Department has sought telephone listings not knowing that it was the phone of Aleksandar Vučić", has unfortunately focused more of the questions on issues such as the chain of command or the timing of this affair rather than on the essence of the problem – namely unconstitutionality of the act itself and a lack of democratic oversight over the security sector. Both issues reinforce a dangerous tendency to establish party control over parts of the system, greatly aggravating their professional work. Therefore it is very important to make public the

content of measures for counter-intelligence protection of top state leadership, as had already been proposed, albeit quite timidly, by some state officials. The allegations that parts of the Interior Ministry acted unconstitutionally were, however, completely marginalized by the very victims of eavesdropping, namely Vučić and Nikolić themselves. Unlike them, the Ombudsman and the Commissioner have continued to point to the essence of the problem. The proposed 14 Points, the aim of which is to improve the situation in the security sector, have to obtain unreserved support by all genuine democratic and pro-European forces in Serbian society.

However, more than a year after this scandal, Serbian President Tomislav Nikolić claims that the eavesdropping affair has not been over yet and that he is still being secretly eavesdropped upon. He stresses that there are parts of the Ministry of Internal Affairs which do not do their job properly and that there are people who sabotage his security. The Serbian President illustrated what he meant by saying that when Prime Minister called him to say that the Ministry of Internal Affairs would be *launching a major* „Thunder strike" campaign against drug trafficking, the President told him to hang the line because „somebody might be eavesdropping." What is interesting is – who could be eavesdropping? If it is a state service or the Criminal Investigation Police Department, which was previously named by Dačić in late 2012, wouldn't they know about the „Thunder strike" campaign anyway? If they didn't – wouldn't they, in accordance with their area of jurisdiction, be supposed to know? If state bodies are not the ones eavesdropping, the criminals must be the ones doing it.

Therefore, despite positive steps such as the fact that the Military Security Agency (VBA) and the Security and Information Agency (BIA) do not interfere into privacy of communication without explicit court decision, there are still worrying concerns when the right to privacy and personal data protection of citizens of Serbia are concerned. The police still eavesdrop on citizens under the Criminal Procedure Code. The provideers who store information on access to the electronic communication of citizens have confirmed to the Commissioner that in 2012 the Security and Information Agency had twice as few inquiries about this communication as the Military Security Agency, while the Ministry of Internal Affairs of Serbia had one thousand times more inquiries about such communication than the Military Agency and two thousand times more inquiries than the civilian Security Agency.

According to an assessment of the Office of the Council on National Security and Classified Information Protection (National Security Authority of the Republic of Serbia), since the Law on Data Secrecy entered into force in January 2010, major problems have been posed by a lack of knowledge about the Law by public government bodies as well as a lack of harmonization among various laws, especially given the fact that some laws and by-laws enacted after January 2010 use the term 'official secret' and 'military secret,' although these terms are disused under the new Law, as well as that secret data are used in an inappropriate way.

According to the Ombudsman Saša Janković, a mere one provider in Serbia has had over 4,000 access requests within a year and over 270,000 direct accesses. There are four telephone providers in Serbia, so the total number of accesses to citizens' communication

according to some estimates might be as many as one million a year. The exact number is unknown, because other providers have not counted the number of accesses to the communication information of their users, and they have not denied access to unauthorized users.

There is also an issue of security checks envisaged under the law, which have not been defined in terms of the kind of data collected for this purpose, the manner of their keeping, the persons authorized to access them or whether their use is prohibited for other purposes etc. A year ago the Commissioner submitted an initiative to the Government of Serbia to draft a special law on security checks (the Initiative is attached in the Annex of this document). The law is supposed to define the notion of security check and specify the procedures it entails, as required by the Constitution of the Republic of Serbia. Interior Minister Ivica Dačić has said that this issue was open and that it must be defined by amending the Law on the Police. This issue is currently regulated only by the Law on Records adopted in 1996, which is outdated given the development of technology, and does not provide a clear definition of the sort of data collected and the purpose of its use.

In certain parts of the security sector in Serbia interference into personal data and citizens' communication is still considered to be an inalienable right of security services and the police. This is one of the issues that have not been publicly discussed before the Commissioner and the Ombudsman raised them, and this fact testifies to the truth of what the Ombudsman has said: „At some point even the National Parliament had defended „the right" of the security services to access data as they please, without heeding anyone else's, let alone court's, decision even though it is required under the Constitution."

Since there are two types of records, namely those held by the Ministry of Internal Affairs and those held by the Security and Information Agency, containing files on potential perpetrators, there are also two types of preliminary investigations – criminal investigation and investigation into possible breach of constitutional order. The basic question is when and against whom a preliminary investigation should be instituted, specifically which forms and methods of work of public and secret security services are allowed. The answer might lie in the source of their financing *(do they only use the state-allotted budget or is there alternative funding?).*

The additional problem is the fact that citizens of Serbia, despite the relative trust they have in independent institutions, maintain that the Ombudsman and the Commissioner do not exercise sufficient influence over the Government's decisions. The public opinion poll conducted by the Center for Euro-Atlantic Studies in April and May 2013 showed that there is a problem of highly divided attitudes toward independent institutions in general, including the institutions of the Ombudsman and the Commissioner in particular.

Only 37% of citizens said that they have trust in independent institutions, while 31% do not have trust, and 32% of Serbian citizens do not have an opinion on this issue. Upon closer inspection, the results show that in the eyes of the citizens, the Ombudsman exercises weak or no influence over Government decisions – 2% of citizens think that he has a strong influence, 10% think he has a moderate influence, 33% think he has a weak influence and 28% think that he has no influence, while 27% do not have an opinion. The situation is similar when the Commissioner for Information of Public Importance and

Personal Data Protection is concerned; only 3% think he has a strong influence, 11% that he has a moderate influence, 32% that he has a weak influence, 29% that he has no influence at all, and 25% do not have an opinion.

Even after a year and a half after the Ombudsman and the Commissioner presented their 14 recommendations, the situation has not significantly changed. The amended draft-law on Electronic Communications still, according to the Commissioner, runs the risk of containing phrases that are controversial in terms of access to citizens' communication data.

The Commissioner has once again insisted that it must be an obligation of a provider to keep records on the number of accesses to data, calling again for unifying procedures that providers of services of electronic communication must observe (point 5).

Even the introduction of the „double key" system into the work of the Security and Information Agency (BIA) has not solved the existing problems. A report by European expert Maurizio Varanese assessing the work of security services in Serbia, written in March 2014, states that the Security and Information Agency actually operates as a „provider" for all other services, so „whenever the police or the VBA want to intercept communication for purposes of investigation, the court warrant is handed to the BIA or the VBA, which use the technical equipment they possess to double the telephone line or to channel towards the Service for Special Investigation Methods (SSIM) of the Criminal Investigation Police Department, which has recently begun to intercept telephone calls using its own equipment or through rechanneling from an operator's equipment."

As the last element of such an alarming state of affairs, there is the fact that the Law on Free Access to Information is actually the only law mostly violated only by officials, because ordinary citizens cannot violate it. However, according to the Commissioner, despite this fact, no procedure against the perpetrators has been recently initiated, and the Commissioner still does not have the right to institute misdemeanor proceedings.

In his opinion, given an absence of strategic and well-designed approaches regarding issues of personal data protection, the activities of the Government of Serbia add new problems to the already numerous existing problems in this area. The laws and by-laws drafted and submitted to the Parliament treat the area of personal data processing in a way that does not accord with the Constitution and the Law on Personal Data Protection (e.g. the Draft Law on Export and Import Control of Dual-Use Goods).

During the course of explanatory screening for Chapters 23 and 24, the work of the police and the judiciary in terms of unified control of eavesdropping (the monitoring system) have not been discussed, except to note that it is necessary to better regulate the area of personal data protection. Independent institutions have given their opinion on the matter during their presentations in Brussels, and more detailed opening of this topic is expected after the arrival of the EU experts who will assess the situation in this area.

## IMPLEMENTED RECOMMENDATIONS

The amendments to the Law on the Military Security Agency and the Military Intelligence Agency were made in February 2013 when the Constitutional Court declared some Articles

of the law unconstitutional. The Court said that the Director of the Military Security Agency may order secret electronic surveillance of communication only if he has an approval from a first-instance court or a higher court in the territory under the jurisdiction of the Court of Appeals, where the measure is instituted for secret electronic surveillance of communication and gains an insight into only the listing of telephone calls (Article 12, paragraph 1, point 6 of the Law: *Secret electronic surveillance of telecommunication and information systems in order to collect required data on telecommunication traffic, without an insight into their content*). The amendment submitted by the Ombudsman Saša Janković was accepted, which specifies that if the VBA or VOA should acquire data and information for which other security or police services are competent, they must submit this data and information to other security services if they are important for national security and to the police if they pertain to criminal offenses. Constituting activities to gather special evidence is in accordance with the Criminal Procedure Code.

The second breakthrough was made in July 2012 by introducing „the double key" system into the work of the Security and Information Agency (BIA) in terms of intercepting communication. „The double key" system prevents eavesdropping of anyone's telephone number upon the request of merely one person within the Agency, thus reducing the possibility of abuse of electronic surveillance of citizens' communication.

Moreover, in September 2013 a series of regulations specifying more closely the subject matter of the Law on Data Secrecy, such as the regulation specifying narrower criteria for determining the degree of secrecy for „state secret" and „strictly confidential" („*The Official Gazette of the Republic of Serbia*" no. 46/2013 of May 24, 2013, which entered into force on June 1, 2013 and is effective as of September 1, 2013), the regulation specifying narrower criteria for determining the degree of secrecy of „confidential" and „internal" within the National Security Authority of the Republic of Serbia („*The Official Gazette of the Republic of Serbia*" no. 86/2013 of September 30, 2013, which entered into force on October 8, 2013) and the regulation specifying narrower criteria for determining the degree of secrecy of „confidential" and „internal" within the Security and Information Agency („*The Official Gazette of the Republic of Serbia*" no. 70/2013 of August 7, 2013, which entered into force on August 15, 2013 and is effective as of September 1, 2013), strengthened the capacity of the Law, as recommended by Point 11.

The enactment of a regulation specifying narrower criteria for determining the degree of secrecy of documents labeled „confidential" and „internal" for most other state bodies is under way, as well as the Law on so-called information security, which should provide a normative closing to the area of protection of secret data at the national level.

The National Security Authority of the Republic of Serbia emphasizes that a Task Force has been set up that is expected to amend the Law on Data Secrecy so as to remove the identified shortcomings and legal gaps of the existing Law and to create conditions for more effective implementation of the Law itself.

In December 2013 the Law on Private Security and the Law on Detectives were adopted, starting normative regulations of the private security sector. At a round table held in February 2014, the Commission for Public-Private Partnership in the Serbian Security Sector, which CEAS is a member of, presented, in cooperation with the Ministry of Interior,

three draft Rulebooks regulating the program and training requirements for private security officers in detail as well as a licensing process, without which this Law is not applicable. The deadline for adopting these Rulebooks is May 6, 2014, and if the new Serbian Government is assembled by then, that is, if the competent Minister is appointed – whose signature is needed for these Rulebooks to enter into force – they will be in place within the prescribed timeframe. In addition, another 4 Rulebooks and 2 Regulations are also prepared, which will be presented to stakeholders and enter into the decision-making process.

## GOOD PRACTICE EXAMPLES AND OTHER INITATIVES

### United Kingdom

The Information Commissioner's Office is an independent agency which maintains the public register of data controllers and implements the Data Protection Act, regulations which pertain to privacy and electronic communications and the Freedom of Information Act.

The area of jurisdiction of the Office was extended in 2010 to include serving a monetary penalty notice amounting as much as £500,000 for graver breaches of the principle of data protection, whereby its relatively limited executive powers were strengthened. The Office has issued guidelines describing the conditions under which the new powers of serving monetary penalty notices can be exercised. According to the guidelines, the Office has to ascertain that a grave breach of the right has occurred i.e. that there is a great possibility to cause significant damage or suffering to a person to which the data refers and to ascertain whether the breach was intentional or not.

Furthermore, the Office was invested with new powers to serve assessment notices to conduct compulsory auditing of non-complying state bodies. A Code of Practice has been written which defines new auditing competences.

The interception of communication is regulated by the Regulation of Investigatory Powers Act 2000 – RIPA. The Regulation empowers the Interior Minister to issue warrants for intercepting communication and requires providers of telecommunication services to ensure reasonable possibility of interception at their networks. The Regulation also envisages a possibility for any state body, authorized by the Interior Minister, to access

communication data without a warrant. This data refers to the source, the target and the type of communication, such as information about the location of a cell phone, location and partial logs of Internet search programs, while, for example, a full URL is considered to be content requiring a warrant.

The interception warrants and communication data are reviewed by the Commissioner for Interception of Communication, who is a former Supreme Court judge.

The British Government took one of the most radical steps in terms of regulation data protection in 2011, when it centralized security data. Security checks for persons who under other regulations required a background security check, namely officials of the Secret Intelligence Service (MI6), the Security Service (MI5) and the Government Communications Headquarters (GCHQ), are now conducted by an independent body – the Agency for Security Checks, which in 2011 became the National Security Vetting service, who together with FCO serves is the only provider of NSV for the entire government.

## The Netherlands

The Dutch Agency for Data Protection, College Bescherming Persoonsgegevens – CBP, supervises whether personal data records accord with the Law on Personal Data Protection. Even though the Agency's competences have mostly remained the same since its inception, its executive powers have grown in terms of instituting administrative measures and servicing monetary penalties for violations. The Agency can charge up to EUR 4,500 monetary penalties for breaches of the obligation to provide warrants for accessing information envisaged by Article 75 of the Dutch Personal Data Protection Act – PDPA. The CBP is at the same time an advisory body of the Dutch government in charge of complaints filed by persons that collected data refers to, initiating investigation proceedings, and making recommendations to personal data controllers.

In January 2008, the CBP President has called upon giving more supervisory competences to this institution in order to strengthen implementation of the Personal Data Protection Act and take direct action in terms of investigations and monetary penalties.

In the Netherlands, interception of communication, which concretely implies scanning and archiving of contents of communication, is regulated under the Penal Code and requires a court warrant (Article 125 of the Criminal Procedure Code). The intelligence services do not need a court warrant to intercept communication, but they have to be authorized by the Interior Minister.

The Law on Special Investigation Competences further advances investigation methods. The Law on Telecommunications requires that all providers of telecommunication services have capacities to intercept telephone and Internet communication, but that they should provide these services only to the bodies possessing a court warrant. A special agency, the Dutch Agency for Radio Communication, is in charge of conducting the eavesdropping procedure in the telecommunication sector.

The Law on Intelligence and Security Services enables interception, searching and scanning of satellite communication. It also grants intelligence services the right to keep data on intercepted communications for up to one year. The keeping of coded data, however, is not

limited. The national SIGNIT organization (NSO) was established in 2003 by the Dutch intelligence services for purposes of intercepting all satellite communication.

## Sweden

The Swedish Personal Data Law incorporates the requirements of the European Union Data Protection Directive 1995/46/EC into its national legislative framework. The Law regulates the establishment and the use of automatic records when pertaining to natural persons, both in the public and in the state sector.

The observance of the Personal Data Law is monitored by the Data Inspection Board (DIB), an independent state agency. The Personal Data Law envisages that the Board should be informed about every automatic data processing. Apart from several exceptions which pertain to obligation of information, any data processing which carries great risk of improper interference with the privacy of persons requires the Data Inspection Board to be notified, in order to conduct preliminary inspection. However, competences of the DIB may be perceived as relatively limited, because the Board may give recommendations, but their implementation depends on a court decision.

The Swedish Government set up in 2004 the Privacy Protection Board, made up of relevant experts and Members of Parliament, with an authority to analyze existing laws concerning privacy and conduct a public opinion poll regarding the issue. Due to the criticism that Personal Data Law is too restrictive, the Swedish Parliament in 2006 amended it, channeling it towards prevention of personal data abuse.

The Board has clearly pointed out that there is no institution bearing supreme responsibility for issues concerning privacy and proposed that a fully new Agency be set up to bear it or at least to mandate the Data Inspection Board with broader authority. This has resulted in the establishment of the Commission on Security and Integrity Protection – SÄKINT, an independent body appointed by the parliament and in charge of monitoring and controlling the use of secret surveillance by the police and the security services.

Every instance of use of video records, as well as surveillance and eavesdropping of communication, requires a court warrant in accordance with the Law on Measures of Investigation of Serious Crimes and the Law on Judiciary Proceedings. The laws on video and audio surveillance have evolved in time and have partly become elements of the Law on Judicial Proceedings, in parallel with a new law regulating these two areas, and giving competences to secret services. When in 2006 a draft law was expected to even further expand the use of secret surveillance, including, among other things, eavesdropping of telephone conversations for preventive purposes, the Parliament decided to postpone the debate on the draft law in order to include Articles on measures preventing possible abuse and obligation of the police to inform persons who are subjects of secret surveillance whenever it is considered safe for purposes of investigation.

Another controversial law was adopted in 2008, allowing the National Defense Radio Institution (Försvarets Radioanstalt - FRA) to use special software to search for sensitive keywords in all telephone and email communications unfolding through wired or wireless networks across country borders without a court warrant. Since the law has jeopardized

cross-border communication by allowing surveillance of electronic communication of persons who do not reside within the Swedish borders, strong public criticism and pressure by privacy protection groups has resulted in an amendment of the said Law.

### Slovenia

In Slovenia the right to privacy is enshrined by the Constitution as well as the Law on Personal Data Protection. The Law on Personal Data Protection is regularly updated to keep up with the development of technological achievements such as video surveillance, biometric data, etc. and is in accordance with the EU Data Protection Directive.

Moreover, Article 150 of the Penal Code bans unauthorized opening of letters and other post messages, interception of messages carried via telecommunication networks, unauthorized access to contents of messages carried via telephone or other telecommunication technologies, as well as unauthorized forwarding of letters to third persons. Article 151 of the Code further prohibits opening of private communication without consent by an authorized person.

The Personal Data Protection Law also specifies that everything which is not explicitly allowed regarding collection and processing of personal data is prohibited. State bodies may process personal data only for purposes for which they are legally authorized to do, while private persons must also possess the written consent of an individual. The persons whose personal data is collected must be notified in advance about this procedure. Generally, personal data may be collected and kept only for so long as it is necessary to accomplish a certain goal and it has to be deleted or blocked as soon as the goal is accomplished. All exceptions have to be clearly defined by the law.

By merging the Office of Personal Data Protection Inspectorate and the Commissioner for Access to Public Information, the Law on the Commissioner for Information has set up an Office of the Commissioner for Information as an autonomous and independent agency.

Privacy of communication can be violated only with a court warrant or if such violation is considered necessary for purposes of criminal investigation or for the sake of national security. In Slovenia, this area is regulated by the Criminal Procedure Code and the Law on Intelligence-Security Agency of Slovenia – SISAA and is implemented by the police and the Intelligence and Security Agency of Slovenia – SOVA.

A court warrant must be obtained before a house search or telephone eavesdropping is conducted. The Law on the Police allows secret surveillance and tracking, as well as secret police cooperation, but only in very special circumstances and with an authorization of the General Police Director.

### European Union

The basic rights are protected in the European Union by a legal framework consisting of three complementary elements:

- General principles and constitutional traditions common to all member states;
- The Charter of Fundamental Rights of the European Union;
- The European Convention on Human Rights.

The Charter explicitly singles out personal data protection and the right to privacy as a special right.

The Lisbon Treaty has created a foundation for further development of legislation pertaining to data protection, applicable to any kind of personal data processing both by private and by public sector, including personal data processing as a part of cooperation between the police and the judiciary.

The EU Data Protection Directive defines the foundations of personal data protection which member states have to adopt in their national laws and is applied to every automatic processing or other handling of personal data which make up a process of creating records. Personal data are defined as any information which pertains to a natural person. A data controller is in charge of processing personal data, ensuring the observance of the principles concerning data quality, the obligation to notify a person to which data refer about their collection and the authorization to take appropriate technical and organizational measures against illegal destruction, accidental loss or unauthorized changing, disclosing or accessing of data.

The Directive also requires member states to ensure supervision of implementation of provisions by establishing independent supervisory mechanisms. Supervisory mechanisms must have executive competences and effective areas of jurisdiction of intervention, such as a competence to order blocking, deleting or destroying data or imposing temporary or permanent ban on their processing.

Under the Directive, the Working Party on Data Protection and Privacy has also been established as a consultative body. The Working Party consists of representatives of supervisory institutions of member states and representatives of the European Data Protection Supervisor (EDPS).

### *The European Data Protection Supervisor*

The European Data Protection Supervisor is one of the key institutions in the area of privacy and data protection in the EU. It is responsible for supervision of personal data processing by the EU administration and has an advisory role in legal matters affecting the right to privacy and the right to personal data protection as well as cooperation with similar institutions.

### *Article 29 Working Party*

Article 29 Working Party (WP29) serves as a platform for exchange and coordination among supervisory bodies of EU member states, and as a consultative body. The main role of the Working Party is to examine all questions pertaining to an application of national measures adopted under the EU Data Protection Directive in order to establish a uniform application; it advises the European Commission on the level of protection in the Union and in third countries; it advises the European Commission on measures to safeguard the rights and freedoms of persons with regard to processing of personal data and on all other proposed measures affecting such rights and freedoms; it gives an opinion on codes of conduct drawn at the EU level.

The Working Party may, on its own initiative, make recommendations on all matters relating to privacy and data protection in the EU. It has so far issued an opinion on issues

such as biometric data in passports and visas, protection of personal data of children, standard contracts on the transfer of personal data processed in third countries, etc. The opinions of the Working Party are a common reference point for interpretation of the EU Data Protection Directive.

### *The Global Network Initiative*

Global Network Initiative is a coalition of IT companies, civil society, investors, and academics. The goal of the Initiative is to provide a framework in which providers of electronic services – companies – may operate in accordance with international standards, ensure responsibility of these companies by providing an independent assessment, enable engagement in policy-making, and enable exchange of experiences among all stakeholders.

In September 2013, the Initiative wrote to governments of member states of the Freedom Online Coalition, demanding that a practice be established to report on warrants issued by states to conduct surveillance of electronic communication, as well as to provide a legislative framework that would allow companies to regularly inform the public on warrants they obtain from the police and security services.

This makes it clear that most European countries have systems in which non-court instances have the right to issue warrants to gain insight into a broad range of data. Secondly, areas of secret surveillance and communication protection on the one hand and personal data protection on the other are often mixed up.

## POINT 4: UNIFY THE EXISTING OVERLAPING TECHNICAL CAPABILITIES OF VARIOUS AGENCIES AND THE POLICE INTO A SINGLE NATIONAL AGENCY

*Unifying the currently overlapping technical capabilities of the police and other various agencies into a single national agency that would provide the technical services necessary for intercepting communication and other signals to all authorized users is required.*

Unifying all overlapping technical capabilities of various agencies and the police into a single capability would certainly largely reduce the possibility of abuse of interception and tracking of telecommunication and other citizens' communication.

Taking into account what one of the four interviewed cell phone providers in Serbia has said, namely that out of 4,400 warrants to access recorded data only 2 were submitted by the Security and Information Agency (BIA), we can conclude that the BIA must have its own capability to access recorded data, enabling it to handle this data autonomously and without any supervision. Does the Interior Ministry also have such a capability? Can such unrestrained access to collected recorded data be both a protection of the country's security and at the same time a protection of the constitutional rights of citizens to whom the kept data refer to? It is debatable whether such access is both justified and in accordance with the established constitutional principles, which is precisely why this Action Plan has been written in the first place. The establishment of a single national independent agency that would provide technical services necessary for intercepting communication and other signals to all authorized users would remove the possibility of illegal action.

Due to the fact that terms of office are limited for most governments in the world, the fear most governments face is the centralization of security services because such an action would „bite the hand that feeds them." This is especially pertinent for Serbia in which coalition governments and the portfolio race prevail.

However, taking into account the situation and the state of affairs in the security sector in Serbia, where, according to media reports and the testimony of former state security officials – for example, Momir Stojanović, former director of the Military Security Agency (VBA) – some employees of the Ministry of Interior Affairs of Serbia (MUP RS) are on the payroll of tycoons and drug dealers, while at the same time two thousand people are on a secret and illegal payroll of the Interior Ministry, including informers who are paid through the secret payroll, it is questionable to what extent the said recommendation is implementable. The unifying of overlapping technical capabilities into a capability of a single agency can be set as a long-term goal, however to attain it would require Serbia to take several smaller short-term, intermediary steps.

It would be primarily necessary to amend the existing legislation. The Ombudsman and the Commissioner pointed in November 2012 to the laws on Electronic Communication, on Military Security Services, on Security and Information Agency and on Criminal Proceedings as the most critical ones in need of reform.

## The Law on Electronic Communications

The first on the list of laws which the Ombudsman and the Commissioner consider requiring urgent amendment is the Law on Electronic Communications. The Constitutional Court of the Republic of Serbia has declared some provisions of this Law unconstitutional in terms of access to recorded data. The same provisions were disputable when the Law was supposed to be enacted. The Constitutional Court declared unconstitutional the provisions of Article 128, paragraph 1, Article 128, paragraph 5, and Article 129, paragraph 4, which pertain to access to recorded data without a court decision and to the authority of a competent Ministry to enact by-laws regulating warrants to access kept data.

The problem has emerged due to the uneven and incoherent legal framework which pertains to the kept data, in particular the content of communication. The kept data represents data on communication that does not concern the content of communication. The data primarily concerns data on tracking and determining the originator of communication, determining the recipient of communication, determining the beginning, the duration, and the end of communication, determining the type of communication, identifying the terminal equipment of the user, and determining the location of the cell terminal equipment of the user. If we take a telephone call as an example, this data refers to the number from which it was dialed, the dialed number, the data and the time of the beginning and the end of the telephone call, the duration of the telephone call, the device used in communication (a cell phone type), as well as data on the geographical location of the telephone from which it was dialed - but the data does not identify the dialed users.

The disputed provisions violate procedural guarantees enshrined under Article 41 of the Constitution of the Republic of Serbia, which envisages that any aberration from the principle of inviolability of secrecy of letters and other means of communication is possible only temporarily and on the basis of a court decision if necessary for purposes of conducting a criminal investigation or protecting the security of the Republic of Serbia in the manner envisaged under the law.

However, the Draft Law Amending the Law on Electronic Communications risks to keep the same unconstitutional clauses despite a provision that limits the secrecy of communication that has to be justified by a court decision. Namely, the Commissioner has emphasized during the conducted public debate on the Draft Law Amending the Law on Electronic Communications that aberrations from the principle of inviolability of secrecy of communication under the Constitution of the Republic of Serbia are possible only in cases of conducting a criminal investigation or protecting national security. The Draft Law Amending the Law on Electronic Communications, however, also adds aberrations in cases of conducting investigation or disclosing a criminal offense, in addition to protecting public security; such a term is much broader than the term national security, thus the provision violates the limitations imposed by the Constitution.

If this and similar objections are not heeded, the provisions of the Law will remain unconstitutional.

## The Security and Information Agency (BIA)

There has been certain progress when it comes to the BIA in terms of personal data protection. Namely, upon the recommendation of the Ombudsman, the Security and

Information Agency (BIA) introduced in August 2012 the so-called „double key" system for accessing citizens' communication. „The double key" system makes it impossible to eavesdrop on someone's phone upon the request of only one BIA employee, which means that it will no longer be possible for one person to be able to order the eavesdropping of someone's telephone on his/her own, but only „in tandem" with a person authorized to approve such a measure. Such a requirement would reduce the possibility of abuse of eavesdropping of the electronic communications of citizens.

As has been mentioned, the report written in March of this year by the European expert Maurizio Varanese assessing the work of security services in Serbia states that the BIA actually functions as *a provider* for all other services. Whenever the police or the Military Security Agency (VBA) want to intercept communication for purposes of investigation, a court warrant is handed to the BIA or the VBA, who then use the technical equipment they possess to double or channel a telephone line towards the Service for Special Investigation Methods (SSIM) within the Crime Police Department, which until recently has been conducting the interception of telephone conversations.

The Constitutional Court has recently declared three provisions of the Law on Security and Information Agency (BIA) unconstitutional. The decision found that the provisions of Article 13 of the Law on the Security and Information Agency specifying aberrations from the principle of inviolability of secrecy of letters and other means of communication is not in accordance with the Constitution because it has not been formulated in a sufficiently precise way. The disputed provision states that „The Director of the Agency may, if necessary due to the security of the Republic of Serbia, make a decision on the basis of an existing court decision to take certain measures regarding certain natural and legal persons who deviate from the principle of inviolability of secrecy of letters and other means of communication in a procedure established under this Law." The Court has found that the disputed provisions of Article 14 and Article 15 of the Law are also not in accordance with the Constitution because they are legally and logically connected with the provisions of Article 13, which had previously been found to be unconstitutional. However, the publishing of this ruling has been postponed for six months instead of four months, as was originally decided on by the Constitutional Court.

This Court's ruling was taken as a result of the initiative to reconsider the Law's constitutionality submitted by the parliamentary Committee for Constitutional Issues and Legislation. Given that the Parliament of Serbia has in the meantime been dissolved, the ruling cannot be published since under the Constitution, only the Parliament can attend to ongoing affairs.

„It means that until the new National Parliament has been constituted, it would objectively not be possible to redress the unconstitutionality by appropriately amending the Law," the Constitutional Court has said.

### Military Services

In February 2013 the Law Amending the Law on Military Security and Military Intelligence Agency was adopted. After the ruling by the Constitutional Court in which two Articles of the Law on Law on Military Security and Military Intelligence Agency were declared unconstitutional, it was established that the Director of the Military Security Agency (VBA)

could only issue a warrant for secret electronic surveillance of communication with a court approval. The law's amendments envisage that a higher court under the area of jurisdiction of an appellate court, competent for the territory where the measure is supposed to be taken, should approve secret electronic surveillance of telecommunication, thus enabling an insight into the „listing" – Article 12, paragraph 1, point 6 of the Law: *Secret electronic surveillance of telecommunication and information systems in order to collect kept data on telecommunication traffic, without an insight into their content.*

It has been specified that special procedures and measures can only be taken on the basis of a written and justified warrant issued by the director of the VBA or an VBA employee authorized by the VBA director and that records must be kept about all issued warrants. This was requested by the amendment submitted by the Democratic Party of Serbia. It is envisaged that a judge of a higher court located in the area of jurisdiction of the appropriate appellate court should issue a ruling to take special measures without delay and within eight hours at most. In addition to the secure protection of information and telecommunication systems, the VBA is to continue to provide cryptic protection.

The adopted amendment submitted by Ombudsman Saša Janković envisages that if the VBA or the VOA (Military Intelligence Agency) should acquire data and information falling under the area of jurisdiction of other security services or the police, they are obliged to forward this data and information to other security services if they are important for national security or the police, such as if they pertain to criminal acts which require special procedure of gathering evidence that are in accordance with provisions of the Criminal Procedure Code.

The Serbian parliamentary Committee for the Control of Security Services has recently adopted a six-month report on the work of the Military Security Agency. The members of the Committee have positively assessed the professional conduct and work of members of this Agency in conducting priority tasks, emphasizing full support to their further engagement on realizing priority tasks of security and counterintelligence protection of the Ministry of Defense and the Serbian Army, as well as of fighting organized crime and corruption.

### The Criminal Procedure Code

The Ombudsman and the Commissioner have submitted the initiative to the Constitutional Court to reexamine constitutionality of Articles 282 and 283/6 of the Criminal Procedure Code that envisage that the prosecution may „submit a request to state and other bodies and legal persons to provide necessary information." This should not be disputable if the legal norm is correctly interpreted, but correct interpretation necessarily implies that the norm should not refer to data which are the subject of special constitutional guarantees of human rights and which can only be made available to someone, including the prosecutor, under conditions and in a manner envisaged by the Constitution. Acting upon the request of the public prosecutor, in order to fulfill duties from paragraph 1 of this Article, the police may acquire records of a telephone communication that has been made by using a base transmitter station or by locating the place from which the communication has proceeded.

This particularly refers to the listing of communications by natural persons to which constitutional guarantees regarding secrecy of letters and other means of communication referred to in Article 41 of the Constitution. Access to this data, under an explicit constitutional provision, is allowed only on the basis of a court decision. Therefore a request by the prosecution to acquire such data without a court decision and accompanied by the possibility of servicing monetary penalties represents an exceeding of competences held by the prosecutor under the Criminal Procedure Code and a violation of the said constitutional guarantees. The Constitutional Court has not yet issued a ruling on this matter. In order to take steps to implement measures proposed by the Ombudsman and the Commissioner, it is necessary that the Constitutional Court declare unconstitutional the disputable provisions of the Criminal Procedure Code in order to consistently apply the principle of procedural guarantees enshrined under Article 41 of the Constitution of the Republic of Serbia in all laws regulating access to kept data.

Therefore the police is the only security service in Serbia which is empowered by a law, which contravenes the Constitution, to acquire access to information and to eavesdrop. Therefore it is technically unfeasible to unify the agencies and the police into a single national agency if the same laws do not equally apply to all services, i.e. if a necessary reform of the security sector is not previously conducted in order to align the laws pertaining to this area with one another and even more importantly with the Constitution.

### Other measures

In order to ensure efficient implementation of the said laws as well as functioning of competent services, these legal solutions have to be accompanied by appropriate organizational measures such as a 24-hour judge service and information solutions that accelerate previous judicial control and ruling on requests to access communication and communication data.

### Conclusion

The consequences of the said Constitutional Court rulings are multiple. Primarily, it is indisputable that the security services and bodies within the national defense and internal affairs system will from now on be able to collect and access data only on a previously issued court decision. In addition, issues concerning kept data will from now on have to be regulated by laws rather than by-laws. Moreover, these two rulings will require full harmonization of the Criminal Procedure Code with the Constitution.

It is therefore necessary to regulate the problem of interception of communication and other signals by BIA, VOA and VBA as well as the police before a single national agency that would implement these measures could be set up. Bearing this problem in mind, a document drafted by world organizations committed to the right to privacy, consisting of both civil society and experts for privacy and technology entitled The International Principles on the Application of Human Rights to Communications Surveillance may serve as a guideline for further steps. The principles have been published simultaneously with a report by the UN Special Envoy On Freedom Of Opinion And Expression, which deals precisely with issues of broad use of state surveillance of communications, concluding that such surveillance gravely breaches the citizens' life to a private life, free expression and other fundamental human rights. The need to strike a balance in the application of

constitutionally guaranteed human rights and constitutionally guaranteed security of citizens has also been recently emphasized by the UN High Commissioner for Human Rights.

According to the International Principles on the Application of Human Rights to Communications Surveillance, when adopting new technology of surveillance and access to electronic communications or expanding the existing technology, before accessing the information, the state must ascertain whether it qualifies as „protected information" and whether the surveillance procedure should be a matter of judicial or other democratic supervisory mechanism, i.e. in what manner it is to be used. When discussing whether the data obtained by surveilling or accessing electronic communications falls under „protected information," the state must take into account the form, the scope and the duration of surveillance as relevant factors. Considering that comprehensive and systemic surveillance may reveal private information that the scope of which far exceeds the concept of inherent pieces of information that are available, it is necessary to raise the level of surveillance of unprotected pieces of communication to the level which implies strong protection.

In order to ascertain whether the state may conduct surveillance and acquire access to electronic communications if it thus impinges on protected data, the following principles must be observed:

- **Legality**: Any limitation to the right to privacy must be prescribed by law.
- **Legitimate aim**: The law should only permit surveillance and access to electronic communications by specified state authorities if surveillance as a measure is necessary in a democratic society to protect a legally envisaged legitimate aim.
- **Necessity**: The laws which permit surveillance and access to electronic communications by the state must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim.
- **Adequacy**: Any measure of surveillance and access to electronic communications authorized by law must at all levels be appropriate to fulfill the specific legitimate aim.
- **Proportionality**: The decisions permitting measures of surveillance and access to electronic communications must be made by weighing a legitimate interest sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests that can be made when applying those measures, and should involve a consideration of the sensitivity of information and the severity of the infringement on the right to privacy.
- **Competent judicial authority**: Any decision on surveillance and access to electronic communications must be made by a competent judicial authority that is impartial and independent.
- **Due process**: Due process requires that states respect human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced and available to the general public.
- **User notification**: Individuals should be notified of a court decision authorizing surveillance and access to electronic communications with enough time and information to enable them to appeal the decision approving the surveillance of

electronic communications, and should have access to the materials presented in support of the application for authorization.

- **Transparency**: States should enable communication providers to publish the procedures they apply when dealing with state surveillance and access to electronic communication data, and how to adhere to these procedures and publish records of state surveillance and access to electronic communications.
- **Public oversight**: States should establish independent oversight mechanisms over how to apply measures of surveillance and access to electronic communications to ensure transparency and predictability of such surveillance.
- **Integrity of the communication system**: In order to ensure the integrity, security and privacy of electronic surveillance, and in recognition of the fact that compromising security for state purposes almost always compromises security more generally, states should not compel operators or hardware and software vendors to build electronic surveillance or monitoring capability into their systems, or to collect or retain particular information purely for state surveillance purposes.
- **Safeguards for international cooperation**: The mutual legal assistance treaties (MLATs) and other agreements entered into by the state should ensure that, where the laws of more than one state could apply to surveillance and access to electronic communications, the available standard with the higher level of protection for individuals is applied. Where states seek assistance for law enforcement purposes, the principle of dual criminality should be applied.
- **Safeguards against illegitimate access**: States should enact legislation criminalizing illegal surveillance and access to electronic communications by public or private bodies. The law should provide sufficient and significant civil or criminal penalties, protection for whistleblowers, and avenues for redress for affected individuals. The law should stipulate that any information obtained in a manner that is inconsistent with these principles or derivative of such information is inadmissible as evidence in any proceeding. States should also enact laws providing that, after material obtained through electronic surveillance has been used for the purpose for which permission was given, the material must be destroyed or returned to the individual under surveillance.

## POINT 5: UNIFY PROCEDURES AND OBLIGATIONS APPLICABLE TO PROVIDERS OF ELECTRONIC COMMUNICATION

*The unification of procedures and obligations applicable to providers of electronic communications is required.*

The right to privacy is a fundamental human right of vital importance in democratic societies. This right is necessary for the observance of human dignity and represents a precondition for observance of other rights such as the right to freedom of expression and information and the right to freedom of association; international treaties protecting human rights also guarantee it. The measures of surveillance and access to electronic communications, which infringe the right to privacy, may be justified only if they are envisaged by law, necessary for achieving a legitimate aim, and proportionate to that aim.

However in Serbia there is no rulebook, code of conduct, or guidelines that would enable service providers to refer to them in case they suspect that cooperation with security services could lead to an infringement of the law.

The Law on Electronic Communications merely specifies that „interception of electronic communications which reveals the content of communication is not permitted without a user's consent, except for a limited time and on the basis of a court decision, if it is necessary for conducting a criminal proceedings or protecting the security of Republic of Serbia, in a manner envisaged by law" (Article 126 of the Law on Electronic Communications). However, the Law does not contain more specific provisions that are standardized and that enable providers of services of electronic communications to adhere to them.

It must be emphasized that Serbia is not the only country which is faced with this problem. The companies which provide services of information and communication technologies throughout the world are faced with increased pressure by states to comply with requests which often breach internationally acknowledged standards of human rights to privacy and freedom of expression. Due to inexistence of clear guidelines, regulations and the legal framework, there is a possibility for providers of services of electronic communication to join forces and self-regulate the sector, thus exerting pressure on the Government to take steps towards full adoption of this Point.

A possible solution is provided by recommendations made by a multi-dimensional group of companies, civil society organizations, investors and academics who have established the Global Network Initiative to protect and advance freedom of expression and privacy in the context of the use of information and communication technologies. The Initiative has issued a guide for implementing principles of freedom of expression and privacy, intended for all stakeholders, including those in information and communication technology industry, describing a series of steps that would enable alignment with the principles, as well as a series of steps for their implementation.

In accordance with these principles, the providers of services of electronic communications are among other things advised to:

- *Firstly assess the impact of human rights on their market, products, technologies and services and determine which aspects represent the greatest threat to freedom of expression and privacy and to human rights*
- *Update these assessments of impact of human rights regularly whenever there are significant changes of legislation, regulations, market, products, technologies or services*
- *Use the advantages afforded by cooperation with human rights groups, state bodies, international organizations and publications generated through such cooperation*
- *Incorporate the results of such assessments of impact on human rights into their other activities such as assessment of corporate risk*.

By joining forces, the companies could compel the state to be transparent and consistent in its requests, laws and regulations, and to make them accord to international rights and standards. The next step would be to adopt policies and establish procedures, i.e. the manner in which providers of electronic services may assess and respond to requests by state services to access personal data. The providers should therefore interpret the requests in a narrow way and act only upon those which sufficiently respect the preservation of privacy; requiring clarification or altering requests when they seem to exceed the given competences, are unlawful, do not adhere to legal procedure, or do not accord with international standards of human rights and standards pertaining to privacy is necessary.

For the sake of more efficient implementation and better control of legality of surveillance measures, the Commissioner and the Ombudsman have suggested that it is necessary to create conditions at both normative and practical levels to unify existing overlapping and multiple technical capabilities of various agencies and the police into a single national agency which would provide technical services necessary for intercepting communication and other signals to all authorized users. In the long run, this would unify procedures applicable to providers of services of electronic communications and their obligations and would ensure undeletable recording of accesses to telecommunications, including all data necessary to make subsequent serious oversight of legality and regularity of access. In the meantime, self-regulation in cooperation with other stakeholders such as civil society, academics, investors etc., seems to be a more viable option at this point.

## POINT 10: INTRODUCE OBLIGATARY INTERNAL SUPERVISORY MECHANISMS TO NOTIFY THE OMBUDSMAN ABOUT THEIR FINDINGS

*Introducing obligatory internal supervisory mechanisms to inform the Ombudsman and the competent parliamentary committees about findings which concern observances of human rights, especially when these rights are violated by top officials in state bodies in which internal supervisory mechanisms operate or in cases which testify about grave alleged or confirmed human right violations, is required.*

The establishment of a system in which supervisory mechanisms of internal control would be directly channeled towards cooperating with the Office of the Ombudsman and the Commissioner in order to exercise full protection of personal data and data of public importance represents a fundamental step towards their institutional strengthening. However, an implementation of this Point might pose two problems.

Firstly, the biggest resistance towards implementation of this Point comes from state institutions themselves. The fact that they consider their interior mechanisms *theirs* makes them perceive independent control mechanisms, such as the Ombudsman and/or the Commissioner, as a potential threat.

On the other hand, despite media attention enjoyed by the institutions of the Ombudsman and the Commissioner, it seems that competent institutions, but also organization and companies (such are providers of services of electronic communications) are not sufficiently acquainted with the legal framework within which the Ombudsman and the Commissioner work. This is also confirmed by the fact that, as the Ombudsman himself has underlined, some providers of electronic communication, despite the adopted Law on the Ombudsman, have maintained that they had to ask the Security and Information Agency (BIA) whether they are allowed to transfer the collected data to the Ombudsman as an independent, control state body.

Secondly, the topic of this Point is narrowly associated with the question of protection of whistleblowers, which both the Ombudsman and the Commissioner had referred to also in Point 8 on the list of 14 Points, calling upon the need to „enable strong legal and factual protection of whistleblowers." Despite the fact that the Law on the Ombudsman specifies that the Ombudsman has the right to conduct a conversation with *any* employee within an administrative body when it is important for the proceedings being conducted, this practice is often common because it is made impossible, or because the employees do not want to cooperate due to a lack of institutional protection of the whistleblowers.

The Law on the Protection of Whistleblowers would regulate the protection of persons who, due to reasonable doubt of corruption or the disclosing of data on other harmful or potentially damaging phenomena for the legally protected public interest, report such data to competent state and independent bodies.

The public debate on the working version of the Draft Law on the Whistleblowers made by the Ministry of Justice has recently been completed. In our opinion, as well as the opinion of the majority of the non-governmental sector, and the Commissioner and the Ombudsman, the working version of the Draft Law has missed the intention and does not provide an

adequate protection to whistleblowers which is necessary for the protection of the public interest, which had not even been defined in the working version of Draft. It remains to be seen how much the comments would be acknowledged and whether this very important Law would be enacted in accordance with the general intention.

## CONCLUSIONS AND RECOMMENDATIONS

The analysis of the existing legal framework has shown that it is necessary to regulate the protection of privacy and protection of personal data of the citizens of Serbia, which presently greatly diverges from the constitutional guarantees.

The 14 Points, which the Ombudsman Saša Janković and the Commissioner for Information Rodoljub Šabić published in July 2012, represents the starting point for the regulation of this area in order to enable unhindered exercise of constitutionally guaranteed human rights.

CEAS reminds that, according to results of the research "For a more dynamic security sector reform in Serbia" on the state of affairs in the security sector and necessity further reform steps, conducted within the project "It's Time: Advocacy of Continuation of Security Sector Reform in Serbia" in November 2012, the engaged public within the target group (including the MPs, state officials and civil society) has expressed an interest to regulate this area. Unfortunately the political elite, neither the previous one nor the present one, has not shown sufficient political will to place this issue on the public agenda.

CEAS believes that it is necessary to adopt a specific Law on Security Vetting in order to, primarily, have the assessments and conclusions arising from security vetting procedures of individuals placed under democratic control in order to reliably prevent possible abuses.

CEAS supports the proposed 14 Points in full and calls on the competent institutions to adopt the envisaged regulations and rulebooks as soon as possible in order to ensure implementation of laws regulating this area.

CEAS maintains that the expected beginning of negotiations with the European Union and opening of Chapters 23 – Reform of the Judiciary and Fundamental Rights and 24 - Justice, Freedom and Security, as well as 32 - Financial Control, open the possibility for the Western international community to exert an additional pressure on the political elite in Serbia to regulate this area in full.

CEAS welcomes cooperation of military security services, or more precisely, the Military Security and the Military Intelligence Agency with the Ombudsman and the Commissioner.

CEAS also welcomes the cooperation of the Security and Information Agency with the Ombudsman and the Commissioner.

CEAS hopes that the Ministry of Internal Affairs will follow suit in accordance with support for the Ombudsman and the Commissioner, which the Minister Ivica Dačić has publicly expressed. CEAS hopes that the Ministry, as a service of the security system, takes necessary measures as soon as possible to regulate the area of surveillance and access to electronic communications of citizens also within the Ministry.

CEAS supports the activities of the National Security Authority of the Republic of Serbia towards normatively regulating of area of protecting data secrecy.

CEAS has, after detailed consultations with the Ombudsman and the Commissioner and other representatives of these institutions, as well as consultations with the Office of the National Security Authority of the Republic of Serbia, articulated the following short-term recommendations:

- Amend the Law on Electronic Communications after the Constitutional Court has found that provisions 128 and 129, which concern access to kept data without a court decision and upon the authority of the competent Ministry to more closely regulate requests regarding kept data with by-laws, are unconstitutional;

- Amend the Criminal Procedure Code which envisages that the prosecution „can submit a request to state and other bodies and legal persons to provide the necessary information";

- Align, within the given deadline, the disputable provisions of the Law on the BIA, which the Constitutional Court of Serbia has proclaimed unconstitutional, and which pertain to secrecy of letters and closer defining of category of persons against which special measures of surveillance can be applied (including eavesdropping upon a court's warrant)

- Regulate the question of intercepting electronic communications of citizens by the police so that the question could be regulated in a uniform way by all security services of Serbia;

- Encourage the electronic communication service providers to more closely cooperate and self-regulate in order to develop a common standard adhered to by all service providers;

- Adopt an adequate Law on the Protection of Whistleblowers which would ensure both legal and factual protection to them in order to enable a safe legal framework for cooperation with institutions of the Ombudsman and the Commissioner;

- Adopt a specific Law on Security Vetting;

- Remove the identified shortcomings and legal gaps of the existing Law, as well as create conditions for more efficient implementation of the Law itself;

- Educate public authorities about the Law on Data Secrecy and align the normative framework in terms of terminology and handling of secret data in general.

This would enable realization of some of the long-term goals:

- **Unifying all overlapping technical capabilities for interception of communication and other signals into a single national agency (point 4);**

- **Unifying procedures applicable to electronic communication service providers (point 5);**

- **The cooperation between internal control mechanisms and the institutions of the Ombudsman and the Commissioner (point 10).**

CEAS will continue, as a part of its activities, within this as well as other projects, to monitor the events in this area.

## ANNEX I: The Initiative of the Commissioner for Information of Public Importance and Personal Data Protection to Enact a Law on Security Checks; submitted to the Government of the Republic of Serbia on October 15, 2012

**Republic of Serbia**
Commissioner for Information of Public Importance and Personal Data Protection
42, Svetozara Markovića street
11000 Belgrade

Tel: +381 (0) 11 3408-900
Fax:+381 (0) 11 2685-023
office@poverenik.rs
www.poverenik.rs
Mail address:
22-26, Nemanjina street, Belgrade

Number: 011-00-685/2012-01 Date: 15.10.2012

THE GOVERNMENT OF THE REPUBLIC OF SERBIA

11000 Belgrade
11, Nemanjina street

Upon an overview of laws and other legislation regulating the subject matter of security checks, on the basis of actions taken in response to petitions submitted by citizens and in accordance with Article 44, paragraph 1, point 1 and point 11 of the Law on Personal Data Protection („Official Gazette of the Republic of Serbia“ no. 97/2008, 104/2009 – state law and 68/2012 – Constitutional Court ruling), the Commissioner for Information of Public Importance and Personal Data Protection submits

AN INITIATIVE TO ENACT A LAW ON SECURITY CHECKS

Assessing that there are several reasons which make it necessary to regulate the subject matter of security checks in the Republic of Serbia in a uniform and comprehensive way, I submit to the Government of the Republic of Serbia the Initiative to draft and submit to the National Parliament of the Republic of Serbia for adoption a Draft Law on Security Checks, in accordance with its jurisdiction under Article 123, point 4 of the Constitution of the Republic of Serbia.

At present, the Constitution of the Republic of Serbia („Official Gazette of the Republic of Serbia“ no. 83/2006) envisages that the Republic of Serbia regulates and ensures security of the Republic of Serbia (Article 87, point 4). The Law on Foundations for Regulation of Security Services of the Republic of Serbia („Official Gazette of the Republic of Serbia“ no. 116/2007 and 72/2012) regulates the subject matter of the country’s security-intelligence system, the

question of channeling and aligning the work of security services, as well as an oversight over their work, but not the subject matter of security checks.

The subject matter of security checks is regulated by several laws and other regulations but in an inappropriate way. The reason is that conducting of security checks is only regulated in the context of the subject matter directly regulated by the given law or other legislation. This pertains to laws and other legislation which regulate the subject matter of civil service employment, especially in the police, the army and the security services, as well as the subject matter of education in educational institutions which lead towards employment in the aforementioned state bodies.

Thus for example the Law on Data Secrecy („Official Gazette of the Republic of Serbia“ no. 104/2009) contains provisions, which regulate this subject matter more comprehensively than other laws, but only in the context of an access to secret data. Similarly, the Law on Organization and Jurisdiction of State Authorities in Combating Organized Crime and Other Serious Criminal Offenses („Official Gazette of the Republic of Serbia“ no. 42/2002, 27/2003, 39/2003, 67/2003, 29/2004, 58/2004 – state law, 45/2005, 61/2005, 72/2009, 72/2011 – state law and 101/2011 – state law) regulates this subject matter in the context of a narrow circle of persons from a very small number of judicial bodies and does so under unclear and insufficiently precise provisions. Moreover, provisions of the Law on the Police („Official Gazette of the Republic of Serbia“ no. 101/2005, 63/2009 – CC ruling and 92/2011) contain only a very general definition of a security threat and regulate the security check only in the context of employment in the Ministry of Internal Affairs. These provisions of the Law on the Police to conduct security check are referred to by the Decision to Establish the Crime Police Academy („Official Gazette of the Republic of Serbia“, no. 38/2006), even though this academy is a higher education institution and not an organizational part of the Ministry of Internal Affairs; nevertheless, security check are envisaged as a part of the conditions for submitting applications to enroll this higher education institution. The Army of Serbia also does not regulate the conducting of security checks in the process of recruitment to the Army under a Law, but under a Rulebook on Security Checks of Persons conducted by the Military Security Agency („Official Military Gazette“, no. 18/2010).
The basic shortcomings and disputable issues regarding the provisions of these and other not unmentioned laws and other legislation as well as regarding their implementation are:

1. For decades, the subject matter of security checks has been regulated in Serbia by laws and other legislation, but only in a segmented, incomplete and imprecise way;
2. Most of these laws and regulations do not contain provisions on basic terms, subjects undergoing security checks, purposes and procedures of conducting the check, deadlines etc, which leaves too much space for discretionary interpretation and conduct of competent bodies, even individuals. In case when aforementioned legislation contains these provisions, it is almost always incomplete and/or pertains exclusively to areas which are directly regulated by these regulations;
3. Several decades of implementation of this as well as previously valid regulations incorporating the same or similar solutions has produced breaches of human rights and freedoms, especially the right to privacy, that is, the right to personal data protection. For example, the processing of data is often conducted with no legal grounds or legal consent of persons to which data refer; the processing of data of third persons, normally family members, for which a person whose data are

processed cannot give consent is often conducted; almost without exception provisions of the Law on Personal Data Protection are breached which regulate the right to information about personal data processing, the right to gain an insight into such data, the right to a copy of these data etc, for which misdemeanor and in some cases criminal responsibility have been envisaged under the law.

In order to amend the identified shortcomings, I submit this Initiative to enact a Law on Security Checks. The solutions envisaged by the Law the enactment of which is hereby initiated should enable competent bodies to conduct security checks in all situations in which they consider and legally envisage it as necessary, in accordance with the Constitution (which in Article 42 envisages that „collection, keeping, processing and using personal data is regulated by Law“ to which security checks certainly belong), but such solutions should at the same time be aligned with the Constitution of the Republic of Serbia, the Law on Personal Data Protection as well as universally accepted rules of international law.

The Law on Security Checks should basically in a uniform and comprehensive way consistently regulate conducting of security checks and in particular the following issues: definition of basic terms, primarily the terms of a security check and a security threat; types of security checks being conducted; data that are checked, the instance conducting the check and the situations in which it should be conducted; official capacities, positions, that is, persons who should undergo security checks; purposes of conducting security checks; the procedure of conducting a security check; deadlines for conducting security checks; consequences of conducted security checks; the manner of and the deadlines for retrieving results of conducted security checks as well as other issues that must be defined by representatives of competent Ministries, that is, state bodies.

THE COMMISSIONER

Rodoljub Šabić

## ANNEX II: Transcripts of speeches by state institution representatives at the CEAS closing conference "Let's take part in the global debate about the balance between security and privacy"

The conference at which this document was presented as the final version of the Action Plan of Public Advocacy of 14 Points identified by the Ombudsman and the Commissioner for Information of Public Importance and Persona Data Protection was held on March 31, 2014. Apart from CEAS team members, the presenters at the conference included Saša Janković, the Ombudsman, Aleksandar Resanović, the deputy Commissioner for Information of Public Importance and Personal Data Protection, and Sanja Dašić of the National Security Authority of the Republic of Serbia, representatives of institutions as well as Dragiša Jovanović, an independent CEAS security expert.

The transcripts of presentations held by representatives of institutions are hereby attached.

### Saša Janković, Ombudsman

I am glad to be here with you today. I would like to comment on a couple of things that we have heard today. First, I would suggest we gently dump this false issue, of false dilemma that is - on setting of a balance between *security* and *human* rights, from the discourse. There is no security where human rights are not respected, nor are there any human rights in the absence of citizen security. Security and human rights are not inverses of each other, strengthening one does not come at the cost of the other, but conversely – by strengthening security human rights are fully realized, while human rights guarantees reduce risk (objectively and subjectively interpreted) for the values to which citizens have the highest regard, and hence there is greater security. An analysis of the terms "security" and "human rights" easily demonstrates this. Reducing security to threats to physical existence is unacceptable and dangerous oversimplification. The dilemma which, however, I truly consider as legitimate is the search for a balance between *efficiency* and *control*. Will we allow services to do as quickly as possible due to efficiency and then control only subsequently, or will we establish a mechanism of control in parallel with activities of the service, because today this is technologically possible – that is, in real time, and there are no fears that application of control mechanisms could slow down the operation of the service. I believe that the dilemma between efficiency and control could be overcome exactly thanks to today's information and communication technologies. Will the strengthening of the capacity and powers of services be followed by proportional strengthening of control or not? I think that this is logical, to say the least. Will we allow an indiscriminate access of services to privacy, in order to analyze the whole haystack and in it eventually find a needle (which seems to be position the U.S. intelligence and security apparatus) or will the services have to provide credible suspicion that a particular straw (in the haystack) is in fact a needle, in order to gain permission to analyze it (and with it inevitably all the straws in its immediate environment) is another important issue.

It was also mentioned that the previous Government was inefficient regarding security sector reform, but I have been the Ombudsman since 2008 and I do not see a significant difference regarding security sector reform in the past – all Governments to date had a reserved attitude towards democratization of the security sector and all of them, including this one in its technical term, have some tendency to keep this sector unreformed, and the operating mechanisms inferior. Perhaps one Government was more than another efficient in its aspirations to create a more repressive apparatus from the security system, with less elements of control.

We also heard the position of investors, that is, of the business sector, that the effect of *human rights* on the *market* should be assessed, but I consider this position twisted. I argue that we should assess the impact of the market on human rights and adjust the rules and behavior of the market to so that they enable a more complete realization of human rights, not the opposite.

Let us be clear, not everything falls under human rights, it is not a human right to drive a BMW just because someone else does in an advert. Human rights are the basic things that make up our life, the dignity of our life and the future of the human society. Whether a man will be free in 50 years depends on whether human rights are respected or not, while whether he drives a Trabant or a BMW depends on respect of market rules and success in the market.

Two years have passed since the Commissioner for Information of Public Importance and Personal Data Protection and I suggested 14 measures for improving the situation with regard to respect for human rights guarantees in procedures of the security sector. However, I must say that some of these measures date back even earlier. For example, I submitted the request to have the Law on BIA (Security Intelligence Agency) aligned with the constitution already in 2010, and in another capacity, not as the Ombudsman, I pointed out to its inconsistency with the Constitution already in 2006. Provisions of this law on the use of special measures are unconstitutional due to the reasons made current by the Šarić case – the law practically fails to state what are the measures that BIA can take in case legally prescribed requirements are met, and therefore it is formally unknown what are the ways in which the Agency resorts to in stirring into human rights from the aspect of privacy. Such measures must be prescribed by law, and the law specific in order to make the behavior of the services predictable. When the First Deputy Prime Minister publicly stated what measures BIA applied in the Šarić case, for me, as an institution protecting human rights, those do not pose as a problem, on the contrary, such measures should be written into law. But they are not. They are prescribed by bylaws that carry a label of confidentiality, thus they are secret.

Finally, one of the publicly mentioned measures is a *secret search*. This measure is not undertaken for the immediate apprehension of the offender; its purpose is something else – entrance into a space when there is nobody there, in order to search for incriminating evidence or any information. The search is carried out in a manner which leaves no evidence or doubt that anyone was in the space, without a court warrant and witnesses. However, following adoption of the 2006 Constitution, entry into a flat for the purpose of searching it is made possible only with a court warrant and in the presence of two witnesses. However still, it was recently publicly stated that secret searches are still being

conducted. This means that it is possible to have BIA Officers without anyone's knowledge, secretly enter and exit flats and that after that it can happen that in the course of a subsequent search, this time in line with the Constitution – therefore with a court warrant and impartial witnesses, incriminating material be found in a specific space, and that no one, not even the Court, knows that the secret service was present in that space previously. This is a great threat to the integrity of the evidence and objectivity of the court proceedings and that threat must be eliminated.

I will mention one more thing – an MP was arrested without having the National Assembly of the Republic of Serbia previously removing his immunity. Immunity is not given for personal commodity, but to ensure the smooth execution of the most important state functions and to prevent anyone from abusing authority to disable the carriers of these functions to perform their duties impartially and free. Imagine that on the day of the vote of no confidence in the Government, the freedom of movement of three opposition MPs is temporarily restricted for alleged traffic violation - which is possible in practice.

A provision of the Constitution states – a person with immunity cannot be detained until the National Assembly calls it off. An unofficial explanation which I heard is that the this "detention" should be interpreted as "the determination of custody measures", rather than deprivation of freedom of movement. So someone thinks that the constitutionally guaranteed immunity prevents a judge (as the judge determines custody) from restricting the freedom of an immunity holder, and that at the same time this is allowed to the Prosecutor in cooperation with a Police Officer! Does this mean that we are becoming a police state?

At the end - whistleblower. A law that says that a suit for protection of whistleblowers cannot protect the whistleblower from an act of the employer presiding on the rights and obligations arising from labor, is not a law that protects whistleblowers, but a pamphlet . What is the point of a law on whistleblowers that cannot protect the whistleblower against retaliation in the form of dismissal, transfer to a lower position, assignment to a remote place... whistleblowers need protection from this, not from looks under the eye. If the "political will" is not to protect whistleblowers from that which makes 100% of known cases that involved retaliation, then we should not waste time writing laws. At the same time the public is presented with an image that whistleblowers are protected and that they should trust the system. People believe in these calls, citizens come seeking protection, investigation... complaints from the Police, the Armed Forces, the secret services are numerous. The Ombudsman, however, or any other body, is not really in a position to provide protection to these people. I cannot, as a conscientious person, ask them for materials on whistleblowing, because I know that their job is at risk, and if they are telling the truth I do not have a mechanism to protect them, nor can I refer them to someone who can. The last example comes from a university - apparently it is about corruption worth million, in which, after documented reporting, a man, without any explanation, is dismissed from the university. And I have to tell him not to give me the documents, because if I start the process of control, I will not be able to protect him with certainty. Unless he believes me, or unless he is exceptionally brave, he will think that I, as the Ombudsman, turn a blind eye and keep my eyes closed at the lawlessness and violation of his rights and the public interest, that I am part of the defected system...

In any case, without the adoption of at least the majority of the mentioned 14 measures, we will not go far.

On the other hand, the grey image of the Ombudsman's 2013 Annual Report can be changed quickly, Serbia can do that. We do not need training; people who misbehave know that they are misbehaving. It is the intention to do harm, not ignorance. The intention due to the knowledge that the evil done too often has good consequences for the person who makes it, and bad for those who oppose. Most people are not in a position to refuse unlawful orders from superiors, as is required by law, if they know that by doing so they are sacrificing their career, economic status, family, survival. No system can be based on heroism.

Therefore, there is knowledge in Serbia, great solutions can be reached. The question is only whether the new Government will want to put this capacity to work, or will we continue to gather like this, saying things that the wind will blow away.

## Aleksandar Resanović, Deputy Commissioner for Information of Public Importance and Personal Data Protection

*Regarding the compilation of lists of those unsuitable and call for lynching of the Women in Black*

I would agree with what Mr. Janković said and add that this is not the first time that the so-called lists of those unsuitable are compiled. Namely, in the past, so-called black lists of those unsuitable and disobedient were compiled, based on political, national, religious and/or ideological grounds. Therefore, these lists are a call for lynching of the individuals whose names are on the list, but are also a kind of warning, or rather a threat, to all of those who think the same as the people on the list.

There is no doubt the compilation of any kind of lists of those unsuitable should belong to the past times. The compilation of such lists belongs inherently to authoritarian regimes, as was the regime in Serbia at the end of the twentieth century, or rather its predecessor, the totalitarian communist regime. The compilation of such lists should not, under any circumstances, be inherent in a system which calls itself democratic.

This is a global view of the disrespect of human rights, while from the aspect of jurisdiction of the Commissioner for Information of Public Importance and Personal Data Protection I could highlight specific irregularities. Namely, the Law on Personal Data Protection regulates the processing of personal data if there is an adequate basis for it within the law, not within bylaws, and if the persons whose data is being processed gave their consent. Having in mind that in this case there are neither of the these two mentioned requirements, hence the act of processing, that is, drafting lists of subjects with personal names and several other pieces of information which make these persons identified or at least identifiable, is not permitted.

*Moving on to the topic of today's program*

I will reflect some of the statements mentioned in the CEAS analysis and at this event. Allow me to first go a step back and highlight what led to the 14 measures. Namely, the Commissioner carried out a monitoring of implementation of the Law on Personal Data Protection by all mobile and landline telephone operators in Serbia – Telekom, Telenor, VIP and Orion, in the period March-July 2012. The subject of monitoring was the treatment of retained data only, not including the contents of communications, for a period of one year before the time of monitoring. It is fact that by analyzing and cross-checking of retained data, especially over a longer time period, which can last between 6 and 12 months, more information can be obtained than from the content of communication itself. We primarily wanted to see whether provisions of our Constitutions are being complied with; whether at the same time the generally accepted provisions of international law are being respected, which our Constitution prescribes to; whether there are any deviations from these and to what extent; whether there is a need for an adequate reaction of the Commissioner, etc.

The results of this monitoring surprised us. Firstly, all 4 operators received little more than 4,000 requests for access to retained data, which at first we thought was very little. The next thing we noticed, and which explains why there is so few requests, was that independent access to retained data was applied simultaneously, meaning that security services are able to access retained data independently, without submitting a request. We were surprised that around 90 percent of such requests were approved, and were additionally surprised that, in a large number of cases, a legal basis on which access to retained data is being requested, was not stated. Nevertheless, the providers usually met all requests.

Furthermore, one provider informed the Commissioner that little more than 270,000 independent requests to retained data has been recorded for a period of one year. It is fact that providers have no legal obligation of recording such access, but the fact that only one operator recorded this many independent accesses point to the conclusion that other operators probably had a similar amount of independent accesses. Based on this we can conclude that overall (taking into account all 4 providers in Serbia) we have several hundred thousands, maybe even a million, independent accesses to retained data on actual communications of citizens. If we compare this data to the 4,000 accesses achieved on the basis of submitted requests, we can see a great disproportion which points out that independent access to this data is a rule, and the submitting a request is the exception. It is therefore not surprising that out of these 4,000 requests, only two came from BIA (Security Intelligence Agency) and four from VOA (Military Security Agency).

When we analyze the number of 270,000 independent accesses to retained data with one operator, we should ask ourselves whether all of this was in compliance with the Constitution, that is, for the purposes of criminal proceedings and state security of Serbia, or was it perhaps abuse of independent access to retained data for private, commercial, political or any other purpose.

Such suspicions of possible abuse would be eliminated through the implementation of these 14 measures of the Commissioner and Ombudsman.

The Commissioner was often, after publishing those 14 measures, asked why he failed to act on the measures within his jurisdiction, that is, why hasn't he for example ordered the

removal of irregularities within a specific timeframe, or temporarily banned such processing of data, or ordered deletion of data gathered without legal basis. The reason is that the results of monitoring have shown that these problems are of systematic character, whose solution calls for implementing the same, systemic measures, and these are significant amendments of existing laws (especially Law on Criminal Procedure), adopting several new laws, uniting the current parallel technical abilities of security services and the Police into one, national agency for providing technical services for accessing retained data, uniting procedures towards the providers of electronic communications, etc. Therefore, it is about systemic measures that can and must be adopted by the state.

The decisions of the Constitutional Court on the Law on Electronic Communications and the Law on VBA and VOA (Military Security and Military Intelligence Agency) were already discussed today. The Constitutional Court decided that certain provisions of these laws are inconsistent with the Constitution of Serbia, because someone else, and not exclusively the Court, could decide on departing from the inviolability of secrecy of letters and other means of communications.

The generally accepted rules of international law, and especially the practice of the European Court for Human Rights in Strasbourg, as well as the current practice of the Constitutional Court, indicate to us that retained data presents an integral element of communication, that is, that unlawful access to retained data equates with unlawful access to the very contents of actual communication.

The Constitutional Court remained silent nearly 2 years on the recommendations of the Commissioner and Ombudsman to review the constitutionality of the Law on Criminal Procedure, which compared to the period of 10 years it took to assess the constitutionality of the Law on BIA (Security Intelligence Agency) is not such a long period.

Now we have before us two main courses of action while we wait the Constitutional Court's decision on the constitutionality of provisions of the Law on Criminal Proceedings, even though based on the current practice of this Court these are clearly unconstitutional provisions – first, to explore the technological potentials, modern IT and other solutions that enable effective operation of security services and the Police, and have the subject area regulated by law in compliance with realistic needs and the Constitutions; and second, not to do anything until the Constitutional Court reaches a decision, and then we will see where we go. This second approach certainly does not contribute to effective operation of security services and the Police, nor the respect for human rights, especially the right to privacy.

And just briefly I will reflect on the need for adopting a Law on Security Vetting, having in mind that the Commissioner initiated the adoption of this law. The reason for this initiative is that the subject matter is scattered across several regulations, especially in the sphere of education and employment in the Police, Armed Forces and security services. We believe that with a specific law, in a unified and comprehensive manner, should regulate the process of security vetting, and especially the following issues: definition of basic concepts, primarily security vetting and security threats; the types of security vetting being conducted; what data is checked, who does this and in what situations; the functions, positions, that is, persons that are subject to security vetting; the purpose of security vetting; the procedure of security vetting; deadlines for carrying out security vetting;

consequences of performed security vetting; the manner and timeframe for storing the results of completed security vetting, as well as other issues that need to be defined by representatives of the relevant ministries and authorities.

Unfortunately, a lot of time has gone by since the Commissioner's initiative, and on it, as far as I know, nothing has been done. I hope that the new Government will take appropriate measures in this regard, and perhaps the new CEAS project announced today could contribute to this end.

## Sanja Dašić, representative of the Office of the Council on National Security and Classified Information Protection (National Security Authority of the Republic of Serbia)

*Comments and suggestions regarding the "Action plan on 14 points"*

Regarding the CEAS Draft Action Plan of advocating for the adoption of the 14 measures of the Ombudsman and Commissioner within the project "Promotion of comprehensive security sector reform", the Office of the Council on National Security and Classified Information Protection (NSA), as a competent body within the field of classified information protection in the Republic of Serbia, according to its competences under the Law on Classified Information (Articles 86 and 87, paragraph 1, item 1 to 12 of the Act), has the mandate to comment solely on the issues within its jurisdiction, and in this specific case only on the part of the Action Plan that concerns the mentioned Law.

Bearing in mind that the 14 points/recommendations which the Ombudsman and Commissioner gave in July 2012 makes up an integral part of you Action Plan, within which Measure 11 recommends a "review of the results of the implementation of the Law on Classified Information (including the adoption of necessary bylaws, declassification of old document, conducting investigations, issuing security certificates…) and undertaking serious amendments of the Law or adopting a new one, we consider it expedient to suggest that this measure should be updated having in mind that the Law does not deal with declassification of old documents and conducting of investigations. Namely, this is a problem that relates to other special rules dealing with archives or court proceedings.

Furthermore, we highlight that in the past there have been some developments in the field of adoption of bylaws that regulate this issue more closely. The Regulation on detailed criteria for determining the level of classification of documents as "state secret" and "strictly confidential" entered into force, while adoption of the Regulation on detailed criteria for determining the level of classification of documents as "confidential" and "internal" for the majority of public authority bodies is in procedure, as well as the Law on the so-called Information Security , which should normatively round up the field of classified information protection at the national level. We also point out that the formation of a Working Group for amendments to the Law on Classified Information is underway, aiming to eliminate the identified shortcomings and legal gaps in the existing Law, as well as to create conditions for a more effective implementation of the Law itself.

We also believe that the term “confidential information” in Measure 12 of the Action Plan should be replaced with the term “secret data”, given that confidentiality determines the degree of secrecy, and not the type of data/information.

*On the NSA and its responsibilities*

The NSA is a professional service of the Government of the Republic of Serbia, which was formed on November 16, 2009. In accordance with the Law on the Security Services (“RS Official Gazette, No. 116/07), the NSA provides only technical and administrative support to the activities of the National Security Council and the Office for the Coordination of Security Services. One of its jurisdiction relates to the implementation and control of the implementation of the Law on Classified Information (“RS Official Gazette”, No.104/09), as well as the activities in accordance with the regulations of the civil service.

Regarding the implementation and control of implementation of the Law on Classified Information, the NSA implements *activities related to: the implementation of the Law and adoption of bylaws, international cooperation in the field of classified information exchange and protection, issuing certificates for access to classified information and training of civil servants in state administration and Government services.*

Otherwise, in accordance with signed and ratified international treaties the Office of the Council represents a *National Security Authority (NSA)* of the Republic of Serbia. Namely, our country established international cooperation in the field of exchange and protection of classified information concluding the *Agreement between the Government of the Republic of Serbia and the North Atlantic Treaty Organization (NATO) on information security and the Code of Conduct* ("Official Gazette of RS - International Treaties" 6/11) and concluding the *Agreement between the Republic of Serbia and the European Union on security procedures for exchanging and protecting classified information* ("Official Gazette of RS - International treaties", No. 1/2012).

For the needs of implementation of these agreements the Central Registry for Foreign Classified Information has been established within the Office of the Council, as well as sub-registers within the Ministry of Foreign Affairs, Mission of the Republic of Serbia to NATO and Mission of the Republic of Serbia to the European Union in Brussels, Ministry of Interior, Ministry of Defense and the Security Intelligence Agency. The exchange of classified information with NATO and the EU, commenced after the formation of the Central Registry and the mentioned sub-registers, as well as a completed certification visit of an expert teams from NATO and the European Union.

In addition, further seven agreements on exchange and protection of classified information have been signed with *Slovakia, Bulgaria, the Czech Republic, Slovenia, Bosnia and Herzegovina, Macedonia and Spain*, while initiated activities with other specific countries in this field are currently in various phases of realization.

## ABOUT THE CENTRE FOR EURO-ATLANTIC STUDIES (CEAS)

### History and Values

The Center for Euro-Atlantic Studies (CEAS) is an independent, atheist, socio-liberal*, policy research think tank, driven by ideology and values. It was established in 2007 by a small group of like-minded colleagues who shared an awareness of the inter-conditionality between global and regional trends, foreign policy orientation of the country, security and defense sector reform, and transitional justice in Serbia. With these linkages in mind, CEAS was established with the following mission:

- To accelerate the process of Serbian EU integration and to strengthen its capacities to confront global challenges through collective international action, resulting in full and active membership of the EU;
- To strengthen the cooperation with NATO and advocate for full and active Serbian membership in the Alliance;
- To promote regional cooperation and raise public awareness of its significance;
- To impose a robust architecture of democratic oversight of the security system;
- To support the development of transitional justice mechanisms, their enforcement in Serbia and the Western Balkans, and the exchange of positive experiences; to emphasize the importance of mechanisms of transitional justice for successful security sector reform in post-conflict societies in transition towards democracy.

To accomplish its mission, CEAS is targeting Serbian policy makers and the Serbian general public, as well as international organizations, governments and other actors dealing with Serbia and the region of Western Balkans, or dealing with the issues that CEAS covers through the promotion and advocacy of innovative, applicable and practical policies aimed at:

- Keeping up with the trends and developments in socio-liberal studies and practice, and strengthening socio-liberal democracy in Serbia;
- Adopting the principle of precedence of individual over collective rights without disregard for the rights which individuals can only achieve through collective action;
- Strengthening the secular state principle and promoting an atheistic understanding of the world;
- Contributing to the erection and preservation of a more open, safe, prosperous and cooperative international order, founded on the principles of smart globalization and equitable sustainable development.

With its high quality research and devoted work, CEAS generates accurate and recognized analyses primarily in the fields of foreign, security, and defense policies with recommendations based on its core values, with specific focus on:

- Acceleration of the processes of Serbian EU integration and strengthening of its capacities for confronting global challenges through collective international action, resulting in full and active Serbian membership of the EU;
- Strengthening cooperation with NATO and advocacy for full and active Serbian membership in the Alliance;
- Promotion of the significance of regional cooperation;

- Imposition of the robust architecture of democratic oversight of the security system;
- Supporting development of transitional justice mechanisms, their enforcement in Serbia and the Western Balkans, and the exchange of positive experiences; emphasizing the importance of mechanisms of transitional justice for successful security sector reform in post-conflict societies in transition towards democracy;
- Promotion of humanitarian and security norm Responsibility to Protect arguing that the state carries the primary responsibility for the protection of populations from genocide, war crimes, crimes against humanity, and ethnic cleansing. Recognizing that the international community has a responsibility to assist states in fulfilling this responsibility and that the international community should use appropriate diplomatic, humanitarian, and other peaceful means to protect populations from these crimes if a state fails to protect its populations or is in fact the perpetrator of crimes;
- Promotion of Open Government Policy aiming to secure concrete commitments from governments to promote transparency, empower citizens, fight corruption, and harness new technologies to strengthen governance.

**Programs and Donors**

CEAS is carrying out its mission through various projects within its five permanent programs:

I Comprehensive monitoring of contemporary international relations and foreign policy of Serbia
II Advocacy for full-fledged active membership of Serbia in the EU and NATO
III Advocacy for comprehensive Security Sector Reform in Serbia
IV Advocacy for development of the discourse of Energy Security in Serbia
V Liberalism, Human Rights, Responsibility to Protect, Transitional Justice, and Open governance in the Globalized World

CEAS programs have so far been supported by the European Commission Directorate General for Enlargement, the European Commission through Europe for Citizens, Balkan Trust for Democracy, the Friedrich Naumann Foundation, Fund for an Open Society-Serbia, the National Endowment for Democracy, NATO Public Diplomacy Division, the Rockefeller Brothers Fund, and the Royal Norwegian Embassy in Belgrade.

The above listed donors have thus far supported the following CEAS projects:

- Balkan Trust for Democracy: How the EU Can Best Employ its Leverage to Compel Sustainable Reform; Responses to local, regional and global security threats.
- European Commission: Advocacy for Open Government: Civil society agenda setting and monitoring of action plans (European Commission Directorate General for Enlargement), Enlargement and Citizenship: Looking into the future (Europe for Citizens program).
- Friedrich Naumann Foundation: Support for Serbian EU integration – Lobbying for the Stabilization and Association Process agreement.
- Fund for an Open Society: Serbia and the EU: What do we have in common in the areas of security and defense and how to make the most of it – continued advocacy

of security sector reform in Serbia through intensive use of Serbia's EU accession process resources; End oblivion - Legal and media support to families of civilians and soldiers killed under mysterious circumstances.

- National Endowment for Democracy: Now is the Time: Advocacy of the Continuation of the Comprehensive Security Sector Reform in Serbia; Promoting Comprehensive Security Sector Reform; Erection of NGO and expert groups focused on the process of EU integration in Bosnia and Herzegovina and Serbia; Strengthening debate skills and promoting democratic values among youth.
- NATO Public Diplomacy Division: 30 Young Experts on NATO; Conference: "Let's talk about NATO"; NATO, Serbia and the Western Balkans – Conference on NATO's new Strategic Concept.
- Rockefeller Brothers Fund: Serbian Security Sector Reform and Integration
- Royal Norwegian Embassy in Belgrade: Regulated Private Security Sector – Safer life of citizens.

**Membership of International Organizations**

CEAS has also developed its membership in several international coalitions and organizations:

- The International Coalition for the Responsibility to Protect – ICRtoP. The coalition brings together non-governmental organizations from all over the world to collectively strengthen normative consensus for the doctrine of Responsibility to Protect (RtoP), with the aim of better understanding the norm, pushing for strengthened capacities of the international community to prevent and halt genocide, war crimes, ethnic cleansing and crimes against humanity and mobilize the non-governmental sector to push for action to save lives in RtoP country-specific situations. CEAS is the first civil society organization from the region of South-Eastern Europe to have full membership in this coalition.
- The Policy Association for an Open Society – PASOS, an international association of think-tanks from Europe and Central Asia which supports the erection and functioning of an open society, especially in relation to issues of political and economic transition, democratization and human rights, opening up of the economy and good public governance, sustainable development, and international cooperation. CEAS is an associate member.
- The REKOM coalition which suggests that governments (or states) establish REKOM, an independent, inter-state Regional Commission for the Establishment of Facts on all the victims of war crimes and other heavy human rights violations undertaken on the territory of the former SFRY in the period 1991-2001.
- The Atlantic Community, the first online foreign policy think tank, which is primarily focused on issues affecting transatlantic relations with numerous special features, sections, and events that promote debate and cooperative solutions to transatlantic issues and provide members with access to policy makers.