Short Thematic Report

National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

Legal update

Country: Croatia

Version of 11 July 2016

Author: Gordan Bosanac MA

Reviewer: Dr Ivana Radačić

1.1 Summary

1. The legislative reform(s) that took place or are taking place and highlight the key aspect(s) of the reform;
2. the important (higher) court decisions in the area of surveillance;
3. the reports and inquiry by oversight bodies (parliamentary committees, specialised expert bodies and data protection authorities) in relation to the Snowden revelations;
4. the work of specific ad hoc parliamentary or non-parliamentary commission (for example the NSA inquiry of the German Parliament) discussing the Snowden revelations and/or the reform of the surveillance focusing on surveillance by intelligence services should be referred to.

In the period from September 2014 to May 2016 there were no legislative reforms related to the intelligence services or surveillance measures in Croatia. However, the Croatian Government has adopted two national strategies relevant for the work of the security and intelligence agencies: National Strategy for Preventing and Combating Terrorism (*Nacionalna strategija za prevenciju i suzbijanje terorizma*)[1], and the National Strategy for Cybernetic Security (*Nacionalna strategija kibernetičke sigurnosti*)[2]. The Strategies do not call for legislative reforms, apart from minor changes to the Data Protection Act not related to the surveillance measures. In addition, the Government has recently adopted an Annual Plan for Regulatory Activities for 2016 (*Godišnji plan normativnih aktivnosti za 2016. godinu*)[3] – where all national laws that are planned to be changed or adopted in 2016 are listed. There are no plans for changing legislation related to surveillance.

On 30 March, 2016, the Zagreb County Court delivered an important decision regarding the indictment against City of Zagreb Mayor Mr. Milan Bandić[4]. The Court has dismissed the evidence collected through surveillance measures (phone tapping and SMS messages conducted by special police unit responsible for combating corruption PNUSKOK), on the basis that the State Attorney's Office for Combating Corruption and Organized Crime (USKOK) (*Državno odvjetništvo – Ured za suzbijanje korupcije i kriminala*) did not present sufficient reasons for activation of the surveillance measures, which the Court (the same one, different chamber) nevertheless authorised.

This was the first court decision which challenges the argumentation of USKOK for authorisation of surveillance measures. In its decision, Zagreb County Court referred to the European Court of Human Rights (ECtHR) judgment in the case of *Dragojević vs. Croatia*[5]. In that case, ECtHR noticed the failure of the investigative judge to comply with the procedures envisaged by the law, in particular those related to an effective assessment as to whether the use of secret surveillance was necessary and justified in that particular case. It stated: *In this case the four secret surveillance orders issued by the investigative judge of the Zagreb County Court with respect to the applicant were essentially based only on a statement referring to the existence of the USKOK request for the use of secret surveillance and the statutory phrase that "the investigation could not be conducted by any other means or that it would be extremely difficult". No actual details were provided based on the specific facts of the case and particular circumstances indicating a probable cause to believe that the offences had been committed and that the investigation could not be conducted by other, less intrusive, means….It follows from the foregoing that whereas the*

[1]Croatia, Croatian Government (Vlada Republike Hrvatske), National Strategy for Prevention and Combat Terrorism (Nacionalna strategija za prevenciju i suzbijanje terorizma), 7th October 2015.
[2]Croatia, Croatian Government (Vlada Republike Hrvatske), National Strategy for Cybernetic Security (Nacionalna strategija kibernetičke sigurnosti), 7th October 2015.
[3] Croatia, Croatian Government (Vlada Republike Hrvatske), Annual plan for regulatory activities for 2016 (*Godišnji plan normativnih aktivnosti za 2016. godinu*), 17th session, 28th April 2016.
[4] Račić-Knežević, A. (2016), "*Fall of great affair Agram: Milan Bandić and his closest associates illegally followed and bugged? (Pada velika afera Agram: Milana Bandića i njegovi bliske suradnike nezakonito su pratilii i prisluškivali?)*, Net.hr, 30 March 2016.
[5]European Court of Human Rights (ECtHR), *Dragojević vs. Croatia*, No. 68955/11, 15 January 2015.

Code of Criminal Procedure expressly envisaged prior judicial scrutiny and detailed reasons when authorising secret surveillance orders, in order for such measures to be put in place, the national courts introduced the possibility of retrospective justification of their use, even where the statutory requirement of prior judicial scrutiny and detailed reasons in the authorisation was not complied with.[6]

ECtHR concluded that there had therefore been a violation of Article 8 (right to privacy) of the European Convention for Human Rights. Although this judgment was delivered in relation to the surveillance measures implemented by the special police unit PNUSKOK in a drug-related case, it can also be applied to overall approvals of secret surveillance measures by the Croatian courts.

On 14 June 2015, the Security and Intelligence Agency (*Sigurnosno-obavještajna agencija* – the rein after SOA) published the second public report on its activities[7]. This was the second report of SOA, hence we can observe the continuity of reporting. The report was again presented at a separate meeting to civil society organizations. The report has similar structure as the previous one. It is divided in the following sections: 1. About SOA – general information, 2. State of security in Croatia, 3. State of security in the geographical neighbourhood, 4. Statistical data on SOA work (number of security clearances conducted, number of intelligence analysis, SOA management (overall yearly budget, financial ratio of human resources vs. development and modernization expenses, gender structure of employees - ratio of man and women) and 5. Oversight over SOA. The report is written in very general manner without substantial information due to the legal limitation of information which SOA could disclose to the public. For example, the chapter on oversight describes already known institutional model of SOA oversight (internal oversight, parliament, courts, and expert bodies). It further states that in 2014 SOA received 29 different oversight requests from different oversight bodies and that nine disciplinary actions were initiated against SOA employees due to the breach of SOA regulations but no further details are provided[8]. As the new SOA director was appointed in May 2016, it is to be seen if the new SOA administration will keep publishing these reports in the future.

There have not been any public reports or inquiries by oversight bodies (parliamentary committees, specialised expert bodies and data protection authorities) or specific ad hoc parliamentary or non-parliamentary commissions in relation to the Snowden revelations. In the Ombudsperson's Yearly Reports for 2014[9] and 2015[10] there are no information related to the Snowden revelations. There is also no information in the Yearly Report on the Right to Access Information for 2014[11] and 2015[12] written by the Information Commissioner.

The only public activity related to the Snowden revelations was a public screening of the movie "Citizen Four" and a public discussion organized by the Centre for Peace Studies – NGO from Zagreb[13].

---

[6] Ibid., Par. 95-97.

[7] Croatia, Security and Intelligence Agency (Sigurnosno-obavještajna agencija), Public report 2015 (Javno izvješće 2015.), 14th June 2015.

[8] Ibid., pp. 38-39.

[9] Croatia, Ombudsperson Office (Ured pučke pravobraniteljice), Ombudsperson Yearly Report for 2014 (Izvješće pučke pravobraniteljice za 2014. godinu), March 31 2015.

[10] Croatia, Ombudsperson Office (Ured pučke pravobraniteljice), Ombudsperson Yearly Report for 2015 (Izvješće pučke pravobraniteljice za 2015. godinu), March 31 2016.

[11] Croatia, Information Commissioner (Povjerenica za informiranje), Yearly Report on the Implementation of Right to Accesses Information Act for 2014 (Izvješće o provedbi Zakona o pravu na pristup informacijama za 2014. godinu), March 2015.

[12] Croatia, Information Commissioner (Povjerenica za informiranje), Yearly Report on the Implementation of Right to Accesses Information Act for 2015 (Izvješće o provedbi Zakona o pravu na pristup informacijama za 2015. godinu) March 2016.

[13] Croatia, Centre for Peace Studies (Centar za mirovne studije) , Yearly report for 2015 (*Godišnji izvještaj o radu za 2015. godinu*), (2016).

1.2 International intelligence services cooperation

1. It is assumed that in your Member State international cooperation between intelligence services takes place. Please describe the legal basis enabling such cooperation and any conditions that apply to it as prescribed by law. If the conditions are not regulated by a legislative act, please specify in what type of documents such cooperation is regulated (eg. internal guidance, ministerial directives etc.) and whether or not such documents are classified or publicly available.

From the last SOA *Public report 2015*[14] it is clear that international cooperation plays an important role in SOA work. In several places, the report emphasizes commitment to cooperation with foreign security and intelligence agencies due to the new global challenges which cannot be dealt with solely from a national perspective.[15] Detailed aspects of cooperation are not known to the public. In SOA *Public report 2015*[16] it is stated that SOA is cooperating with different EU and NATO bodies through different multilateral security intelligence platforms. Furthermore the report states that there is enhanced intelligence interest of third countries and the need for more intense international cooperation, and that SOA cooperates and exchange information on daily basis with international partners[17].

The legal basis for international cooperation of SOA is given in the Act on Security Intelligence System (*Zakon o sigurnosno-obavještajnom sustavu*- there in after ZSOS)[18]:

The relevant articles read:
Article 5
(1) The Council for Coordination of Security and Intelligence Agencies (…) is giving opinions on cooperation with the relevant services of other countries (…).

Article 59
(1) Security and Intelligence Agencies may, on the basis of international obligations, cooperate with foreign security, intelligence and other appropriate services for the exchange of information, equipment, conducting joint activities within their mandate and training of staff.
(2) The National Security Council shall approve the establishment and termination of cooperation with individual foreign agencies, on the basis of a proposal from the Director of security and intelligence agencies, and after obtaining the opinion of the Council for Coordination of Security and Intelligence Agencies.

Article 60
(1) Security and Intelligence Agencies may provide information on Croatian citizens to corresponding foreign agencies if they provide relevant information that such a person endangers the national security of the country seeking information or else endangers values protected by international law. Data cannot be provided if doing so would be contrary to the interests of the Republic of Croatia or if the protections of the interests of the individual in question are of greater importance.
(2) If security and intelligence agencies perform security clearance for relevant foreign agencies or international organizations for the purpose of employment in foreign state bodies or international organizations, the security clearance check will be made on the basis of submitted consent of the individual being checked.

[14] Croatia, Security and Intelligence Agency (Sigurnosno-obavještajna agencija), Public report 2015 (Javno izvješće 2015), 14th June 2015.
[15]Ibid., pp. 1, 5, 8, 24 and 36.
[16] Croatia, Security and Intelligence Agency (Sigurnosno-obavještajna agencija), Public report 2015 (Javno izvješće 2015), 14th June 2015.
[17] Ibid.
[18] Croatia, Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*), Official Gazette (Narodne novine) Nos. 79/06 and 105/06, 30 June 2006.

(3) The submitted data must be documented. In addition to the information provided to the foreign agency, the documentation must also include a written disclaimer that the information provided can only be used for the purposes for which they were provided, and that the Security and Intelligence Agency that provides the data reserves the right to seek feedback on how the submitted data were utilized.

Article 97
Security and intelligence agencies officials may be sent to work abroad in the framework of cooperation with foreign security or other appropriate agencies or on the basis of international agreements.

Article 60 refers to any citizen who is under surveillance of SOA. Even if, for example, a foreign agency asks the Croatian agency to conduct surveillance, SOA has to get court approval. The grey zone is if a foreign agency operates by itself, with consent of SOA. However, there is no article regulating the processing of data / information by the Croatian intelligence services which are collected by a foreign intelligence service.

The National Security Council (*Vijeće za nacionalnu sigurnost* - from here on VNS), as the strategic decision making body in the field of national security policies, approves or terminates any cooperation of Croatian intelligence agencies with individual foreign agencies. It is composed of the President of the Republic, the Prime Minister, member of the government appointed for national security (most often that is the Minister of Interior but in the last government that was the first vice president of the Defence Minister), the Minister of Interior, Minister of Foreign Affairs, Minister of Justice, advisor to the President for National Security, Chief of Croatian Armed Forces, Director of SOA, Director of Military Security and Intelligence Agency and the head of the Office of the National Security Council. International collaboration is initiated on the proposal of the Directors of the security and intelligence agencies (either civil or military agency).

The Council for Coordination of Security and Intelligence Agencies (*Vijeće za koordinaciju sigurnonosno-obavještajnih agencija* – the rein after VKSOA) also has to give its opinion regarding the cooperation. VKSOA is the body that coordinates the work of agencies and other bodies within the security and intelligence systems, based on the decision of the National Security Council. VKSOA is composed of a member of the Government appointed for national security, advisor to the President for national security, the head of the Office of the National Security Council and Directors of security and intelligence agencies. At its meetings, if necessary, another person from the judiciary, police, inspection, control and other bodies and institutions may take part.

2. Please describe whether and how the international cooperation agreements, the data exchanged between the services and any joint surveillance activities, are subject to oversight (executive control, parliament oversight and/or expert bodies) in your Member States.

According to Article 103 of the Act on Security and Intelligence System (*Zakon o sigurnosno-obavještajnom sustavu*)[19] (ZSOS), oversights of the work of intelligence agencies is conducted by: the Croatian Parliament through the Parliamentary Committee for Internal Affairs and National Security (*Saborski Odbor za unutarnju politiku i nacionalnu sigurnost*), the Council for Civic Oversight of the Intelligence Agencies (*Vijeće za građanski nadzor sigurnosno-obavještajnih agencija* – therein after VGNSOA) and the Office of the National Security Council (*Ured Vijeća za nacionalnu sigurnost* – therein after UVNS). Only the UVNS has explicit written legal power to conduct oversight of international cooperation between agencies. This is defined in Article 107 of ZSOS which states that UVNS *oversees coordination and collaborations between security and intelligence agencies and relevant services of other countries.*[20]

[19] Croatia, Act on the Security Intelligence System of the Republic of Croatia (Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske), Official Gazette (Narodne novine) Nos. 79/06 and 105/06, 30 June 2006.
[20] Ibid.

The Parliamentary Committee, apart from requesting reports from agencies on possible irregularities, also has the power to conduct direct oversight of agencies. Although the responsibilities of the Committee within the framework of international cooperation are not explicitly mentioned in ZSOS, there are no limitations in that respect. If the Parliamentary Committee notices irregularities related to international cooperation, it may initiate its oversight powers. However, there is one explicit restriction in Article 105(3) 3 which states that *information delivered to the Parliamentary Committee* (from domestic intelligence and security agencies) *cannot contain information received from foreign intelligence or security agencies except if the permission is obtained from the foreign agencies or if there is a VNS decision on that matter*[21].

VGNSOA has a mandate to monitor the legality of the work of the security agencies and to monitor and supervise the application of measures of secret data collection that restrict constitutional human rights and fundamental freedoms[22]. It may initiate investigation of the perceived unlawful actions or irregularities in the work of security and intelligence agencies that restrict constitutional human rights and fundamental freedoms only under the program adopted by the Parliamentary Committee for National Security, or at the request of a citizen, state bodies and legal persons[23]. It cannot initiate investigations *proprio motu*.

The biggest problem related to the oversight of possible international cooperation is the fact that neither the Parliamentary Committee, nor VGNSOA has the power to monitor the work of the Operative Technical Centre for Telecommunication Oversight (*Operativno-tehnički centar za nadzor telekomunikacija* - from here on OTC). OTC is the central independent institution which implements all interception measures and provides intercepted or wire-taped data to police, judicial, security and intelligence agencies. It is not known to the public if OTC transfer data directly to foreign intelligence services. The ZSOS does not explicitly give oversight powers over OTC to the Parliamentary Committee and VGNSOA. The OTC authorities, with Government support[24], interpret the ZSOS in a way that OTC is not under the control of Parliamentary bodies. This is particularly concerning given the massive data collection measures which are taking places exactly in institutions such as OTC.

Any surveillance measure which collects the content of exchanged information (such as taping a conversation between persons) needs to be approved by a judge. Even if a foreign agency requests the surveillance of information exchanges of a Croatian citizen, the national intelligence agency must get approval from a judge[25]. However, some surveillance measures such as listings of dialled numbers, or visited IP addresses can only be implemented with the approval of the intelligence agencies Directors.

Finally it is important to note that according to Article 33 of ZSOS, SOA may implement *secret surveillance of international telecommunication connections.*[26] However, the law doesn't define what constitutes an international telecommunication connection. This measure must be approved only by the SOA Director.

---

[21] Ibid, Art 105, para. 3.
[22] Ibid, Art 108 -114.
[23] Ibid, Art 108 -114.
[24] Croatia, Croatian Government (Vlada Republike Hrvatske) The proposal to provide credible interpretation of Articles 110, 111 and 112th of Security and Intelligence System Act (Prijedlog za davanje vjerodostojnog tumačenja članaka110., 111. i 112.Zakona o sigurnosno-obavještajnom sustavu), 15th session, 20th April 2016.
[25] This information was confirmed by a SOA representative. Any operation conducted by SOA, regardless if initiated by foreign or domestic actors has to be in line with Croatian laws could exempt SOA from court approval for surveillance measures required by the foreign agency; Croatia, Act on the Security Intelligence System of the Republic of Croatia (Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske), Official Gazette (Narodne novine) Nos. 79/06 and 105/06, Art. 36, 30 June 2006.
[26]Ibid., Art. 33(3)

1.3 Access to information and surveillance

1. **Does a complete exemption apply to surveillance measures in relation to access to information?**
2. **Do individuals have the right to access information on whether they are subject to surveillance?**

Article 40 of ZSOS states that the security-intelligence agencies are obliged, upon a citizen's request, to inform the citizen by written notice, and within 15 days, if he/she was the subject of secret data collection measures (including surveillance). However, paragraph 3 of the same article stipulates exemptions to this rule. The agencies are not obliged to inform the citizens about the measures of secret data collection if: 1. this information could endanger the execution of the tasks of the agencies, 2. the information could lead to endangering the safety of another person or 3. the information could have adverse consequences for the national security or national interests of the Republic of Croatia.

Moreover, according to Article15 of the Freedom of Information Act[27] (*Zakon o pravu na pristup informacijama* - from here on ZPPI), public authority bodies may restrict access to *information if the information has been classified by a degree of secrecy, pursuant to the act governing classified information or if access to information has been restricted pursuant to international treaties, or pertains to information arising in procedures of concluding or acceding to international agreements or negotiations with other countries or international organisations, until the completion of such proceeding, or pertains to information arising in the area of diplomatic relations.*

Having in mind that surveillance measures are classified information by definition, accessing information on whether a person is subject to surveillance is in general impossible. According to the Data Secrecy Act (Zakon o tajnosti podataka)[28], SOA has a possibility to classify information with one of four different categories: very secret, secret, confidential and limited. Any surveillance measure is defined within the Security and Intelligence System Act (Art. 33) as a secret measure of data collection. Since the measure is secret, it has to be classified as a very secret, secret, confidential or limited – depending on the target of surveillance.

Article 16 of ZPPI, as well as Article 16 of the Data Secrecy Act[29] (*Zakon o tajnosti podataka)* foresees the proportionality test and the public interest test to be conducted when citizens ask for classified information. The information holder, upon the previous acquired consent of the Office of the National Security Council, is obliged, prior to reaching a decision, to conduct the proportionality test and the public interest test. However, we are not aware of any case in the scope of surveillance activities to be declassified according to the proportionality or public interest test.

The lawfulness of Article 15 ZPPI is primary under the Information Commissioner responsibility. However, the Commissioner can only monitor if SOA and Office of the National Security Council has conducted proportionality test, but cannot go into the questioning the quality of proportionality test. VGNSOA – since it has in a mandate to monitor "lawfulness of the work of the security agencies" -could challenge SOA decisions related to classified information as a secret. In other words, they have a mandate to monitor how SOA is respecting Data Secrecy Act. However, they have never exercised this power.

Finally, citizens or any legal or state body may submit complaints to VGNSOA about unlawful procedures or misconduct of security and intelligence agencies, particularly in the case of violations of

[27]Croatia, Act on the Right of Accesses to Information (*Zakon o pravu na pristup informacijama*), Official Gazette (*Narodne novine*), Nos. 25/13, 85/15, 15th July 2015.
[28] Croatia, Data Secrecy Act (Zakon o tajnosti podataka), Official Gazette (Narodne novine), Nos. 79/07, 86/12, 7th August 2007.
[29]Croatia, Data Secrecy Act (Zakon o tajnosti podataka), Official Gazette (Narodne novine), Nos. 79/07, 86/12, 7th August 2007.

human rights and fundamental freedoms guaranteed by the Croatian constitution[30]. The VGNSOA may then initiate an investigation of possible violations or illegal treatment. To conclude, citizens cannot access information from VGNSOA about whether they are/were the subject of surveillance, but can only challenge misconducts in the work of the agencies related to them before VGSOA.

1.4 Update of FRA report

1. If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.

2. If you Member State is mentioned, please update the data (new legislation, new report etc.)

3. If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.

Table of Contents of the FRA Report

Introduction

1. **Intelligence services and surveillance laws**

1.1. Intelligence services

No additional comments.

1.2. Surveillance measures

In Croatia, the legislation recognizes only "targeted surveillance". However, although untargeted collection of big data (open source intelligence collection) is not explicitly mentioned in the legislation it is also not explicitly forbidden.

1.3. Member States' laws on surveillance

No additional comments

FRA key findings

2. Oversight of intelligence services

On p. 32 (end of the section 2. Oversight of intelligence services) FRA report could be updated with the information that Security and Intelligence Agency (SOA) (*Sigurnosno-obavještajna agencija*) has continued to publish report in 2015[31]. The report was published in June 2015.

2.1. Executive control

[30]Croatia, Act on the Security Intelligence System of the Republic of Croatia (Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske), Official Gazette (Narodne novine) Nos. 79/06 and 105/06, 30 June 2006
[31]Croatia, Public report 2015 (Javno izvješće 2015.), Security and Intelligence Agency (Sigurnosno-obavještajna agencija), 14th June 2015.

It is important to note that in Croatia executives don't have power to approve or disapprove surveillance measures. Those powers have directors of security and intelligence agencies and courts.

No need for amendment to the reference.

2.2. Parliamentary oversight

No additional comments.

2.2.1 Mandate

No additional comments.

2.2.2 Composition

No additional comments.

2.2.3 Access to information and documents

In Croatia, parliamentary oversight bodies have the right to access classified documents. The members of oversight bodies must have security clearance certificate. This is not needed for members of parliament which can accesses classified data without previous clearance.

2.2.4 Reporting to parliament

No additional comments.

2.3. Expert oversight

2.3.1. Specialised expert bodies

No additional comments.

2.3.2. Data protection authorities

No additional comments.

2.4. Approval and review of surveillance measures

No additional comments.

FRA key findings

No additional comments

3. Remedies

No additional comments

3.1. A precondition: obligation to inform and the right to access

No additional comments

3.2. Judicial remedies

No additional comments

3.2.1 Lack of specialisation and procedural obstacles

No additional comments

3.2.2 Specialised judges and quasi-judicial tribunals

No additional comments

3.3. Non-judicial remedies: independence, mandate and powers

No additional comments

3.3.1 Types of non-judicial bodies

No additional comments

3.3.2 The issue of independence

No additional comments

3.3.3 Powers and specialisation of non-judicial remedial bodies

No additional comments

FRA key findings

No additional comments

Conclusions

No additional comments

1.5 Check the accuracy of the figures and tables published in the FRA report (see the annex on Figures and Tables.

FRANET contractors are requested to check the accuracy of the Tables and Figures published in the FRA Report and reproduced in Annex 8.2 below. Please answer each questions under paragraphs 2.1 to 2.12.

1.5.1 Overview of security and intelligence services in the EU-28

FRANET contractors are requested to check the accuracy of the table below (see Annex p. 93 of the FRA Report) and add in track changes any missing information (incl. translation and abbreviation in the original language). Please provide the reference to the national legal framework when updating the table.

	Civil (internal)	Civil (external)	Civil (internal and external)	Military
HR			Security Intelligence Agency/Sigurnosno-obavještajna agencija (SOA)	Military Security Intelligence Agency/*Vojna sigurnosno-obavještajna agencija* (VSOA)

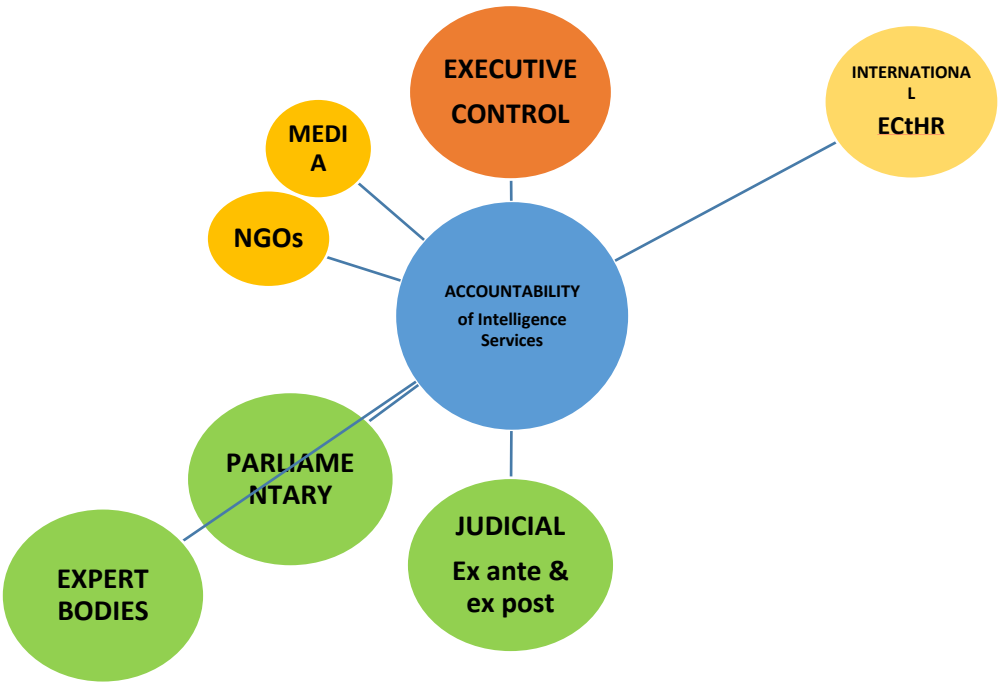
Explanation:

Security Intelligence Agency (SOA) is since 2006 working on both levels: internal and external (meaning inside and outside Croatia). There was mistake done in first report.

1.5.2 Figure 1: A conceptual model of signals intelligence

According to Croatian legislation there is no legal grounds for "mass surveillance" which would result with big data collection. In that sense it is impossible to comment Figure 1.

1.5.3 Figure 2: Intelligence services' accountability mechanisms

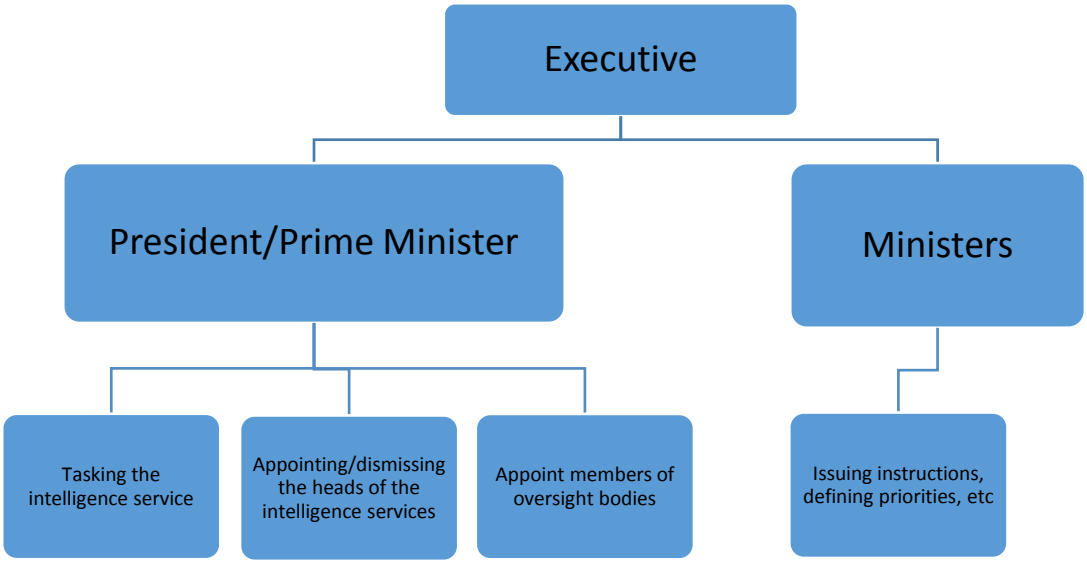


For Croatia, I have made a small change in the Figure 2, shifting "Expert bodies" closer (under) the parliamentary accountability mechanism. Croatian expert body, the Council for Civic Oversight of the

Intelligence Services (*Vijeće za građanski nadzor sigurnosno-obavještajnih agencija)* works under the Parliament Committee for Internal Affairs and National Security. This expert body reports primary to the Parliamentary Committee. It submits regular yearly report on their work. Members of the expert body are not allowed to make public statements without previous approval of the Parliamentary Committee.

I would also add another body – Ombudsperson (and locate this body between parliament and NGOs) who can also initiate investigations related to the human rights violations by services. It is also important to note that the Ombudsperson (including his/her deputies) doesn't need security clearance to accesses classified data in Croatia.

1.5.4 Figure 3: Forms of control over the intelligence services by the executive across the EU-28



Approval of surveillance measures is fully in the domain of the director of Security Intelligence Agency. It means, he/she doesn't need approval from the executives to implement surveillance measures.

1.5.5 Table 1: Categories of powers exercised by the parliamentary committees as established by law

The data for Croatia are correct.

Member States	Essential powers	Enhanced powers
HR	X	

1.5.6 Table 2: Expert bodies in charge of overseeing surveillance, EU-28

The data for Croatia are correct.

EU Member State	Expert Bodies

HR	The Office of the Council for National Security*(Ured Vijeća za nacionalnu sigurnost)* Council for Civic Oversight of Security and Intelligence Services (*Vijeće za građanski nadzor sigurnosno-obavještajnih agencija*)

1.5.7 Table 3: DPAs' powers over national intelligence services, EU-28

EU Member State	No powers	Same powers (as over other data controllers)	Limited powers
HR		X	

1.5.8 Figure 4: Specialised expert bodies and DPAs across the EU-28

No changes.

1.5.9 Table 4: Prior approval of targeted surveillance measures, EU-28

EU Member State	Judicial	Parliamentary	Executive	Expert bodies	None
HR	X				

No changes.

1.5.10 Table 5: Approval of signals intelligence in France, Germany, the Netherlands, Sweden and the United Kingdom

N/A

1.5.11 Figure 5: Remedial avenues at the national level

The Figure is correct.

1.5.12 Figure 6: Types of national oversight bodies with powers to hear individual complaints in the context of surveillance, by EU Member States

The Figure is correct.