TRANSPARENCY INTERNATIONAL GEORGIA

DCAF
a centre for security, development and the rule of law

ადამიანის უფლებების სწავლებისა და მონიტორინგის ცენტრი
EMC
Human Rights Education and Monitoring Center

OPEN SOCIETY GEORGIA FOUNDATION

INTERNATIONAL STANDARDS AND GOOD PRACTICES IN THE GOVERNANCE AND OVERSIGHT OF SECURITY SERVICES

TBILISI 2018

Nazli Yildirim Schierkolk

Disclaimer: The research and drafting of this report was supported with financial assistance by the Geneva Center for the Democratic Control of Armed Forces (DCAF). The analysis and assessments expressed in this report do not necessarily reflect the views of DCAF.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND AND OBJECTIVES OF THE PROJECT

In the framework of the Georgian Ministry of Internal Affairs' reform, the State Security Service was separated from the Ministry and was established as a distinct institution. The new Law on State Security Service of Georgia[1] regulates its mandate, powers and functions. The law provides the Service with a substantially broad mandate, which includes inter alia, fighting against transnational organized crime, and preventing, detecting and eliminating corruption. Furthermore, the State Security Service is granted law enforcement powers such as investigation, search, arrest and detention of suspects and perpetrators. Such a broad mandate and police powers, coupled with a lack of strong safeguards for the oversight of the Service has been a matter of concern for international and local actors, who called for the need to enhance democratic governance and oversight of the State Security Service.

In an effort to foster public debate on these matters, the Transparency International Georgia (TI Georgia) and the Human Rights Monitoring Center (EMC) have launched the project 'Advocacy for the Creation of the Modern System for the Security Sector' with financial support from the Open Society Foundation (OSF). The project aims to advocate for an accountable, human rights-oriented and a modern security service, carrying out its activities in compliance with international standards.

METHODOLOGY AND STRUCTURE OF THE REPORT

As a part of its advocacy effort, the Project aims to publish a report, which outlines international standards and best practices in the governance and oversight of security services. In this respect, the TI Georgia and the EMC jointly identified four key areas to be addressed in this report: (i) mandate and functions of security services; (ii) executive control of security services, (iii) oversight and accountability of security services; (iv) transparency of security services.

The report consists of four chapters, mirroring the key areas identified. Each chapter starts with an overview of international standards established by the most notable international and European bodies and actors such as the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; the Council of Europe European Commission for Democracy through Law (Venice Commission), the Council of Europe Commissioner for Human Rights, and the European Union Agency for Fundamental Rights (EU FRA).

In each chapter, international standards are followed by a brief overview of relevant practices in selected four countries. For the purposes of this report, the following countries were chosen, by taking into consideration Georgia's overall Euro-Atlantic integration perspective:

- Germany and Belgium as two European countries with advanced oversight and accountability mechanisms, which are often referred to as representing best practices;
- Croatia as a European country with a recent history of democratization which undertook substantial reforms of the security sector in the framework of its EU integration process;
- Canada as a non-European country, yet a member of NATO and OSCE, often referred to as embodying best practices in the governance and oversight of the security sector.

It should be noted that there is no country with a perfectly functioning security and intelligence governance and oversight system. Each country has its unique circumstances, struggling to counter multiple transnational threats in an ever-changing global security environment. The practices from the selected four countries are not meant to prescribe a 'solution' to challenges encountered in Georgia. They are intended to illustrate the different

1 Available from: https://matsne.gov.ge/ru/document/download/2905260/1/en/pdf

ways in which international standards are implemented in those countries, and provide a platform for Georgian stakeholders to discuss and reflect on the mechanisms that would work most effectively in the Georgian context.

A NOTE ON TERMINOLOGY

The EU Fundamental Rights Agency makes a basic conceptual distinction between intelligence and security services: intelligence services are agencies have a foreign mandate and focus on countering external threats, while security services tackle domestic threats.[2] International standards and practices outlined in this report cover predominantly security services, but makes references to intelligence services whenever necessary.

Security services

The term 'security services' is defined in this report as 'state bodies, including both autonomous agencies and departments/units of other government that have a mandate to collect, analyze and disseminate intelligence within the borders of their state in order to inform decisions by policy makers, police investigators and border/customs agencies about threats to national security and other core national interests.'[3]

Oversight

The term oversight is frequently used in this study, and it is therefore important that it is clearly defined from the outset. Oversight is a comprehensive term that refers to several processes including: ex-ante scrutiny, on-going monitoring, and ex-post review, as well as evaluation and investigation. Oversight of security services is undertaken by a number of external actors, including the judiciary, parliament, National Human Rights Institutions (NHRI) and ombuds institutions, National Preventive Mechanisms (NPM), audit institutions, specialised oversight bodies, media and NGOs. Oversight should be distinguished from control as the latter term implies the power to direct an organisation's policies and activities. As such, control is typically associated with the executive branch of government.[4]

2 European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Mapping Member States' legal frameworks, (hereinafter EU FRA, Surveillance by Intelligence Services)* (Luxembourg, 2015), p. 13, available from: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

3 Council of Europe (2015) Democratic and Effective Oversight of Security Services, p.18, available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770

4 Born and Geisler Mesevage, 'Introducing Intelligence Oversight' in Born and Wills (ed.) 'Overseeing Intelligence Services: A Toolkit' (DCAF, 2012) p.6.

CHAPTER 1- MANDATE AND FUNCTIONS OF SECURITY SERVICES

The way in which the institutional organization, mandate and functions of security services are defined has important implications upon the functioning of services and the protection of fundamental human rights and freedoms in democratic societies. This chapter provides an overview of key international standards on the aforementioned features, with a focus on organization; mandate and the definition of national security threats; the controversial question of granting the services law enforcement powers, and the surveillance function of security services.

1.1 ORGANIZATION OF SECURITY/INTELLIGENCE SERVICES

The overall institutional set-up of security & intelligence services is generally considered the prerogative of national states; decided upon identified threats and needs unique to each country. However, one pattern that is clearly observed is the distinction between civilian and military intelligence. As of 2017, all EU member states except Malta and Luxembourg have established at least two different services responsible for civilian and military intelligence respectively.[5] This report focuses on the civilian services.

There is a considerable degree of variance when it comes to how civilian services are organized. Some European countries have one civilian agency with both domestic security and foreign intelligence mandates. Danish, Dutch, Slovenian, and Portuguese security/intelligence services are an example of this approach. Other European countries chose to establish two separate services with distinct domestic security and foreign intelligence mandates, such as the Czech Republic, France, Italy, the UK, and to a certain degree, Germany.[6] Yet other countries, such as Austria and Finland established one civilian security service with only a domestic mandate.[7]

There is no single widely accepted standard at the international level, as to how civilian security and intelligence services should be organized. A single civilian service with both domestic security and foreign intelligence mandates inevitably results in too much consolidation of power in one institution. In the absence of a clear legislative framework and strong oversight mechanisms, there is a risk that methods used for foreign intelligence gathering (which is typically less strictly regulated) are applied in the context of domestic security mandate (which generally requires higher degrees of control). On the other hand, having two separate agencies with internal and external mandates may lead to potential turf battles since the line between internal and external threats are increasingly blurred, and coordination/cooperation problems between those agencies, as well as the fragmentation of oversight. [8]

Therefore, beyond the exact institutional set-up, the bottom-line is to have a comprehensive legal basis in line with international laws and standards covering all aspects of the work of security and intelligence agencies; as well as a strong accountability system, whereby the executive, the Parliament, the judiciary and independent bodies effectively carry out their respective oversight roles and duties.

Matters related to hierarchical set-up and subordination of security services are explained in Chapter 2 on Executive Control of Security Services.

---

5 EU FRA, Surveillance by Intelligence Services, (2015), p.13, also see the table in Annex of the same publication on p.94.

6 At the federal level, Germany has a distinct domestic security service (BfV). The federal intelligence service (BND), although most of its focus is on foreign intelligence, is categorized by the EU FRA as an agency with both an internal and external mandate. See EU FRA, Surveillance by Intelligence Services, (2015),, p.94

7 Ibid. In these countries, foreign intelligence is carried out by the military intelligence service.

8 Venice Commission, *Report on the Democratic Oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session* (2007), (hereinafter Venice Commission, *Democratic Oversight of the Security Services* (2007)) paras 94-97 available from: http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx

1.2. MANDATE OF SECURITY SERVICES

As per the 'UN Compilation Of Good Practices on Legal and Institutional Frameworks and Measures That Ensure Respect For Human Rights by Intelligence Agencies while Countering Terrorism' (hereinafter UN Compilation of Good Practices), the main purpose of security services is to '[*c]ollect, analyze and disseminate information* that assists policymakers and other public entities in taking measures to protect national security'[9] and that '[M]andates are strictly limited to *protecting legitimate national security interests* as outlined in publicly available legislation or national security policies, and identify the threats to national security that intelligence services are tasked to address'.[10]

In this respect, the way national security threats are defined has a significant impact on the scope of the security services' mandates. The definition of national security and identification of respective threats is undeniably a national process, which should take into account the unique geopolitical and security circumstances of the country. Hence, there cannot be a strictly uniform list of threats to national security at the international level. However, case law of the European Court of Human Rights as well as the Parliamentary Assembly of the Council of Europe (PACE) recommendations provide guidance as to what is, and is not, commonly regarded as a threat to national security.

Born and Leigh compiled the following list of activities that are commonly considered as threats to national security based on the ECtHR case law:

- Espionage (in Klass and others v. Federal Republic of Germany)[11]
- Terrorism (idem)
- Incitement to/approval of terrorism (in Zana v. Turkey)[12]
- Subversion of parliamentary democracy (Leander v. Sweden)[13]
- Separatist extremist organizations which threaten the unity or security of the State (United Communist Party of Turkey and Others v. Turkey)[14]

It should be noted that this list is not exhaustive, and other matters such as interference with electronic data relating to defense, foreign affairs or other matters affecting the vital interests of the State may also be considered as a threat to national security.[15]

The Parliamentary Assembly of the Council of Europe, in its landmark Recommendation 1402 (1999) on 'Control of internal security services in council of Europe member states' stated that '[E]conomic objectives, or the fight against organized crime per se, should not be extended to the internal security services. They should only deal with economic objectives or organized crime when they present a clear and present danger to national security'.[16]

This statement is open to interpretation as there is no objective measure of what types of economic/organized crime present clear danger to national security. By way of example, in a recent judgment, (*C.G and others v. Bulgaria)* the ECtHR ruled that 'drug trafficking' in the context of the case concerned, cannot be considered as a threat to national security. [17]

In line with those normative standards and case law, many states do not entrust their security services with a mandate to counter organized crime and other crimes with economic gains such as corruption. Amongst the advanced European democracies such as Germany and the UK, combatting organized crime and corruption falls

9 UN Compilation of Good Practices, Practice 1
10 Ibid, Practice 2
11 http://hudoc.echr.coe.int/eng?i=001-57510 para 48
12 http://hudoc.echr.coe.int/eng?i=001-58115, para 49-50
13 http://hudoc.echr.coe.int/eng?i=001-57519 para 59
14 http://hudoc.echr.coe.int/eng?i=001-58128 para 39-41
15 Council of Europe, Experts Report: European Committee on Crime Problems (CDPC), Group of Specialists on Internal Security Services (PC-S-SEC), Addendum IV, Final Activity Report, 40703, para. 3.2.
16 PACE Recommendation 1402, Guidelines A2, available from: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16689&lang=en
17 http://hudoc.echr.coe.int/eng?i=001-86093, paras 40-43

within the mandate of police or specific law enforcement units/agencies, and not the security services.

However, some states include 'protection of vital economic interests' in the definition of national security. If the 'vital economic interests' are not well defined in the law, there may be a risk of misuse of the mandate of security services. In this respect, the Venice Commission states that proliferation of weapons of mass destruction, circumvention of UN/EU sanctions, and major money laundering are three areas that could be legitimately included in the mandate. [18]

While the focus of this section was on mandates of security services in relation to national security threats, typically services are also mandated to carry out other tasks such as conducting security vetting, and protecting designated persons (high-level state officials) and critical infrastructure.

1.3. LAW ENFORCEMENT POWERS

As per the UN guidance referred to earlier, the core tasks of security services should be to 'collect, analyse and disseminate' information to protect national security. The implication is that when security services identify a threat to national security, they share the information they collected with state bodies who have the authority to ***act*** on this intelligence and ***enforce the law***, i.e. police and other law enforcement agencies. Thus an institutional separation between security services and law enforcement agencies is regarded as a strong safeguard against too much concentration of power in one service, and the risk of arbitrary use of intelligence collected through covert methods.[19]

In this respect, PACE Recommendation 1402 clearly stipulates that '[I]nternal security services should not be authorized to carry out law-enforcement tasks such as criminal investigations, arrests, or detention. Due to the high risk of abuse of these powers, and to avoid duplication of traditional police activities, such powers should be exclusive to other law-enforcement agencies'.[20] Similarly the UN Compilation of Good Practices acknowledges the strong arguments made against combining intelligence and law enforcement powers in one agency, taking into consideration the risk of developing a parallel enforcement system.[21]

In line with these international standards, most democratic states limit the mandate of their security services to collection, processing and dissemination of information; and do not entrust them with law enforcement powers.[22] For the exceptional cases where arrest and detention powers are granted to the security services, Practices 28-30 of the UN Compilation of Good Practices provides a set of important standards:

- **Practice 28**: 'The exercise of arrest and detention powers is restricted to cases in which there is reasonable suspicion that an individual has committed or is about to commit a specific criminal offence.' Furthermore, it is good practice to limit this power to specific threats to national security, such as terrorism, [23] and not the entire mandate of the services.
- **Practice 28**: 'Intelligence services are not permitted to deprive persons of their liberty simply for the purpose of intelligence collection.'
- **Practice 28:** 'The use of any powers and arrest and detention by intelligence services is subject to the same degree of oversight as applies to their use by law enforcement authorities, including judicial review of the lawfulness of any deprivation of liberty.'
- **Practice 29**: When exercising these powers, intelligence services comply with international standards set out in, inter alia, the Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment,

---

18 Venice Commission , *Report on the Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session,* CDL-AD (2015) 011, p.20 available from: http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)011-e,

19 European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU*- - Volume II: field perspectives and legal update (Luxembourg, 2017) (hereinafter EU FRA, Surveillance by Security Services, (2017) ,p.28 available from http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and/publications,

20 PACE Recommendation 1402, Guidelines B3

21 UN Compilation of Good Practices, Para 41

22 Except, for instance, in cases of close protection and safeguarding critical infrastructure, see Belgium case below.

23 UN Compilation of Good Practices, Para 41

the Code of Conduct for Law Enforcement Officials and the Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.

- **Practice 30**: 'Intelligence services are not permitted to operate their own detention facilities or to make use of any unacknowledged detention facilities operated by third parties.' This is an important safeguard against incommunicado detention, torture and other forms of ill-treatment.

1.4 SURVEILLANCE FUNCTION OF SECURITY SERVICES

As explained in the previous sections, security services carry out a number of functions within their mandate; including collection, analysis, dissemination of information; security vetting, counter-intelligence and protection of critical infrastructure. Among the functions of the services, information collection is probably the most controversial, as it may significantly infringe upon fundamental human rights, particularly the right to privacy. Therefore, this section will focus on information collection by providing a typology of information collection and relevant essential international standards.

Typology of information collection

Covert vs. overt information collection: With respect to methods, information collection by security services can be broadly categorized into two as overt and covert. Overt methods include gathering information from publicly available records, media reports, websites, blogs and so forth. These sources are also called OSINT (open source intelligence). Covert methods aim to obtain information without the knowledge and consent of the person. These methods include HUMINT (human intelligence) such as the use of informants or carrying out undercover operations; SIGINT (signals intelligence), which covers information collection by interception of electronic and/or telecommunications and IMINT (imagery intelligence),which collects information via satellite and aerial photography.[24] Beyond this categorization, security services apply methods ranging from more conventional ones such as monitoring postal communications, or newer methods including computer network exploitation (hacking). In this context, using covert, intrusive methods for information collection without the knowledge of the target is generally referred to as **surveillance**.[25] This report will focus mostly on electronic and communications surveillance.

***Targeted vs. mass surveillance*:** In terms of scale, security services conduct two types of surveillance. Targeted surveillance aims at monitoring identified individuals or groups of individuals that are suspected of committing an act falling within the mandate of security services.[26] On the other hand, as per Venice Commission's definition, mass surveillance 'is not necessarily predicated on a suspicion against a particular person or persons; rather it is proactive, aiming to identifying potential threats'.[27] There is no international agreement on the terminology with respect to 'mass surveillance': The UN, EU, and various organs of CoE use different terms; including 'broad surveillance'', strategic surveillance', 'bulk access to communications' each, with a slightly different definition, or aspect stressed.[28] This report will however use mass surveillance, except when country legislations specifically refer to another term.

It is good practice to regulate by law the two types of surveillance. A review by the EU FRA revealed that all EU member states except Cyprus have codified the use of targeted surveillance by their security and intelligence services. A majority of member state legal frameworks do not clearly regulate mass surveillance as such. However, an emerging good practice is to adopt laws clearly stipulating the regulation of mass surveillance by security/intelligence services.[29] With their recently adopted laws covering mass surveillance, Germany, France, UK, and Sweden are pioneers in this regard.

***Domestic vs. foreign surveillance*:** Surveillance by security services can be further distinguished by the geographical

---

24 Lauren Hutton, 'Tool 5: Overseeing Information Collection' p.90 in Born and Wills, *Overseeing Intelligence Services – A Toolkit*, (DCAF: 2012).

25 UNODC, 'Current practices in electronic surveillance in the investigation of serious and organized crime' (New York, 2009) available from: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf;

26 EU FRA, Surveillance by Intelligence Services, (2015), p.20

27 Venice Commission, Report on the Democratic Oversight of Signals Intelligence Agencies (2015), paras 38-46.

28 For a detailed overview of which term is used by which institution, see EU FRA, Surveillance by Intelligence Services, (2015), p.16

29 Ibid, p.17

area it covers. Whereas it is good practice to regulate by law both domestic and foreign surveillance with necessary safeguards against human rights abuses; in practice countries tend to place stricter rules and higher thresholds on domestic surveillance measures. This is because there is a higher risk of the executive using domestic surveillance for political purposes, endangering democratic order.[30] However this approach is criticized by expert circles in Germany, based on the argument that the right to privacy as recognized in the German basic law (Grundgesetz) is universal, and therefore nationality or country of residence should not be decisive factors for restricting the rights of foreign data subjects more than those of German citizens and lawful residents in Germany. [31]

Content vs. metadata: Lastly, surveillance can be categorized into two, depending on the type of data collected from communications. Security services can either access the actual content of communications, or metadata, i.e. the data about the communication, which includes the location that it originated from, the device that sent or made the communication, the times at which the message(s) were made and sent; the recipient of the communication, their location and device, and the time they received the message; information related to the sender and recipients of a communication, e.g. email address, address book entry information, email providers, ISPs and IP address; amongst others.[32] Traditionally, there have been weaker systems of oversight over the collection and use of 'metadata' on the basis that it does not contain the content of the communications, and that the collection is done through automated, computerized systems, which constitutes less of an interference with privacy than wiretapping. However, current technology makes it possible to analyze and combine metadata to create a comprehensive profile of a person including where they are at all times, with whom they talk and for how long, patterns of behavior, viewpoints, interactions and associations.[33]

An emerging standard is to more strictly regulate metadata collection by security services. In this regard, the Court of Justice of the European Union has invalidated the EU Data Retention Directive on the grounds that it 'interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data'[34] Recently, a German court has ruled that Germany's foreign intelligence agency (BND) must not store the metadata - such as phone numbers - of international phone calls for the purpose of intelligence analysis.[35]

Essential international standards on regulating surveillance

The previous section provided a brief overview of the methods, types and extent of surveillance conducted by security services, along with some emerging practices. If surveillance measures are not regulated, controlled and overseen effectively, there would be a high risk of abuse of surveillance powers and misuse of information collected. In this regard, based on the ECtHR case law on article 8 (right to privacy) and the UN compilation of good practices, a set standards concerning legislating on surveillance have emerged:

- **Legality:** The most fundamental standard is that any surveillance measure available to security services must be grounded in publicly available laws. National laws on surveillance should not contradict international law and human rights standards.
- **Necessity and proportionality:** That a surveillance measure is legally available to security services does not mean it should be used in any circumstances. Provisions of the law should comply with necessity and proportionality principles, and thus limit the use of surveillance for circumstances where it is absolutely necessary to counter a threat and stipulate that the level of intrusiveness of a measure should be proportional to the suspected threat.[36]

---

30 EU FRA, Surveillance by Intelligence Services Vol.2, (2017), p.91

31 See the discusssion in Thorsten Wetzling, 'Germany's Intelligence Reform: More surveillance, modest restraints and inefficient controls' SNV Policy Brief (2017), p.6 available from: https://www.stiftung-nv.de/en/project/digital-basic-rights-surveillance-and-transparency/publikationen,

32 Privacy International, *Explainers : What is Metadata*, available from: https://www.privacyinternational.org/node/53

33 Ibid.

34 See: Court of Justice of the European Union, *The Court of Justice declares the Data Retention Directive to be invalid*, Judgment in Joined Cases C-293/12 and C-594/12, Press Release No 54/14, (Luxembourg, 8 April 2014), available from: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

35 https://www.reuters.com/article/us-germany-surveillance/german-court-rules-against-foreign-intelligence-mass-communication-surveillance-idUSKBN1E82RS?feedType=RSS&feedName=technologyNews

36 Lauren Hutton, 'Overseeing Information Collection', Tool 5, p. 100, in Born and Wills, *Overseeing Intelligence Services – A Toolkit*, (DCAF: 2012)., Also see UN Compilation of Good Practices, paras 27-30

- **Specific safeguards in the law:** UN Compilation of Good Practices laid out a set of concrete safeguards for surveillance legislation to comply with necessity and proportionality principles. Practice 21 states that national laws outline:
  - Types of collection measures available to intelligence services;
  - Permissible objectives of intelligence collection *(this is also a key criteria considered by the ECtHR. The Court evaluates whether a surveillance measure pursue a legitimate aim, and if it is necessary in a democratic society to achieve that aim)*[37]*;*
  - Categories of persons and activities which may be subject to intelligence collection;
  - The threshold of suspicion required to justify the use of collection measures;
  - The limitations on the duration for which collection measures may be used.
- **Protected professions:** As per UN guidance, it is a good practice to impose certain restrictions on the use of surveillance measures against members of particular professions, notably lawyers and journalists. Respect to lawyer-client confidentiality as well as journalists' undisclosed sources are essential to the exercise of fundamental rights (the right to a fair trial) as well as the functioning of a free society.[38]
- **Control, authorization, and oversight:** Legal safeguards by themselves are not sufficient to ensure that surveillance measures are implemented appropriately. Practice 22 of the UN Compilation of Good Practices states:
  - '[I]ntelligence-collection measures that impose significant limitations on human rights are authorized and overseen by at least one institution that is external to and independent of the intelligence services. This institution has the power to order the revision, suspension or termination of such collection measures. Intelligence-collection measures that impose significant limitations on human rights are subject to a **multilevel process of authorization** that includes approval within intelligence services, by the political **executive** and by an **institution that is independent** of the intelligence services and the executive.'
  - Complying with this UN standard, surveillance measures in a majority of democratic countries are subjected to control, authorization and oversight processes by multiple actors. Relevant international standards and country practices are explained in the following Chapters of this report:
- Executive control of surveillance measures in Chapter 2;
- Judicial and quasi-judicial authorization of surveillance measures in Chapter 3.3;
- Continuous and ex-post oversight of the implementation of such measures by parliamentary committees and specialized oversight bodies in Chapters 3.1 and 3.2 respectively;
- The role of the civil society in monitoring surveillance related policies as well as bringing critical litigation against surveillance laws in Chapter 3.4.
- Individuals' access to their personal data held by security services is explained in Chapter 4, and therefore these issues will not be repeated in this section.

International standards on surveillance are by no means limited to what is presented in this section, however a detailed legal overview is beyond the purposes of this report. Countries are struggling with legislating on surveillance, as it is challenging to keep up with the pace of technological advancements and capabilities allowing for ever greater collection of data. The overview of country cases below does not aim to give a comprehensive legal analysis, instead it provides a brief outline of essential safeguards.

37 See EU fra, *Surveillance by Intelligence Services Vol 2.*2017, p.37

38 UN Compilation of Good Practices, Para 20 and 34

PRACTICES IN SELECTED COUNTRIES:

CROATIA

Organization: Croatia has two security/intelligence services, one military (Military Security Intelligence Agency/ Vojna sigurnosno- obavještajna agencija -VSOA) and one civilian (Security Intelligence Agency (Sigurnosno-obavještajna agencija -SOA). This section will focus on the latter. The SOA has both domestic and foreign mandates. For the hierarchical set-up and subordination of the SOA, see Chapter 2 on Executive Control of Security Services.

Mandate: Article 23 of the 'Act on the Security Intelligence System of the Republic of Croatia'[39] (hereinafter the Law), defines the mandate of the SOA as follows: 'SOA **collects, analyzes, processes and assesses** the political, economic, scientific/technological and security-related information concerning the foreign countries, organizations, political and economic alliances, groups and persons, especially those showing intentions, potential, concealed plans and clandestine activity directed **against the national security**, or other information relevant for the national security of the Republic of Croatia'.

Representing good practice, the law explicitly lists the national security threats. It consists of:

- terrorist acts and other forms of violence;
- the intelligence activity of foreign intelligence services, organizations and individuals;
- the organization of extremist activities of groups and individuals;
- endangering the safety of top state officials and protected facilities and areas;
- organized and economic crime;
- unauthorized access to protected information and communication systems of state authority bodies;
- disclosing of classified information, by state officials or the employees of state authority bodies, scientific institutions and legal persons with public authority, and other activities aimed at endangering national security

Contrary to the PACE Recommendation 1402, organized crime is included in the national security threats, and therefore the mandate of the SOA. However, it should be noted that in line with international standards, the SOA's mandate is restricted to collection, analyzing and processing of data, thus it does not have investigatory functions. The SOA is obliged to share organized crime related data with police and prosecutorial authorities who are in charge of investigating those acts.

Law enforcement powers: As the SOA does not have law enforcement functions, it is not granted investigation, arrest and detention powers. Article 27 of the Law stipulates that SOA officers can only interview persons, with expressly stated consent of the person, at the official premises of the SOA, by keeping interview records and making it available to judiciary and oversight bodies. In cases where a person does not give consent for such an interview, SOA is obliged to request the police to conduct the interview, if there are grounds to assume that the person possesses information related to national security. Indeed the Croatian law clearly establishing the terms of cooperation between security services and law enforcement agencies is good practice.

The law does not refer to the use of force by the SOA. However, a publicly available decree[40] stipulates that SOA officials who obtain the necessary certifications to bear firearms, are permitted to use a firearm, only in exceptional circumstances to protect their own or another person's life, as well as in their capacity to protect state authorities, (including SOA itself), protected individuals, or critical infrastructure in the frame of their counterintelligence mandate.

39 See https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf
40 https://www.soa.hr/UserFiles/File/Decree_bear_and_use_firearms.pdf

- **Surveillance measures and essential safeguards**: The Croatian law only recognizes targeted surveillance. Articles 33-37 of the Law are dedicated to the regulation of targeted surveillance, and explicitly list all measures of secret information, thereby complying with the legality principle. The measures include secret surveillance of telecommunications, postal surveillance, physical surveillance (bugging), secret surveillance through audio/visual recording of images/and the content of communications in public spaces (Article 33). The law allows both the collection of content and metadata, but subjects them to different level of authorization; and specifies their permitted duration (for more details, see the Chapter 3.3. on Judicial oversight). Representing best practice, the law clearly endorses the *necessity and proportionality principles* by stipulating that the surveillance measures 'may be applied if the information can not be obtained in any other way or the collection thereof is linked with disproportionate difficulties. In cases where choice between several different measures of secret information collection is possible, the one less invasive to constitutionally protected human rights and basic freedoms shall be applied' (Art 33). There are no specific provisions protecting journalists or lawyers in the Law.

CANADA

Organization: Canada has one civilian security/ intelligence agency (Canadian Security Intelligence Service- CSIS) and one military intelligence service (Canadian Forces Intelligence Command). In addition, as part of its defense portfolio, Canada has set-up the Communications Security Establishment, mandated to collect foreign intelligence. This section however will focus on the civilian service, the CSIS. The CSIS has both a domestic and foreign mandate, that is, it is allowed to also collect security intelligence abroad. Representing best practice, section 12(2) of the Canadian Security Intelligence Act[41] (hereinafter 'the Law') explicitly stipulates that the Service may perform its functions within or outside of Canada. For the hierarchical set-up and subordination of the CSIS, see Chapter 2 on Executive Control of Security Services.

Mandate: As stipulated in the Law the CSIS is mandated to 'collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada '(Section 12(1)). Complying with international standards, section 2 of the Law lists in detail what is meant by 'threat to the security of Canada:

(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage;
b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person;
(c) activities within or relating to Canada directed to- ward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and;
d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada
It is important to note that neither organized /economic crime, nor corruption is included in the list of threats and thereby excluded from the mandate of the CSIS.

Law enforcement powers: The law represents best practice concerning the clear prohibition of law enforcement powers. Section 12.1(1) of the law defines the powers of the service as follows: 'If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat.' However the Section explicitly states: 'For greater certainty, **nothing in subsection (1) confers on the Service any law enforcement power**.' In addition to explicitly prohibiting CSIS from using police powers, section 12.2(1) stipulates further prohibited conduct by stating:

'the Service shall not:

(a) cause, intentionally or by criminal negligence, death or bodily harm to an individual;

(b) willfully attempt in any manner to obstruct, pervert or defeat the course of justice; or

(c) violate the sexual integrity of an individual.'

Such clear provisions of the Law on prohibited conduct constitute a strong safeguard against torture, ill-treatment and incommunicado detention.

Surveillance measures and safeguards: Complying with the legality principle**,** Sections 21-28 of the Law regulates targeted surveillance conducted by the CSIS. The law lists the measures available to CSIS officers as 'to intercept any communication or obtain any information, record, document or thing and, for that purpose, (a) to enter any place or open or obtain access to any thing; (b) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or (c) to install, maintain or remove any thing' (Sec. 21(3)). In line with international standards, the law obliges CSIS to justify the necessity (21(2)b), and reasonableness & proportionality of measures (21.1(2)c) in warrant requests. It is important to note that the law establishes different criteria for applying surveillance measures to 'investigate a threat' and 'reduce threats to the security of Canada' (For further details on the authorization of surveillance requests, see the Chapter 3.3. on Judicial Oversight). The law does not stipulate any special protection for journalists or lawyers.

41 Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23) available from: http://laws-lois.justice.gc.ca/eng/acts/c-23/index.html

BELGIUM

Organization: Belgium has two security/intelligence services: The General Intelligence and Security Service of the Armed Forces (GISS) which is the military intelligence agency; and the 'State Security' (Sûreté de l'État), which is the civilian security / intelligence service (hereinafter the Service) with both a domestic and foreign mandate. This section will focus only on the Service. For the hierarchical set-up and subordination of the Service, see Chapter 2 on Executive Control of Security Services.

Mandate: The Organic Law on Intelligence and Security Services[42] (hereinafter the Law), regulates mandate, powers and functions of the Service. Article 7 of the Law defines the Mandate of the Service as follows:

- Research, analyze and process information related to all activities which threaten or may threaten internal security of the State and the continued existence of the democratic and constitutional order, the external security of the State, and international relations, the scientific or economic potential as defined by the National Security Council, or all other fundamental interests of the country defined by the King, on the proposal of the National Security Council;
- Perform security vetting as entrusted to it upon directives of the National Security Council;
- Research, analyze and process intelligence related to activities of foreign intelligence services on Belgian territory;
- Perform any other duties entrusted to it by virtue of the Law.

In line with best practice, Article 8 of the law lists the threats to national security. They include any individual or collective activity developed in the country or abroad that might relate to espionage, terrorism, extremism, proliferation, harmful sectarian organizations or criminal organizations. Although the categories seem broad in the first instance, they are defined in great detail in the law. In particular, the Service can only collect information on these threats insofar as they relate to the internal security of the State and the continued existence of the democratic and constitutional order, the external security of the State, and international relations, the scientific or economic potential.

Therefore, it should be noted that the Belgian model complies with internationals standards, since it largely restricted the Service's mandate to collection, analyzing and processing of information. The Service is not allowed to investigate on its own the crimes falling under its mandate. However, if requested, the Service can provide technical support to criminal justice institutions in the framework of judicial investigations (e.g. terrorist cases) as long as it is carried out within the boundaries of protocols approved by the concerned Ministers.[43]

Law enforcement powers: As a general rule, the Service does not have law enforcement powers, such as stop and search, arrest and detention, which is in line with international standards. However, the Service has an 'intervention team', designated by the Ministry of Justice, for the sole purpose of protecting certain personnel and infrastructure of the Service. Members of this intervention team are given certain police powers, however the cases which they can apply those powers are very precisely defined in the law. For instance, the Law stipulates that 'members of the intervention team may, if absolutely necessary, arrest a person if there are reasonable grounds for believing that, the person is preparing to commit or commits an act that seriously endangers the life or physical integrity of a protected officer or an infrastructure. In this case, the person can only be held until the police arrive, but it may in no case exceed one hour'. (Art 27 of the Law).

Surveillance measures and safeguards: According to the Law, the Service is only allowed to carry out targeted surveillance. In line with the legality principle, articles 14-18 of the Law regulate in great detail the application of surveillance measures. The law categorizes surveillance measures as 'ordinary', 'specific' and 'exceptional' based on their intrusiveness, which represents best practice. Ordinary measures include, inter alia, requesting information from criminal justice authorities (even that is subject to certain restrictions) as well as access to public sector data

42 Loi Organique des Services de Renseignement et de Securite (18 decembre 1988), available from : http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032

43 Article 20 of the Law, also see http://www.comiteri.be/index.php/en/39-pages-gb/305-what-do-intelligence-and-security-services-stand-for

banks (Art 14). Specific measures include

- Entry, search and surveillance of public places with technical devices;
- Inspection of identification data for postal traffic;
- Inspection of identification, call and localization data (metadata) for communications.

Exceptional measures include: (Art 16-18 of the Law)

- Entry into, search and surveillance of private places;
- Setting up false identities and using undercover agents;
- Opening and inspecting private posts;
- Collecting data on bank accounts and banking transactions ;
- Penetrating an IT system (computer network exploitation/hacking);
- Monitoring, intercepting, recording the content of communications[44]

By distinguishing between the intrusiveness of measures, and by regulating in detail the circumstances in which such measures can be applied, the Belgian law best practice in implementing the necessity and proportionality principles. The Belgian law is considered very progressive as it includes hacking practices and undercover operations in the exceptional surveillance measures, with the strictest controls.

Protected professions: Complying with international standards, the law imposes specific restrictions on the application of surveillance methods for professionally confidential information of lawyers and doctors, as well as secret sources of journalists (Art 2).

44 Also see http://www.comiteri.be/images/pdf/Jaarverslagen/Activity_Report_2014_15.pdf p.148-149

Organization: Germany has quite a different set up than the other countries. Each of its 16 states (Länder) has its own domestic security service. At the federal level there are three services: the Military Counter-Intelligence Service (MAD), the Federal Office for the Protection of Constitution (Bundesamt für Verfassungschutz - BfV) which is the civilian domestic security service, and the Federal Intelligence Service (Bundesnachrichtendienst -BND) which is the civilian external intelligence service.[45] This section and the report will mostly focus on the BfV, however, where relevant, references to the BND will also be made. For the hierarchical set-up and subordination of the BfV, see Chapter 2 on Executive Control of Security Services.

Mandate: As per the Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution (hereinafter the BfV Law),[46]the BfV is mandated **to collect and analyse** information on efforts:

- directed against the free democratic basic order;
- against the existence and the security of the Federation or one of its States;
- aimed at unlawfully hampering constitutional bodies of the Federation or one of its States or their members in the performance of their duties;
- jeopardizing foreign interests of the Federal Republic of Germany by the use of violence or the preparation thereof ;
- directed against the idea of international understanding (as per article 9, para. 2 of the Basic Law, especially against the peaceful coexistence of peoples.

Beyond this core mandate, the BfV also collects information on intelligence activities carried out on behalf of a foreign power (counter-intelligence) and contributes to counter-sabotage and personnel/physical security.[47]

It should be noted that the limits of BfV's mandate comply with international standards: the threats under the BfVs mandate do not include corruption or organized crime. However, Germany grants "intelligence-like means to units specialized in a defined threat" such as the Federal Criminal Police) in the area of counterterrorism; and the Customs Criminal Investigation Office in the area of combating proliferation, smuggling, money laundering and other cross-border organized crime.[48]

The BND is mandated to collect and analyze information relating to important political, economic, and technical developments abroad, as well as abstract or concrete security of the Federal Republic of Germany and its citizens. More precisely, the BND is mandated to conduct strategic surveillance on armed attack, international terrorism, arms proliferation, smuggling of narcotics of substantial important in the EU, counterfeiting of money undermining the stability of the Euro, money laundering, and human trafficking of substantial importance.[49]

It is also tasked with[50]:

- supporting the Federal Government in its security and foreign policy decisions, by providing information on foreign countries,
- providing information to the Military in its foreign missions,

---

45 As stated earlier, although the BND has a predominantly foreign focus, it is also mandated to carry out domestic-foreign surveillance, and therefore can be categorized as having both an internal and external mandate.

46 https://www.gesetze-im-internet.de/bverfschg/

47 BfV Law, article 3 see https://www.verfassungsschutz.de/en/about-the-bfv/tasks/what-exactly-are-the-tasks-of-the-domestic-intelligence-services

48 German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.16 available from: http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu

49 Germany, Act on the Federal Intelligence Service, Sections 1 (1) and 2(1); Germany, G 10 Act, Section 5 (1).

50 http://www.bnd.bund.de/DE/Auftrag/Aufgaben/aufgaben_node.html

► Mediation in humanitarian negotiations worldwide,

► Inform ministries and authorities on specific issues.

Law enforcement powers: The BfV is not given the powers to conduct criminal investigations and exercising law enforcement powers. Representing best practice, it also cannot order the police to carry out arrests on its behalf. However, the BfV law outlines in detail the specific and circumstances under which the BfV is allowed to share information with the law enforcement agencies (Articles 20-23 of the Law).

Representing best practice, the BND Law explicitly bans the service from exercising police powers. Article 2(3) states: 'The BND is not entitled to any law enforcement authority /task. Nor may it ask the police, by way of mutual assistance, measures which itself is not entitled to take'[51].

The unequivocal prohibition of law enforcement powers for security/intelligence services in Germany constitutes best practice.

Surveillance safeguards

Legality: Surveillance in Germany is regulated mainly by the Law on the Secrecy of Post and Telecommunications (referred as the G-10 Law named after Article 10 –right to privacy- of the German Basic Law (GrundGesetz)), as well as the BND Law. The BfV carries out domestic surveillance, while the BND conducts predominantly foreign surveillance (it can however wiretap international communications from/to Germany too, subject to the G10 Law). While both can carry out targeted surveillance, the BND is also allowed to conduct mass surveillance (it is referred to as 'strategic surveillance' in German legislation).

Necessity and proportionality: In line with the proportionality principle, the G10 Law lists the categories of persons who may be subjected to intrusive surveillance measures upon concrete indications of suspicion. They include, inter alia, those who are suspected of high treason, threats to state of law, offenses against the national defense and security of troops, committing cybercrimes, insofar as it is directed against internal/external security of Germany (Art 3(1)). Furthermore, it complies with the necessity principle by stating that resort to such measures are only permissible, if the investigation of threats would otherwise be impossible or substantially more difficult. (Art 3(2)).

Complying with international standards, Articles 9-13 of the Law include detailed provisions on how surveillance measures should be requested, authorized, implemented, and terminated. For more details on the authorization of surveillance measures, see Chapter 3.2 on Judicial Oversight).

Protected professions: The German Criminal Procedure Code lists a number of professions, whose members have a right to refuse testimony on professional grounds, including, inter alia, clergymen, lawyers, doctors, parliamentarians and journalists (Article 53)[52]. Representing good practice, the G-10 Law makes a reference to those professions listed in the CPC; and imposes certain restrictions on the application of surveillance measures targeting such professionals (Article 3b of the G-10 Law).

51 https://www.gesetze-im-internet.de/bndg/

52 Code of Criminal Procedure in the version published on 7 April 1987 (Federal Law Gazette [Bundesgesetzblatt] Part I p. 1074, 1319), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I p. 410) https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html

CHAPTER 2: EXECUTIVE CONTROL OF SECURITY SERVICES

2.1. THE ROLE OF THE EXECUTIVE AND THE SCOPE OF ITS CONTROL

As per the UN Compilation of Good Practices, 'States are internationally responsible for the activities of their intelligence services[53] and agents, and any private contractors they engage, regardless of where these activities take place and who the victim of internationally wrongful conduct is. Therefore, the executive power takes measures to ensure and exercise overall control of and responsibility for their intelligence services'[54] Whereas the exact role of relevant government departments and the extent of control exercised by them differs across countries, typically the role and responsibilities of the executive includes:[55]

- ***Appointing the director of the service:*** While there are different practices for consulting with external oversight actors (see the next subsection below), it is generally accepted that the executive, as the politically responsible organ for the services, takes the lead in nominating and appointing the director.
- ***Establishing policies and formulating directives for the security service:*** As for any other agency under its control, the Government is in charge of policy setting in the area of security and intelligence. In addition, it issues directives on the work of the security service, including guidance on human rights compliance by the service. [56]
- ***Approving cooperation with foreign security services:*** It is a widely accepted standard that the cooperation with foreign counterparts of security services is subjected to the executive's approval. In almost all EU member states, security services must receive the approval of the executive before concluding an international agreement. [57]
- ***Authorizing sensitive operations and the use of intrusive surveillance:*** As per international practice, another crucial role of the executive is to approve and authorize the activities and methods of security services that have the greatest potential for infringing fundamental human rights. In several Council of Europe and EU Member States, the executive is part of the authorization process.[58] However, it is important to note that the executive shall not be the only authorizing authority; either the judiciary or quasi-judicial bodies shall be entitled to review the legality, proportionality and necessity of such measures.
- ***Reporting to the parliament:*** Having the abovementioned crucial role and powers, the executive is politically responsible for the conduct of security services. [59] A basic consequence of this responsibility is that the executive is held accountable by the Parliament regarding the security services. In this respect ministers are required to report to the parliament concerning the overall functioning of security services.

2.2. SAFEGUARDS FROM ABUSE OF POWER BY THE EXECUTIVE

While executive control is essential to ensure that security services function effectively and properly, it also carries the inherent risk of abuse of powers by the executive, such as using the services for personal or own political motivations, or exerting political influence and pressure over the services. There are certain international standards, which serve as safeguards from such abuse of power from the Executive.

---

53 UN Compilation of Good Practices' reference to intelligence services, cover both intelligence and security services as used in this report. See p.4

54 UN Compilation of Good Practices, Practice 14

55 The list is adapted from Born and Mesevage, Introducing Intelligence Oversight, in Born and Wills (ed) 'Overseeing Intelligence Services : A Toolkit' ,(2012), p.8

56 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p. 57 available from:https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770

57 EU FRA *Surveillance by Intelligence Services Vol 2.* 2017, p.101

58 EU FRA , *Surveillance by Intelligence Services* 2015, p.34, also see CoE, 2015, p.57-58

59 Born and Mesevage, Introducing Intelligence Oversight, in Born and Wills (ed) 'Overseeing Intelligence Services : A Toolkit' ,(2012), p.10

- ***Subordination / open –door policy:*** Security services are typically subordinated to an executive ministry, such as the Ministry of Interior or the Ministry of Justice. There are however examples of subordination to the Prime Minister, the President, or to both as in the case of Croatia.[60] In certain contexts, direct subordination to a single person or a Ministry can carry the risk of abusing the services for personal /political motives. One safeguard against this risk is the 'open-door policy', i.e. entrusting the director of the service with direct access to another Ministry, different than which it is subordinated to. For instance, In the United Kingdom, the agency heads of the Security Service, the Secret Intelligence Service and Government Communications Headquarters, although responsible to the Home Secretary and Foreign Secretary respectively, have a right of access to the Prime Minister.[61]

- ***Separation between control and management:*** Whereas the executive is expected to carry out the overall control of the services, it should not assume the direct managerial responsibility for security and intelligence operations. In the words of the Venice Commission: '[I]t will be impossible for political leaders to act as a source of external control if they are too closely involved in day-to- day matters and the whole oversight scheme will be weakened. There is the danger also of politicising the intelligence cycle, with the consequence that the analysis stage and the end- product will be less useful.'[62] Therefore, in order to prevent abuse and improper interference, national laws should clearly stipulate the responsibilities of both the relevant minister (or the executive body in charge), and the director of the service.

- ***Transparency of ministerial directions:*** Another key safeguard to ensure that the executive do not issue directives to further their political interests and motives, is to subject ministerial directives to external review. While it is understandable that such directives may need to be shielded from general public due to protection of confidential information, expert oversight bodies are well suited to access ministerial directions. [63]

- ***Prohibition of serving political interests and targeting political adversaries:*** As per UN guidance, it is considered good practice when '[N]ational law prohibits intelligence services from engaging in any political activities or from acting to promote or protect the interests of any particular political, religious, linguistic, ethnic, social or economic group'[64]. For instance, the UK's Security Service Act has an explicit stipulation that 'that the Service does not take any action to further the interests of any political party'.[65] Another good practice endorsed by the UN is that '[I]ntelligence services are prohibited from using their powers to target lawful political activity or other lawful manifestations of the rights to freedom of association, peaceful assembly and expression'.[66] Such a provision in the law would serve as a strong basis for political neutrality.

- ***Appointment procedures:*** As mentioned earlier**,** it is common practice that the executive takes the lead in appointing the director of the security service. However, an important standard is that there should be a democratic and inclusive consultation mechanism in the process of nominating a candidate. There are different country practices in this respect. In Australia, the Prime Minister must consult with opposition leaders before appointing the director. [67] In a number of European states, including Estonia, Portugal, Hungary, and Croatia the competent parliamentary committees hold a hearing with a nominee and can issue a non-binding opinion or recommendation on the proposed appointment. Such involvement of competent parliamentary committees (usually the committee in charge of overseeing security services) ensures that the nominee has a broad political backing. Lastly, in some countries such as the US and Romania, parliamentary committee hearing is followed by a vote on the plenary on whether to approve the nomination. It should be noted that, although a parliamentary vote is the ultimate form of democratic nomination, it has an inherent risk of 'politicization' of the process, turning into a partisan matter.[68] Furthermore, in parliamentary models where the ruling coalition disproportionally

---

60 For further discussion and examples, see Council of Europe*, Democratic and Effective Oversight of National Security Services*, (2015),p.57

61 Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, (DCAF: 2005), p.70

62 Venice Commission, *Democratic Oversight of the Security Services* (2007), para 143

63 Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, (DCAF: 2005), p.69, available from: http://www.dcaf.ch/making-intelligence-accountable

64 UN Compilation of Good Practices, Practice 11

65 UK , Security Service act, 1989, Section 2 (2)b, https://www.legislation.gov.uk/ukpga/1989/5/section/2

66 UN Compilation of good practices, Practice 12

67 Australia, Security Intelligence Organisation Act, section 17(3),

68 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p.107, 108

dominates the seats (due to electoral thresholds), voting may not serve the intended affect. In such cases, an obligatory consultation with opposition leaders, and hearings at the parliamentary committee can be more effective.

- ***Fixed tenure and dismissal processes:*** Another standard to protect the service from abuse of power by the executive is to provide by law a minimum tenure time to the director, so that he/she can operate without the fear of dismissal at the whim of the executive. The procedures for the dismissal should be clearly stipulated by law, and should not leave much room for interpretation and discretion of the executive.
- ***Disclosing information and whistleblowing:*** Lastly, the members and staff of the security services should be given the legal rights and avenues to disclose information to external bodies in cases where they are concerned with wrongdoing (for instance unlawful orders from the executive, improper political pressure and so forth). As per UN standards, it is good practice for national law to outline specific procedures for members of intelligence services to disclose concerns about wrongdoing. Accordingly, members of services should be protected from legal reprisals.[69] When there are such legal safeguards in place, members of the executive would be less inclined to misuse their powers and exert political influence if they know such misconduct could be made public.

69 UN Compilation of Good Practices, Practice 18

PRACTICES IN SELECTED COUNTRIES

CANADA

The Canadian Security Intelligence Service Act[70] (hereinafter ' the law') is a prime example of a legal basis embodying most of the international standards and safeguards against abuse of power mentioned in this section. In Canada, the executive, in particular, the Minister has a considerable degree of control over the CSIS. In line with the key roles listed in this section, the Ministry in charge is responsible for, inter alia:

- Establishing directives to the service
- Approving CSIS agreements with foreign counterparts (Section 13(3) of the Law)
- Authorizing CSIS domestic cooperation with other security forces in Canada (Section 17)
- Review periodic reports on the Service's operational activities (Section 4)
- Reviewing warrants (to employ special measures) before they are submitted to the designated judge (Section 6(2)).

***Subordination**:* The Canadian Security Intelligence Service (CSIS) reports to the Ministry of Public Safety and Emergency Preparedness.

Separation between control and management: Complying with international standards, the law clearly stipulates that '[T]he Director, *under the direction of the Minister, has the control and management* of the Service and all matters connected therewith (Section 6(1)). Subsequent sections of the law also explicitly list the duties and responsibilities of the director of CSIS, in terms of when to report to the Minister, under which circumstances and over which issues to consult with the Minister (Section 6(4)).

Transparency of ministerial directives: According to the law, a copy of each written direction issued by the Minister to the CSIS, should be submitted to the Security Intelligence Review Committee (SIRC)(Section 6(2)). By proactively obliging the security service to share ministerial directions with the expert oversight body, the Canadian model adopted a powerful safeguard against Ministerial abuse, and thus represents international best practice.

Prohibition of serving political interests and targeting political adversaries: Another example of best practice is the Section 2 of the Law, which explicitly bars CSIS from investigating "lawful advocacy, protest or dissent," unless it is carried out in conjunction with one of the threat-related activities defined in the law.

***Appointment and tenure**:* The director is appointed by the cabinet (through a process known in Canada as Governor in Council (GIC) appointment), for a five-year term, renewable only once (Section 4). The Minister in charge is responsible for recommending appointments, but the GIC appointment process is one which is open to all Canadians, transparent and merit-based.[71]

Disclosing information and whistleblowing The Canadian Security of Information Act has a special section for persons who are permanently bound by secrecy. The Act outlines specific procedures for the officers of the CSIS to disclose information in the public interest. However, before disclosing the information, the officer should bring the matter to the attention of Deputy Attorney General, and in case of no response, with the Security Intelligence Review Committee, before disclosing the information (Section 15(5)).[72]

---

70 Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23) available from: http://laws-lois.justice.gc.ca/eng/acts/c-23/index.html

71 This is a quite a unique approach and do not have much equivalence in Europe. For more information, see https://www.appointments-nominations.gc.ca/prsnt.asp?menu=3&page=FAQ&lang=eng

72 Canada, Security of Information Act (R.S.C., 1985, c. O-5), available from http://laws-lois.justice.gc.ca/eng/acts/O-5/

Subordination: The Croatian Security and Intelligence Agency (SOA) is subordinated to both the President and the Prime Minister through the National Security Council (NSC). According to the Act on the Security and Intelligence System of the Republic of Croatia[73] (hereinafter 'the Law'), the NSC serves to 'effectuate the cooperation between the President of the Republic and the Government in directing of the work of SOA' (art 3(1)). While the NSC is chaired by the President, all decisions need to be co-signed by the President and the Prime Minister. Contrary to the Canadian model the SOA does not fall under the portfolio of a single ministry, instead subordinated directly to the National Security Council. The NSC performs almost all the functions of executive control, including:

- Defining annual guidelines for the work of the service
- Propose the budget
- Approves international cooperation agreements
- Reviewing the reports of the SOA, and evaluating the implementation of decisions/directives issued by the President and the Prime Minister.

The NSC has a dedicated office facilitating its executive control functions. The Croatian model provides an important safeguard against the risk of executive abuse of power, since the power to control the service is not concentrated in a single Ministry and all decisions shall be co-signed by the President and the PM.

Appointment of the director: In line with the subordination structure, the Director of the SOA is appointed by a decision co-signed by the President and the PM, for a four-year term, with possibility for renewal. However, in compliance with international standards, the law requires that the opinion of the Parliamentary Committee for Interior Policy and National Security should be obtained (art 66(1)). While the parliamentary committee does not have a formal veto power, a strongly articulated negative opinion of a candidate would damage the legitimacy of the President's and the PM's nomination.

Dismissal of the director: The law stipulates the dismissal procedure in detail, with a long list of all the conditions under which a Director can be dismissed. The conditions include: "become permanently incapacitated for the performance of their duties; if they do not implement the decisions of the President of the Republic and the Government, which direct the work of the security intelligence agencies, or they fail to implement the oversight measures; due to the violation of the Constitution, laws and other rules and regulations the abuse of powers or overstepping of authority; the violation of classified data secrecy, and if a final judgment for a criminal offence has been pronounced against them which renders them unworthy of the position."(art. 66(4) of the Law). While it is good practice to enlist clearly the dismissal conditions, broad formulations such as 'violations of rules and regulations' gives a wide discretion to the executive, given that such rules and regulations are by law, secret. According to the law, before a final decision about the dismissal is reached, the opinion of the Croatian parliament *may* be sought. (art 66(5)) Since it is not obligatory, it cannot be considered as a strong safeguard against arbitrary dismissal.

Prohibition of serving political interests*:* Article 77 of the Law explicitly forbids the employees of the security services from 'membership in political parties, participation in activities thereof, acting on behalf of any political party within the security intelligence agency', which represents best practice.

Transparency of directives*:* Regulations passed by the Government (with approval of the President) concerning the security service is classified (Art 62) and there is no obligation to proactively share them with oversight bodies, as is the case in Canada.

Disclosure of information by SOA officials*:* There are strict measures against the disclosure of information, and unlike in the Canadian system, there are no mechanisms for disclosing information on wrongdoing in the interest of the public. Only in the circumstances when an officer receives an unlawful order from superiors, which constitute a criminal act, the person is obliged to notify the chairperson of the Parliamentary Committee and the head of the Office of the National Security Council (Art 67(2)).

73 https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf

The extent of the external control in the Belgian system is more limited compared to the Canadian and Croatian models. In view of legal experts 'there is no real executive control over the civil intelligence service, as it is does not require government authorization for any of its missions.'[74]Accordingly, there seems to be less of a focus in the legal framework concerning safeguards against executive abuse.

Subordination: According to the Organic Act on Intelligence and Security Services, The 'State Security', the civilian intelligence service of Belgium, is primarily subordinated to the Ministry of Justice, although the Ministry of Interior has also authority over the service insofar as it relates to maintaining public order and the protection of people.[75]This partial co-supervision can be seen in the fact that the Minister of Justice may in some cases need the signature of the Minister of the Interior, or shall obtain his concurring advice in a number of other cases.[76]The Ministry of Justice's role concerns the overall supervision of expenditure, management and training of personnel, the internal rules and discipline, the pay and remuneration, and equipment (art. 5(3) of the Law).

As a part of recent security sector reforms, Belgium established the National Security Council, which has been put in charge of inter alia, establish policies and priorities of the security service. In addition, the NSC is in charge of determining the conditions for international cooperation of the Service with its foreign counterparts. Beyond the legal stipulation that the security service should carry out its activities in accordance with the directives set by the NSC, the Service is not, however, controlled by the NSC.[77]For comparison, the office of the National Security Council of Croatia has broader supervisory competences over the Croatian security service.

Appointment: The Director of the service is appointed by the King, de jure on the proposal of the Minister of Justice, but in practice by the government as a whole. The tenure term is five years and renewable[78] While there is no formal involvement of the Parliament, the Director is obliged to take the oath before the chairman of the Monitoring Committee for Supervision of the Intelligence and Security Services before taking office.[79]

Disclosure of information: Similar to the Canadian model, the legal framework in Belgium provides a strong safeguard against executive abuse of powers, by providing the members of the security service with the opportunity to disclose information to the expert oversight body. The Committee I is empowered to: [E]xamine the complaints and denunciations of individuals who have been *directly concerned by the intervention of an intelligence service*... *Any public officer*, any person performing a public function, and any member of the armed forces directly *concerned by the directives, decisions or rules applicable to them, as well as by the methods or actions*, may lodge a complaint ... *without having to request authorization from his superiors*.[80]

74 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.19 available from: http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu

75 Loi Organique des Services de Renseignement et de Securite (18 decembre 1988), Article 6, available from : http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032

76 Wauter Van Laetham, The Belgian Civil Intelligence Service: Roles, Powers, Organisation and Supervision , EJIS, Volume 2, (2008), p.21 available from : http://www.comiteri.be/index.php/en/publications/specialized-literature

77 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.23

78 Wauter Van Laetham, The Belgian Civil Intelligence Service: Roles, Powers, Organisation and Supervision , EJIS, Volume 2, (2008), p.22

79 Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, (DCAF: 2005),p.34

80 Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment, Articles 40, available from: http://www.ennir.be/sites/default/files/pictures/pdf_11.pdf

Subordination: As mentioned earlier, Germany has two civilian security services: BfV (Federal Agency for the Protection of Constitution) and the BND (Federal Intelligence Service). While the BfV is subordinated to the Ministry of Interior, the BND reports to the Federal Chancellery.

Contrary to the Belgian model, the executive plays a larger role in Germany, especially when it comes to controlling surveillance measures. Upon a request by the head of the intelligence service, the Federal Ministry of Interior studies the merit of the interception order, puts any favorable decision in writing, and forwards it to the G 10 Commission, which is the expert oversight body in charge of its final approval. The Ministry of the Interior may also authorize surveillance in emergency circumstances, but the authorization is subject to ex-post review by the G 10 Commission.[81]

Appointment and dismissal of directors: The executive is in charge of nominating the BfV and BND directors.[82]

Transparency of ministerial directives: In the framework of the most recent security/intelligence reforms, Germany amended its laws to oblige the BfV and BND to proactively inform the parliamentary oversight committee on the 'internal administrative directions/developments with substantial ramifications for the pursuit of the services' mandate.[83]This practice is similar to the one in Canada, which can be regarded as a safeguard against the executive issuing arbitrary directives to the Service for its own political gains.

Disclosure of information by service officials: The German legal framework allows the officials of security/intelligence services to disclose information concerning misconduct to the Parliamentary Oversight Committee. However, before accessing the Committee, officials should first raise the issue they are concerned with internally, within the service. [84]This conditionality can be considered as a less optimal than the practice in Belgium, whereby an official can disclose information on misconduct directly to the oversight committee without having to raise it internally first.

81 *EU FRA, Surveillance by Intelligence Services (2015), p.33*

82 In the framework of the research for this report, no information was found concerning the involvement of the Parliament in the appointment /dismissal processes of service directors.

83 The Law on the Parliamentary Control of Federal Intelligence Services Art.4.1, available from : http://www.gesetze-im-internet.de/pkgrg/BJNR234610009.html

84 Ibid, Article 8(1)

CHAPTER 3: OVERSIGHT AND ACCOUNTABILITY OF SECURITY SERVICES

There is no single 'correct' model for the oversight of security services, however as per international standards, oversight should be comprehensive, and conducted by a number of actors including, the parliament, specialized bodies, the executive, judiciary, as well as civil society organizations.[85] The mandate and powers of such oversight actors should be carefully elaborated to ensure that there is no overlap and duplication among each other, while no aspect of the work of security services shall be left outside of the oversight system. This chapter outlines international standards and good practices for oversight exercised by each of those actors.

3.1. PARLIAMENTARY OVERSIGHT OF SECURITY SERVICES

The Parliament is an essential component of an accountability system, since it has the ultimate 'democratic legitimacy', as elected individuals oversee security services. [86] Although the mandate and scope of parliamentary oversight varies in each country, parliaments usually carry out three main functions with regards to the security services: (i) drafting and adoption of legislation regulating security services, (ii) scrutinizing and approving the budget of security services, (iii) overseeing policies and activities of security services.[87] This section will focus on the third function and outline some of the key features for an effective oversight.

Parliamentary committees: Although there are several parliamentary tools for oversight (plenary debate, questions to the Ministers, ad-hoc inquiries and so forth), a widely accepted international standard is to ensure that oversight of the security services fall under the remit of at least one standing parliamentary committee to ensure continuous and comprehensive oversight.[88] In 26 countries out of 28 EU members, there is at least one parliamentary committee responsible for overseeing security services. While some countries chose to establish a specialized committee with an exclusive mandate over security services, in others there is one committee with a broader purview, including defense and law enforcement agencies.[89] However, throughout the Council of Europe area, there is a growing tendency for specialized parliamentary committees with exclusive mandate over security services. [90]

Mandate: The mandate of parliamentary oversight committees may differ in each country, nevertheless EU-wide surveys and comparative research found that a great majority of parliamentary committees oversee the policies, administration and finance of security services. In addition to that common mandate, some committees are further tasked with overseeing completed intelligence operations, and few committees in Europe oversee ongoing intelligence operations. Nevertheless, it should be noted that parliamentary committees mostly perform ex-post facto oversight, except for their budget appropriation function and their involvement in the appointment of the director of services. [91] According to the Venice commission, this practice (ex-post facto oversight) is in line with international standards, since bodies overseeing the security services, should not be tasked with receiving ex-ante information and approving certain types of intelligence operations, which makes them part of the system they are supposed to supervise.[92]

Apart from the aforementioned mandates, some parliamentary committees in Europe are mandated to oversee

85 UN Compilation of Good Practices, para 13.

86 Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, (DCAF: 2010), p. 42, available from: http://www.dcaf.ch/guidebook-understanding-intelligence-oversight

87 Ibid. p.34

88 See Venice Commission, *Democratic Oversight of the Security Services* (2007) p.33 ; Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011) p.87

89 EU FRA, *Surveillance by Intelligence Services Vol 2* (2017), p.66

90 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.42

91 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011) p.102, EU FRA, *Surveillance by Intelligence Services* (2015) p.34

92 Venice Commission, *Democratic Oversight of the Security Services* (2007) para 74

specific aspects of the work of security services, such as overseeing information collection measures, the use of personal data, as well as handling individual complaints against security services. However, given the complexity of those tasks and the time, expertise and resources they require; European countries increasingly opt-for establishing separate expert oversight bodies (16 EU member states have done so far) [93], exclusively dedicated to overseeing security services with extensive oversight powers. The mandate and powers of such expert oversight bodies will be discussed in greater detail in the next section.

Oversight methods and powers: Parliamentary committees have a range of oversight methods available to them. Most common of those methods are to review yearly reports of security services, to hold committee hearings and invite senior management of services to give tesitimony, to invite external experts to give testimony on a thematic issue, to hold regular meetings with security services, and conduct inspections of the facilities of security services.[94] In order to effectively carry out such oversight activities, parliamentary committees should be provided with sufficient powers, most notably the power to access information. International actors including the Venice Commission, the UN[95] and the CoE Commissioner for Human Rights have highlighted the crucial importance of access to information. The latter has stated:

> *"[A]ll bodies responsible for overseeing security services [should] have access to all information, regardless of its level of classification, which they deem to be relevant to the fulfilment of their mandates. Access to information by oversight bodies should be enshrined in law and supported by recourse to investigative powers and tools, which ensure such access. Any attempts to restrict oversight bodies' access to classified information should be prohibited and subject to sanction where appropriate."*[96]

In line with this standard, in a great majority of European parliaments, MPs, especially members of parliamentary oversight committees are granted access to classified information. However, in most of those parliaments certain types of restriction are applied, such as the 'need –to-know' principle[97], signing of a non-disclosure agreement or vetting of MPs before they are appointed to a parliamentary committee.[98] It should be noted that vetting of MPs is not a recommended practice, since in most cases vetting of MPs is carried out by security services, which is supposed to be overseen by those MPs themselves. In cases where vetting is required by law, it is recommended to make the report of security services of advisory nature, and rest the final decision of appointment with the parliament.[99]

Committee composition: As per international standards, former employees of security services as members of such parliamentary committees are not recommended, especially in countries with a history of repressive security services.[100] In order to ensure cross-party membership in parliamentary committees, a great majority of European parliaments adopted the approach of proportional representation, while some countries provided additional guarantees for opposition and minority parties in such parliamentary oversight committees.[101] It is generally considered a good practice to grant chairpersonship of the Committee to the opposition.[102] Furthermore, electing members of that committee by a vote in the plenary, instead of mere appointment by political party heads or parliamentary speaker, enhances the legitimacy of the committee.

Resources: Overseeing security services is a complex and demanding task, which requires substantial knowledge and expertise. Given the competing priorities of MPs and the lack of expertise in the work of security services, it is important that the Parliamentary Committees are supported with the he necessary financial, technological, and human resources to exercise effective oversight.[103] This includes resources for permanent staff of the Committee, the ability to invite external subject matter experts on an ad-hoc basis, and physical measures and equipment to review and handle confidential information.

---

93 EU FRA, *Surveillance by Intelligence Services Vol 2* (2017)p.68, See Table 2 for the countries which have established.

94 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p.135

95 UN Compilation of Good Practices (2011), Practice 7

96 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.13

97 According to this principle, persons can only access information if their official functions necessitate access to particular information, which applies in most parliaments.

98 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p.117

99 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015) p.44

100 Venice Commission, *Democratic Oversight of the Security Services,* (2007), para 173

101 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), pp92-95

102 Ibid, para 176

103 The Tshwhane Principles, Principle 33

GERMANY

Germany has one of the most advanced parliamentary oversight systems in Europe. In line with international standards, there is a specialized parliamentary committee 'Parliamentary Control Panel' (hereinafter the Panel), with a remit to oversee all three federal security/intelligence services. The establishment of this Panel is enshrined in the German basic law, which is a testament to the significance attached to parliamentary oversight. A separate law on Parliamentary Control of Federal Intelligence Services[104] (hereinafter the Law), regulates the oversight by the Panel in more detail.

***Mandate*:** The Panel is mandated to oversee the activities of all federal security services (art 1). However, this mandate is broadly interpreted to also include policies and finances of security services. The Panel scrutinizes finances of the services in cooperation with another specialized parliamentary committee (The Trust Committee). The Panel is further tasked with regularly receive information on internal policies and the implementation of surveillance laws[105] The Panel has also a mandate to receive and handle individual complaints against security services. Over a two-year reporting period, the Panel received 65 petitions, 40 of which dealt with alleged surveillance measures.[106]

Oversight methods and powers: The Panel has extensive *oversight methods and powers* available to it. It applies all the standard oversight methods (review reports, hold hearings, conduct inspections). In doing so it is empowered to require the Federal Government and security services to submit files and transmit electronic data. Having access to all departments to the security services, the Panel may interview or obtain written information from staff of intelligence services, members of government agencies. In cases of non-compliance, Courts and other public authorities are required to provide official assistance to the Panel.[107] Furthermore, the Law obliges the Federal Government to proactively inform the Panel on) notable changes to Germany's foreign and domestic security situation; (b) internal administrative developments with substantial ramifications for the pursuit of the services' mandate and (c) singular events that are subject to political discussions or public reporting (art 4.1 of the Law) In addition to its broad powers to access information, the government's duty to proactively disclose information to the parliamentary oversight body constitutes good practice.

***Composition**:* The Panel is comprised of 9 members, representing all parliamentary groups in the Parliament. Embodying best practice, the members are elected by a majority of the votes in the parliament[108] which ensures broad democratic support, and enhances the legitimacy of the Panel. The members are not vetted but are sworn to secrecy. Their election by majority votes is considered as a good alternative to vetting, since it is seen as a confirmation of trust by the legislature in the professionalism, competence and discreetness of the members.[109]The chairpersonship of the Panel rotates every year between a member from the governing party and an opposition party.

Resources: The Panel is supported by substantial human resources. In addition to the staff of the Panel, the members are permitted to employ staff of their parliamentary group to assist them in their work after consulting the federal government and obtaining the approval of the Panel. As opposed to members, staff goes through vetting procedure.[110]The Panel is also entitled to contract external experts on an ad-hoc basis.

---

104 http://www.gesetze-im-internet.de/pkgrg/BJNR234610009.html

105 *EU FRA, Surveillance by Intelligence Services (2015), p.37*

106 *EU FRA, Surveillance by Intelligence Services Vol 2. (2017), p.117*

107 Hans de With and Erhard Kathmann, 'Annex A- Country Case Studies - Germany', p.220, in Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011)

108 See https://www.bundestag.de/ausschuesse/ausschuesse18/gremien18/pkgr/einfuehrung/248044

109 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.66

110 Hans de With and Erhard Kathmann, 'Annex A- Country Case Studies - Germany', p.220, in Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011)

In an attempt to further strengthen the parliamentary oversight, Germany has recently amended relevant laws and established the position of Permanent Representative, who will be entitled to conduct investigations and budget scrutiny on behalf of the Panel. The Representative shall be authorized to attend all meetings of the Panel, the Trust Panel (specialized parliamentary committee on budgetary oversight of security services) and the G10 Commission (expert oversight body), thereby enhancing coordination between the different oversight mechanisms. (art. 5a of the Law)

CANADA

Parliamentary oversight of the security services in Canada has not been referred as best practice, since there had not been a designated parliamentary committee with a mandate to oversee security services. However, in October 2017 Canada established the 'National Security and Intelligence Committee of Parliamentarians' (hereinafter the Committee) by law.[111] Although it may not be fully in line with international standards, it is still an improvement in parliamentary oversight, and is worth exploring in this section.

***Committee structure**:* Even though the Committee is composed of parliamentarians (a combination of senators and elected MPs), it is not a 'parliamentary committee' in the usual sense, since it does not belong to the Parliament institutionally (art. 4 of the Law). The Committee members are appointed by the Governor in Council (executive), on the recommendation of the Prime Minister (art.51.). The Committee reports first to the Prime Minister, who reviews the report and submits it to the Parliament. The Prime Minister can ask the Committee to revise and amend the report before submission to the Parliament. The Committee not directly reporting to the Parliament is not in line with international best practice.

Composition: The Committee is composed of 11 members (3 senators and 8 elected MPs). There is no proportional representation of parties, but the law guarantees 3 out of 8 seats for opposition party members. The Chair is appointed by the Governor in Council (executive) on the recommendation of the PM (art 5(1)), thus there is no guaranteed or rotating chairmanship for the opposition as per international best practice. Unlike the German model, the members must obtain security vetting from the government (art 10). The Committee meets only at the call of the Chair, and not regularly (art 17), which is also a sub-optimal practice. It could be said that composition and procedures leaves little room for the opposition to effectively determine and exert priorities for oversight.

Mandate The committee has a broad mandate, and tasked with overseeing 'the legislative, regulatory, policy, administrative and financial framework for national security and intelligence' as well as 'any activity carried out by a department that relates to national security or intelligence, unless the activity is an ongoing operation'. However this comprehensive oversight mandate can be obstructed if 'the appropriate Minister determines that a review would be injurious to national security' (art 8). For such an obstruction, the Minister must provide justification (art 8(2)).

***Oversight methods and powers**:* The law gives the Committee the liberty to determine the oversight methods in the exercise of its mandate (art 20). In terms of its powers, the Committee is entitled to 'have access to any information that is under the control of a government department and that is related to the fulfillment of the Committee's mandate.' (art 13(1). However this power is subjected to a number of restrictions, among which is information relating directly to an ongoing investigation carried out by a law enforcement agency that may lead to a prosecution (Art14(1)).

Resources: In compliance with international standards, the Committee is supported by a secretariat and full-time staff.

111 National Security and Intelligence Committee of Parliamentarians Act (S.C. 2017, c. 15), available from: http://laws.justice.gc.ca/eng/AnnualStatutes/2017_15/page-1.html

CROATIA

In Croatia, the Parliamentary Committee for Interior Policy and National Security is the designated body to carry out the parliamentary oversight of security services. However unlike the German and Canadian models, this Committee has a broader purview, which does not only include the security services, but also the law enforcement agencies. In line with international standards, the Committee's work is regulated by Law (the Act on the Security and Intelligence System of the Republic of Croatia.[112]

***Mandate**:* The mandate of the Committee covers reviewing the legality of activities of the services (including special measures for covert information collection), overseeing financial management and reviewing Ombudsman's report with a view to assess protection of human rights *vis a vis* activities of the security service (SOA) (art 105/1 of the Law). In addition, the Committee is mandated to receive and handle individual complaints against the SOA.[113]

***Oversight methods**:* In line with international standards, the Committee has at hand a range of oversight methods, including review of annual reports, requesting specific reports from the SOA (such as reports on the implementation of surveillance measures), hold hearings and summon the Director and officers of the service and conduct inspections to the facilities of the service. The Committee can also request the Office of the National Security Council to carry out such on-site inspections (art 104 -105). The Committee members have the right to access classified information, however they must obtain clearance certificate.[114] The only exceptions to the Committee's access to information is information on the persons with whom the SOA has collaborated to perform its functions, and the information obtained from foreign intelligence services.

***Composition**:* The Committee is composed of 13 members, chosen according to the general rules for the selection of members of parliamentary committees from members of parliament with an interest in national security matters[115] . By law, the Committee is always chaired by a member of the largest opposition party (Art 104/4), which represents best practice.

112 https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf

113 *EU FRA, Surveillance by Intelligence Services (2015), p.70*

114 Gordan Bosanac, 'Legal Update Report: Croatia' National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.9 available from: http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu

115 *EU FRA, Surveillance by Intelligence Services (2015),p.39*

Parliamentary oversight of the security service in Belgium is quite unique, in the sense that although there is a designated parliamentary committee[116] in the Chamber of Representatives (lower house of the Belgian Parliament), it does not exercise direct oversight of the security service. Instead, it monitors the work of the independent expert oversight body 'Standing Committee I' which has an exclusive mandate to oversee the security service (see the next section).

***Mandate**:* Due to its unique set-up, the mandate of the Belgian parliamentary committee is different than its counterparts in the other 3 countries. The parliamentary committee drafts and reviews bills, examines the annual activity report of the Standing Committee I and scrutinizes its draft budget, and examines the bi-annual investigation reports of the Standing Committee I, which focuses on the surveillance measures applied by the security service.[117]

***Oversight Methods and Powers**:* Resulting from its indirect oversight mandate, the parliamentary committee has rather limited powers. It can ask the Standing Committee I to issue legal advice on the draft bills that the parliamentary committee prepares or reviews.[118]

***Composition**:* The Committee is composed of 14 members of the Chamber of representatives, who are appointed by the Parliament. In line with international best practice, the Committee membership is based on proportional representation. The Speaker of the Chamber of Representatives chairs the Committee, which is currently a governing party MP. [119]

This section has provided a brief overview of international standards and selected country practices on parliamentary oversight of security services. Taking into consideration the growing volume and complexity of the work of security services, there is no doubt that parliamentary committees, by themselves, could not exercise effective oversight. In fact, there are certain drawbacks associated to parliamentary oversight. First, parliamentary committees carry an inherent risk of 'politicizing' the oversight of security services – for instance MPs from the governing party may tend to protect the services, while opposition MPs may attempt to initiate investigations of services/access information not for the sake of genuine oversight but for damaging the government. Second, MPs usually lack the time, resources and expertise to effectively oversee security services, in particular operational aspects of their work such as the use of surveillance measures.[120] While the valuable work of parliamentary committees, in particular the democratic legitimacy of their oversight cannot be disregarded or replaced, an increasing number of countries chose to establish expert oversight bodies (which often report to the Parliament) in order to strengthen the oversight of the security services.

3.2. INDEPENDENT OVERSIGHT OF SECURITY SERVICES – THE ROLE OF EXPERT OVERSIGHT BODIES AND OMBUDS INSTITUTIONS

In a strong accountability system, independent institutions such as expert bodies, ombuds institutions, data protection authorities/information commissioners, and state audit offices oversee various aspects of the work of security services. This section focuses only on the first two, the role of expert oversight bodies and ombuds institutions.

3.2.1 Expert Oversight Bodies

Over the past decade, there has been a growing tendency among democratic countries for establishing expert

116 The full title of the parliamentary committee is 'Monitoring Committee responsible for monitoring the Standing Committee P and the Standing Committee I'

117 See http://www.comiteri.be/index.php/en/39-pages-gb/307-what-is-the-difference-between-the-standing-committee-i-and-the-monitoring-committee-of-the-chamber-of-representatives-responsible-for-monitoring-the-standing-committee-p-and-the-standing-committee-i

118 Ibid.

119 Ibid.

120 Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, (DCAF: 2010), pp.42-43

oversight bodies to enhance security sector accountability. Expert oversight bodies are independent institutions set-up exclusively for the purpose of overseeing security services, operating with full-time staff who are entrusted with necessary powers and resources. In this regard, the Human Rights Commissioner of the Council of Europe stated that expert oversight bodies 'are often best placed to conduct detailed day-to-day oversight of the legality of security service activity'.[121] As of December 2017, 16 out of 28 EU member states have established such bodies. [122] Below is a brief overview of international standards on the key features of expert oversight bodies.

Institutional set up: Although the way expert oversight bodies are set-up varies, most often such bodies are appointed by the Parliament, and they report to the respective parliamentary oversight committee. This is the case for a large majority of European countries, including Belgium, and Croatia.[123] International standards suggest that being appointed by, and reporting to the Parliament enhances the legitimacy of these expert oversight bodies.[124] However, there are other models such as Canada whereby the incumbent government appoints the oversight body.

Composition: As its name suggests, expert oversight bodies are composed of specialists, often non-political and highly respected senior figures who are selected based on their expertise and qualifications. They are usually given fixed term tenures, which is an important safeguard for their independence. Since such bodies are often mandated to oversee the legality of services' activities, a common international standard is that at least one member of the body should have a legal background (senior lawyer or a former judge/prosecutor).[125] However, it is also recommended that expert oversight bodies should, to the extent possible, be composed of members with diverse backgrounds in order to effectively oversee increasingly technical and complex work of security services.[126]

Resources: Almost all expert oversight bodies are supported by a secretariat with full-time staff. In addition to the permanent staff, it is good practice to ensure that the body is able to hire external experts for short-term on an ad-hoc basis, for highly technical matters or investigations.[127]

Mandate: Mandates of expert oversight bodies vary to a certain extent depending on the remit and powers of the intelligence agencies and the role of other oversight actors in each country. However, a common standard is that such bodies are mandated to oversee the legality of the activities and policies of security services, including their compliance with human rights.[128] In this context, they are mandated to carry out specific functions such as overseeing surveillance measures, which may include:

- Ex-ante authorization/approval: Ex-ante oversight may either take the form of expert body actually authorizing the warrant or the body approving a signed warrant before it enters into force[129], thereby substituting or complementing judicial oversight
- On-going oversight: scrutinizing the information collection process, and checking compliance with the warrant,
- Ex-post oversight: reviewing the retention, use, and sharing of personal data by security services[130]

It should be noted that ex-ante authorization/approval of surveillance measures by expert oversight bodies is not yet common in EU member states. Only Germany, Belgium and Austria adopted this approach so far, while in other countries, ex-ante authorization of targeted surveillance lies with the judiciary.[131] Most expert bodies in Europe focus on ongoing and ex-post oversight of targeted surveillance measures.

---

121 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.8

122 *EU FRA, Surveillance by Intelligence Services Vol 2, (2017)* p.68

123 See the Country practices section below for details.

124 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.48 ; EU FRA, Surveillance by Intelligence Services (2015) p.43

125 Venice Commission, *Democratic Oversight of the Security Services,* (2007), para 228, Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011) p.97

126 EU FRA, Surveillance by Intelligence Services (2015)p.44

127 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.50, Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011) p. 101

128 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015) p.47

129 *EU FRA, Surveillance by Intelligence Services Vol 2. (2017)* p.94

130 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015)p. 49,

131 *EU FRA, Surveillance by Intelligence Services (2015),*p.52

Furthermore, as per UN guidance, good practices suggest that '[a]ny individual who believes that her or his rights have been infringed by an intelligence service is able to bring a complaint to a court or oversight institution, such as an ombudsman, human rights commissioner or national human rights institution'.[132] In this context, most expert oversight bodies are mandated to handle complaints against security services.

Oversight powers: The UN Compilation of Good Practices has set clear standards for powers and methods of oversight institutions:

> *'Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence.'*[133]

This important UN standard has crucial aspects, which necessitates further analysis:

Initiate own investigations: The significance of this power is also recognized by the Venice Commission, which recommends that expert bodies should be able to decide on their agenda, determine priorities for oversight, and launch investigations on their own initiative.[134] This way they are not bound by overseeing only the aspects that the government or the parliament orders them. In line with this standard most expert bodies have the power to launch own-motion investigations.

Access to information: In order to carry out their mandates effectively, expert oversight bodies should be given extensive access to information. While it is typical that the law imposes certain l restrictions to their access (for instance overseers may not be allowed to access information on the sources of security services, or on ongoing investigations) such limitations should be defined in the law in the narrowest sense, otherwise it could lead to the executive imposing arbitrary restrictions to access information, which seriously obstructs the work of expert oversight bodies. [135] An important standard that enhances oversight bodies' access to information is to legally oblige security services and the executive to proactively disclose information to the overseers [136], especially on surveillance measures. However, it should be noted that access to information comes with certain responsibilities. As per UN Compilation of Good Practices, '[O]versight institutions take all necessary measures to protect classified information and personal data to which they have access during the course of their work. Penalties are provided for the breach of these requirements by members of oversight institutions'.[137] Most commonly members and staff of such expert bodies go through security clearance procedures.

Full cooperation of intelligence and law enforcement agencies: In the framework of their mandates, most expert oversight bodies are tasked with conducting inspection to the facilities of security services, investigating complaints and scrutinizing the implementation of surveillance measures by security services. Accordingly, such expert bodies should either be given the power to compel intelligence and law enforcement cooperation in their investigations or the expert oversight body itself should be entrusted with certain investigatory powers. The absence of such powers would render the expert oversight body 'toothless', left at the willingness of intelligence services to cooperate.

As mentioned earlier, there seems to be a growing preference for expert oversight bodies. Such bodies allows for greater expertise and time in the oversight of security and intelligence services.[138] Having fixed tenures, they are able to provide continuous oversight as opposed to parliamentary oversight bodies, which in most cases stops functioning when the parliament is in recess or dissolved for election.[139] However establishing expert oversight bodies with extensive mandate and powers requires significant human and financial resources. Their mandates, power and competences should be carefully considered, in order to avoid duplication and ineffective use of resources.

---

132 UN Compilation of Good Practices, Practice 9
133 Ibid, Practice 7
134 Venice Commission, *Democratic Oversight of the Security Services* (2007), para 229
135 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p 123-124
136 Ibid, p.127
137 UN Compilation of Good Practices, Practice 8
138 Venice Commission, *Democratic Oversight of the Security Services* (2007), para 219
139 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011)), p.90

3.2.2. Ombuds Institutions

Ombuds institutions are offices established by constitution or statute, headed by an independent high-level public official who receives complaints about human rights violations and maladministration against government agencies, officials, employees or who acts on his/her own initiative on the basis of information from a wide range of sources.[140] An ombuds institution has powers to, inter alia, investigate, criticise, and provide recommendations for relevant authorities, as well as to propose new laws or amendments to existing legislation. The **Principles relating to the Status of National Institutions (The Paris Principles)** are considered as the leading normative instrument concerning the mandate, powers, composition and scope of the work of the national human rights institutions, which apply to many ombuds institutions. According to **the Paris Principles**, such institutions should:

- Be vested with a broad mandate;
- Be responsible to submit upon request or on the institution's own initiative, opinions, recommendations, proposals and reports on any matters concerning the protection and promotion of human rights in relation to legislative, administrative, judicial provisions, or any situation in which human rights may have been violated;
- Have the mandate to draw the attention of the Government to situations in any part of the country where human rights are violated and to submit to the Government proposals for initiatives to put an end to such situations and, where necessary, express an opinion on the positions and reactions of the Government;
- Freely consider any questions falling within their competence, hear any person and obtain any information necessary to make an assessment of situations falling within their competence and publicize its opinions and recommendations.[141]

Typically the mandate of ombuds institutions covers all government agencies, including the security services. In the countries where there are no expert bodies to oversee the security services, ombuds institutions can carry out some similar functions, such as handling complaints and conducting inspections. However, in practice, most ombuds institutions in Europe do not take the lead in overseeing the security services (amongst independent institutions), apart from a few examples such as the Serbian Ombudsman or the Finnish Parliamentary Ombudsman, the latter of which is specifically tasked with overseeing covert information collection methods and undercover operations.[142] There are three main reasons for this. First, as stated above, more and more European countries have established expert oversight bodies with extensive mandate and powers to monitor the services. In those countries, ombuds institutions play a secondary role, complementing the work of the expert oversight bodies. Second, almost all European countries established data protection authorities (DPA), which, in some cases, partly took over competences on inspecting facilities of security services and their data files.[143] Third, ombuds institutions may not have sufficient expertise and resources to oversee the highly complex and technical work of security services.

Nevertheless, this does not mean that ombuds institutions cannot or do not play a role in the oversight of security services. Below are some examples of the ways in which ombuds institutions contribute to the accountability of security services:

- Reviewing laws and policies concerning security services with a view to assess their compliance with international human rights standards. Issuing recommendations to the government and parliament concerning amendments.
- Challenging the legal basis of security service activities (for instance surveillance laws) at court,
- Conducting investigations (either based upon individual complaints or thematic investigations concerning the work of security services); cooperating with other oversight actors where necessary (expert bodies, DPAs, judiciary);
- Launching awareness raising/advocacy activities aiming to inform the public on the extent of security services' work and potential risks to fundamental human rights[144]

---

140 The Parliamentary Ombudsman of Malta, Frequently Asked Questions, available from: http://www.ombudsman.org.mt/how-can-one-define-the-ombudsman-institution/

141 *The Paris Principles*, Principles 1-3, available from: http://www.ohchr.org/EN/ProfessionalInterest/Pages/StatusOfNationalInstitutions.aspx

142 https://www.oikeusasiamies.fi/en_GB/web/guest/the-tasks-of-the-ombudsman

143 Mandate and powers of DPAs in the EU vary. Some countries entrust DPAs with powers to oversee security services, others exclude security services from the mandate of DPAs. See *EU FRA, Surveillance by Intelligence Services (2015), p.50*

144 For more information on ombuds institutions in overseeing security services, see Nazli Yildirim Schierkolk, Monitoring Security Services: A Guide for Ombuds Institutions (DCAF, forthcoming 2018).

PRACTICES IN SELECTED COUNTRIES

CROATIA

In 2006, Croatia established an expert oversight body, entitled the '*Council for the Civilian Oversight of the Security Intelligence Agencies* (hereinafter Council). The Law on the Security Intelligence System of the Republic of Croatia[145] (hereinafter the Law) regulates its mandate and powers.

Institutional set-up*:* The Council is appointed by and accountable to the Parliament. The Parliamentary Committee for Interior Policy and National Security is tasked with overseeing the work of the Council (art. 110 of the Law). The Council reports to the Parliament, at the request of the Speaker, as well as twice a year regularly. While this institutional set-up is in line with international standards, one sub-optimal practice is that the members of the Council are not allowed to make public statements, without previous approval of the parliamentary committee.[146] Such a rule carries the risk of rendering the Council too dependent on a political body, which jeopardizes its independence.

Composition: The Council is composed of a chairperson and six members, all appointed by the Croatian Parliament, on the basis of a public call and selection based on qualifications. Representing international best practice, the law requires that members must include at least one who has a degree in law, another in political sciences, and the third in electro/technical sciences (art. 100). Neither the chairperson nor members of the Council may be members of the top leadership of any political party.[147] Members are obliged by law to main the confidentiality of information they obtained while performing their work (art. 114).

Mandate: In compliance with international standards, the Council is mandated to oversee the legality of the work of the security services as well as to monitor and supervise the application of surveillance measures. The Council is also mandated to receive and handle complaints concerning unlawful procedures or misconduct of security and intelligence agencies, particularly in the case of violations of human rights and fundamental freedoms (art. 112).

One concerning issue regarding the Council's mandate is that, while it has the authority to monitor the application of surveillance related measures by the Croatian security service (SOA), the Council's mandate does not extend to the institution that actually conducts interceptions, the Operation Technology Centre for Telecommunication Surveillance (OTC). This is because the OTC is not part of the security service, it is a distinct institution overseen by the Office of the National Security Council (art 8).

Powers: In exercising its mandate, the Council has the power to launch investigation upon complaints and at the request of any state body. In doing so, the Council may review the reports and other documents of security and intelligence agencies and conduct interviews with the heads and other officers of security and intelligence agencies.[148] However, it is not entitled to launch investigations at its own initiative, thus lacking an essential power as per international standards. Upon investigations, if the Council establishes irregularities or unlawful actions by the security services, it informs the President, PM, Speaker of the Parliament, chief Public Attorney (art. 113).

The ***Croatian Ombudsman*** is also mandated to 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.[149]

---

145 https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf

146 Gordan Bosanac, 'Legal Update Report: Croatia' National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.12

147 See Council for Civilian Oversight of Security and Intelligence Agencies, Fact Sheet, available from http://www.sabor.hr/0060

148 See Council for Civilian Oversight of Security and Intelligence Agencies, Fact Sheet

149 Gordan Bosanac, 'Legal Update Report: Croatia' National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.12

BELGIUM

Belgium embodies one of the most advanced models of expert oversight, with two separate bodies (the Administrative Commission, and the Standing Intelligence Oversight Committee- hereinafter the Committee I), which have broad mandates and powers for overseeing the security services.

The Administrative Commission: This body, composed of a state prosecutor and two judges, is mandated to scrutinize the legality and proportionality of specific and exceptional data collection methods used by the security services.[150] The security service, must submit a duly motivated, written request to the Administrative Commission before using exceptional surveillance methods. The methods can only be implemented after the Commission's approval[151]. Therefore, in the Belgian model, an expert oversight body with a quasi-judicial function is in charge of the ex-ante authorization of surveillance methods.

The Standing Intelligence Oversight Committee: The Committee I is one of the pioneers in the area of expert oversight, and has been repeatedly referred as representing best practices.[152]

Institutional set-up*:* As mentioned in the previous section, the Committee I is appointed by the Parliament and reports to a designated parliamentary committee in the Chamber of Representatives. The Parliamentary Committee oversees the work of the Committee through reviewing its annual reports, special reports on investigations and scrutinizing its budget. However, contrary to the Croatian model, the Committee I may decide to make all, or part, of its investigation reports public.[153] This constitutes best practice: while the expert oversight body is overseen by a parliamentary committee, it is not 'controlled' by it. It decides autonomously, what to communicate to the public.

Composition*:* The Committee I is composed of two members and a chairperson, all appointed by the Parliament. In compliance with international standards, they have a renewable tenure term, and the chairperson must be a judge. All employees of the Committee hold a top secret level security clearance.

Resources**:** The Committee I is supported by fifteen administrative staff and a secretary, who is responsible for administrative work of the Committee, protecting the secrecy of documents and archiving them as well as managing the staff. Representing best practice, the Committee has its own team of five investigators, who have police powers when investigating the security services. Furthermore, the Committee I is entitled to contract short –term experts for carrying out special investigations or tasks. For instance, following the Snowden revelations, the Committee called on outside expertise to conduct a number of inquires.[154]

Mandate: The Committee I is in charge of overseeing both the 'State Security' (civilian securtiy service) and The General Intelligence and Security Service (military intelligence agency). Overall, it has an extensive mandate, which covers overseeing the legitimacy (review of observance of the applicable laws and regulations), effectiveness (supervision of the efficiency of the intelligence services), and coordination (the mutual harmonization of the work of the services concerned). In the frame of its broad mandate, it carries out the following specific functions:

- Upon request, it reviews and provides advice on laws, or any other policy documents relating to the governance of security services. Furthermore, it also provides written advice to the judicial authorities on the legality of the way in which information added to criminal proceedings was collected by the intelligence and security services;
- Conducts ex-post oversight of the implementation of targeted surveillance measures, while the Administrative Commission is in charge of ex-ante authorizations.
- Oversees strategic surveillance conducted abroad by the military intelligence agency. It should be noted that very few oversight bodies have the explicit mandate to oversee strategic surveillance carried out in foreign

150 *EU FRA Surveillance by Intelligence Services (2015), p.43*

151 *EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.94*

152 Except otherwise indicated, all information in this section is retrieved from the official website of the Committee: http://www.comiteri.be/index.php/en/standing-committee-i/competences

153 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.20

154 Ibid. p.11

countries. Furthermore, the Committee also oversees the security services' cooperation with their international counterparts, which is a novel approach among expert oversight bodies.

- Upon complaints, requests by the Parliament or judicial authorities, carries out investigations, including investigations against members of the services who are suspected of having committed a felony or misdemeanor,
- Serves as an appeal body for security clearances.

Powers: In order to carry out the extensive mandate explained above, the Committee is entrusted with exceptional powers.

- The Committee enjoys almost unlimited access to information, including those related to ongoing intelligence operations (which is typically not the case for most oversight bodies). The Committee's unfettered access to information is further enhanced by the executive's legal obligation to proactively disclose internal rules and directives, as well as all documents regulating the conduct of the members of these services. Most importantly, the Committee has its own facilities on the premises of the intelligence agencies, which allows them to access directly to the databases of the security services.[155] Belgium is one of the two countries in Europe which gave its expert oversight body this extraordinary power.
- Representing international best practice, the Committee is entitled to launch investigations on its own initiative. In carrying out the investigations, the Committee has *judicial powers,* including subpoenaing anybody, in particular intelligence officers; seizing objects and documents in any location, and compel the assistance of the police and experts.
- When conducting the oversight of surveillance measures, the Committee can:
  - Overrule a positive decision by the Administrative Commission on a surveillance request[156] or
  - If the Committee finds that the security services have broken the law while surveilling the individual concerned, it has the *power to order the cessation of the surveillance method*.[157]

Ombuds institution: Since Belgium has two strong expert oversight bodies, the Belgian Ombudsman plays a more secondary role. The Ombudsman is mandated to receive complaints and handle complaints. One important function of the Ombudsman is that he/she assesses the complaint, and filters the irrelevant, frivolous or baseless complaints. The Ombudsman only refers the well-grounded complaints to the Committee I, which is in charge of investigating complaints. Such cooperation between oversight institutions serves to enhance efficiency and effectiveness of the accountability system.[158]

155 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p.134

156 *EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.94*

157 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.17

158 *EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.132*

CANADA

Canada has established the 'Security Intelligence Review Committee'[159] (hereinafter the SIRC) in 1984, with the 'Canadian Security Intelligence Act' (hereinafter the Law). The SIRC is often regarded as a pioneer, and has been a source of inspiration for various European countries in creating their own expert oversight bodies.[160]

***Institutional set-up**:* The SIRC is an independent review body appointed by the executive; reporting to the Parliament on an annual basis. The report includes unclassified summaries of the SIRC findings and recommendations, as well as the Canadian Security Intelligence Service's responses to those recommendations.

***Composition**:* The SIRC is composed of five members headed by an executive director. As opposed to the European models, all members are appointed by the Governor in Council (a position in the executive), in consultation with the Prime Minister and the leaders of opposition parties. By law, members of the SIRC cannot be current Senators or MPs. In line with international standards, members have a fixed, five-year tenure with possibility of renewal. (Art 34 of the Law) All members and staff are bound by a permanent oath to secrecy.

***Resources**:* A team of full-time researchers and legal staff is supporting the work of the Committee. However the Law does not prescribe the possibility of contracting external experts for complex, technical investigations. Since the size of the Committee is considerably small compared to the ever-expanding size of the security service, the SIRC carries out risk assessments to determine their priorities for oversight.

***Mandate**:* As opposed to the Belgian model, the SIRC's mandate covers only one agency, the civilian security service. It has a broad mandate, including overseeing the service's compliance with the law, policies and internal regulations, scrutinizing the activities of the service and investigating complaints. Furthermore, the law gives the SIRC an explicit mandate to review international information sharing agreements, which represents best practice.

Powers: In compliance with international standards, the SIRC has near absolute access to information; which the law describes as 'any information which the SIRC deems necessary for the performance of its duties and functions' (Art 39(2)) no matter how sensitive and no matter how classified that information may be. The only exception to it access to information is deliberations among Ministers. The SIRC's power to access to information is further strengthened by the security service's and the Ministry's legal obligation to proactively disclose a number of documents including updates to internal operational guidelines, changes to the policy guidance, and any document sent to the Attorney General regarding an unlawful conduct of an employee.

Complying with international standards, the SIRC is entitled to launch review and investigations on its own initiative or upon complaints. In conducting investigations, the SIRC has judicial powers to the same extent as a superior court; such as summoning and enforcing appearance of persons, summoning written documents and evidence, administering oaths and so forth (Art 50). Another notable power of the SIRC is that it can 'direct' the security service to conduct a review of the service's activities and report the findings to the SIRC.

***Ombuds institution*:** The Canadian Human Rights Commission at the federal level is mandated to handle complaints against all federal agencies, including the security service. The Law permits the SIRC to cooperate with the Human Rights Commission during investigations, which is another good practice. Some ombuds institutions at the Provincial level are also active in raising awareness on privacy, protection of personal data, and transparency of government agencies.[161]

159 Unless otherwise indicated, the information in this section is retrieved from: http://www.sirc-csars.gc.ca/abtprp/index-eng.html

160 Venice Commission, *Democratic Oversight of the Security Services, (2007), para 220*

161 See for instance the Manitoba Ombudsman http://www.theioi.org/ioi-news/current-news/ombudsman-celebrates-right-to-know-week

GERMANY

In late 2016, Germany reformed its legislative framework to further strengthen the oversight of its security services. In addition to its internationally renowned expert oversight body, the **G-10 Commission**; the new laws established a second expert oversight body, the **Independent Committee** (Unabhängiges Gremium), tasked with the particular mandate to oversee foreign-foreign communications surveillance. This section will focus primarily on the G-10 Commission, where necessary, references will be made to the Independent Committee.

Institutional set-up*:* The G-10 commission is an expert oversight body, appointed by the German parliamentary oversight committee, the Parliamentary Control Panel (G-10 Law[162], art 15/ 1). Although the Law stipulates that the G-10 Commission and the Parliamentary Control Panel shall regularly exchange information, there is no legal obligation for the G-10 Commission to report to the Parliamentary Control Panel. The Independent Committee is appointed by the Federal Government and is located at the Federal Court of Justice, however the Committee also reports bi-annually to the Parliamentary Control Panel (BND Law[163], art 16(6)).

Composition: The G-10 Commission is composed of four members, appointed by the Parliamentary control Panel upon consultation with the Federal Government (G-10 Law, art 15/ 1). In compliance with international standards, the Chairperson must be qualified for judicial office. As opposed to the Canadian model, there is no restriction for membership on current MPs; they can be appointed to the G10 commission. The Independent Committee is composed of three members, two federal judges and one prosecutor who are appointed by the Federal Government, following recommendations by the Federal Court of Justice and the Public Prosecutor General.[164]

Resources*:* The G-10 Commission is supported by secretariat with full time staff, whose number has been increased from 6 to 13, in the context of recent reforms.[165] Both members and staff of the Commission are under the obligation of confidentiality, even after the end of their term/assignment; which is a common practice.

Mandate: Both the G-10 Commission's and the Independent Committee's mandates relate to the oversight of surveillance measures. The scope of the G-10 Commission's mandate covers the surveillance of all domestic communications, as well as communications originating or ending in Germany. In this framework, as per the G-10 law, the G-10 Commission carries out three core functions:

- Ex-ante approval of surveillance measures: The security services submit the surveillance request to the Interior Ministry. If the Ministry approves the request, it issues the warrant and submits it to the G-10 commission for approval. For strategic (mass) surveillance, the G-10 Commission reviews the search terms (selectors), the area of information collection, the communication channels and the maximum share of communication to be intercepted. Only after the G-10 commission's approval, can the surveillance measure be implemented (except emergency situations defined by the G-10 law).[166] This function makes the G-10 Commission a quasi-judicial body.
- Oversee the entire processes of collection, handling and the use of personal data by security services; and
- Receive and investigate complaints against services with respect to surveillance practices and protection of personal data

On the other hand, the Independent Committee is exclusively tasked with overseeing the legality and necessity of foreign –foreign strategic communications surveillance, conducted by the BND.[167] In doing so, the Committee is given ex-ante authorization powers, whereby it approves the 'selectors' for intercepting the foreign-foreign

162 https://www.gesetze-im-internet.de/g10_2001/index.html
163 https://www.gesetze-im-internet.de/bndg/
164 German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.7
165 Ibid., p.18
166 Thorsten Wetzling, SNV Policy Brief: 'The Key to Intelligence Reform in Germany- Strengthening the G-10 Commission's role to authorize strategic surveillance' 2016, p.9 available from: : https://www.stiftung-nv.de/en/project/digital-basic-rights-surveillance-and-transparency/publikationen
167 *EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.67*

communications.[168] Germany is one of the first countries, which has developed a comprehensive legal framework on foreign surveillance and established a separate expert body exclusively for this task.

***Powers**:* In order to effectively carry out its extensive mandate, the G-10 commission is entrusted with broad powers to access all documentation, information (including stored data and computer programs for surveillance), which the Commission deems relevant to its investigations; as well as the premises of security services at all times. (G10 Law, art. 15/5). As part of its judicial capacity, the G-10 commission can take binding decisions. In particular, similar to the Belgian Standing Committee I, if the G-10 Commission establishes that legal conditions for a surveillance measure has not been met, it can declare the measure unlawful, and order its immediate termination.[169]

Ombuds institution: There is no ombudsman at the federal level in Germany. However, the Parliamentary Petitions Committee serves a similar function to an ombuds institution, and receives complaints concerning all federal agencies, including the security services. Similar to the Belgian Ombudsman, the Petitions Committee acts as a filter, and forwards the complaints with a reasonable ground for investigation to the Parliamentary Control Panel. The Panel has the power to investigate the complaints itself or refers them to the G-10 Commission, especially if they require technical expertise.[170]

3.3 JUDICIAL OVERSIGHT OF SECURITY SERVICES

The judiciary is an indispensible element of the accountability system. Indeed, international actors including the UN rapporteurs, CoE Venice Commission and the Human Rights Commissioner, as well as the EU have reiterated the importance of- and necessity for the judicial oversight of security services. In its landmark ruling, the ECtHR stated that:

> "The rule of law implies, inter alia that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure"[171]

Similarly, the CoE Venice Commission stated that:

> "Judicial authorization requirements subordinate security concerns to the law, and thereby institutionalize the respect for the law."[172]

Although the extent of the judiciary's involvement differs in each country, most commonly it has a role in ex-ante authorization of security sector activities infringing on human rights and adjudicates on cases against security services upon complaints and provides remedies. Beyond these core functions, in some countries the judiciary is also involved in supervising ongoing surveillance activities. However, according to a comparative research by EU FRA, oversight by the judiciary during the implementation of surveillance measures is uncommon, since most Member States mandate an independent oversight body for that task. [173]

Ex-ante authorization of information collection measures:

Security services apply a number of methods to collect information to produce intelligence; including, inter alia, undercover operations using human sources, covert surveillance of communications (post, telephone and electronic communications) as well as direct access to data through computer hacking and searching pre-existing databanks. In most Council of Europe member states, the judiciary does not conduct ex-ante authorization of *all* such measures, but rather focuses largely on surveillance of communications. [174]

---

168 German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.7

169 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), p.223

170 German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.21

171 Klass v. FRG http://hudoc.echr.coe.int/eng?i=001-57510 para 55

172 Venice Cmmission, *Democratic Oversight of the Security Services* (2007) para 204

173 *EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.97*

174 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.54

- *Ex-ante authorization of targeted surveillance of communications:* Targeted surveillance of communications is an extreme measure, seriously infringing on privacy rights. Therefore in the majority of EU and CoE countries, the judiciary is in charge of authorizing targeted communications surveillance requests.[175]The remaining states either entrusted a quasi-judicial expert body (e.g. Germany, Belgium, see below) or entrusted their executive with this power. The main rationale behind the judicial authorization is that, judges are considered to be best suited to assess the legality, necessity and proportionality of such measures. However there are certain international standards to ensure the effectiveness of judicial authorization:

  - Warrant applications: Typically security services draft the request for surveillance warrants, which are then submitted to courts. In order that judges could exercise meaningful review, warrants should include at least:

    - The subject/target of surveillance and an outline of the facility and location of surveillance;
    - The necessary duration of the surveillance (it is good practice that the legislation explicitly stipulates the limits. The duration varies between jurisdictions which regulate this, and ranges from 10 days to three months)
    - The justification for the use of surveillance (an outline of why less intrusive methods cannot be used)[176]

  - Expertise of judges: The effectiveness of judicial oversight depends very much on the expertise of judges in evaluating risks to national security and in balancing these risks against infringements upon fundamental rights.[177] When ordinary courts are mandated to authorize surveillance, judges who are not experienced in such matters may not be able to critically assess the warrant requests coming from the services.[178]Therefore, international good practices suggest that a high- ranking judge or a panel of judges should be given the mandate to authorize warrants. By way of example, in Portugal, authorization is provided by a judicial panel composed of the presidents of all criminal sections of the Supreme Court and a judge appointed by the Superior Council of Magistrates.[179] Another good standard is to provide judges with specialized training on authorization procedures and surveillance methods.[180]

  - Reasoned decisions: If and when judges do not possess sufficient expertise or experience in national security and human rights related matters, they may tend to rubber-stamp the warrant requests coming from the security services. Same behavior is also observed in the contexts where judiciary is not sufficiently independent from the executive. An important safeguard to avoid rubber-stamping is to require reasoned decisions for each warrant application, which ensures that judges take the time to review and assess the merits before authorizing targeted surveillance measures.[181]

  - Security cleared lawyers: The procedure for authorizing warrants is necessarily ex-parte, meaning that they are done on the application of one party alone (security services), without the representation of the other part (person who is the target of surveillance). It is therefore challenging to the judiciary to give an impartial decision. An emerging and promising international standard to nhance human rights protection is to involve a security-cleared lawyer in the authorization processes, who represents the interests of the would-be target of surveillance measures. The lawyer can question the evidence and justification for intrusive surveillance, but he/she can obviously not contact the would-be target, in order to get further information[182]. Norway has already adopted this novel approach in the authorization of surveillance.[183]

- *Emergency situations:* In addition to stipulating the procedures for the ex-ante authorization of targeted surveillance, it is good practice that national laws establish clear rules to be followed in situations of extreme urgency, in which waiting for judicial authorization may pose grave risks to national security. According to

---

175 In 19 out of 28 EU member states, the judiciary is in charge. See *EU FRA Surveillance by Intelligence Services Vol 2.*, p.95. For CoE countries, see Council of Europe*, Democratic and Effective Oversight of National Security Services*, (2015)„ p.53

176 UNODC, 'Current practices in electronic surveillance in the investigation of serious and organized crime' (New York, 2009, p.17

177 Venice Commission, *Democratic Oversight of the Security Services,* (2007), para 15 ;

178 Council of Europe, *Democratic and Effective Oversight of National Security Services,* (2015), p.55

179 *EU FRA, Surveillance by Intelligence Services Vol 2. (2017)*, p. 96

180 Venice Commission, *Democratic Oversight of the Security Services,* 2007, para 211

181 *EU FRA Surveillance by Intelligence Services (2015)*, p.54

182 Ibid para 214

183 Council of Europe*, Democratic and Effective Oversight of National Security Services*, (2015),p.55

the ECtHR case law, in such circumstances, security services may proceed with surveillance measures for a maximum of 72 hours. However, such measures should be subject to a post-factum review by the judiciary. [184]

- *Ex-ante authorization of mass surveillance:* As explained earlier, mass surveillance does not depend on a suspicion against an individual. It is therefore more difficult for the judiciary to oversee mass surveillance measures. In the regard, the UN Rapporteur stated:

  - 'With targeted surveillance, it is possible to make an objective assessment of the necessity and proportionality of the contemplated surveillance, weighing the degree of the proposed intrusion against its anticipated value to a particular investigation. However, **bulk access to digital communications** does not allow for an individualized proportionality analysis, and "[e]x-ante security is therefore possible only at the highest level of generality"[185]

  Nevertheless, as per international standards, the ex-ante authorization of mass surveillance shall focus on reviewing the severity and seriousness of the operation as an intelligence requirement, the level of proportionality (to the extent possible), and the use of selectors (keywords) and other filtering algorithms to ensure that they are not applied in a discriminatory manner. [186]

On-going oversight of information collection measures:

As mentioned earlier, judiciary's involvement (in a supervisory capacity) during the implementation of surveillance measures is not common in Europe. Instead, independent oversight bodies (in some countries, bodies with quasi judicial functions) are tasked with ongoing review of surveillance measures, carrying out investigations and inspections, and scrutinizing the processing, maintenance and destruction of personal data.

Nevertheless, there are two key powers that should be given to the authority supervising the implementation of surveillance measures.

- *Order the termination of surveillance:* If the body in charge of supervising the surveillance measures identifies a violation of the law, it should be able to order the immediate termination of surveillance measures. As per the ECtHR case law, this power is essential for an effective oversight system. [187]

- *Order the destruction of data collected:* In cases where the oversight body establishes unlawful surveillance and orders its termination, it should also be able to order the destruction of the data collected unlawfully.

There is one important caveat with respect to the destruction of data. Beyond the cases of unlawful collection, intelligence services are expected to regularly review the personal data they hold and delete any information that is not relevant to their mandate anymore. However the deletion of data can also be detrimental to the work of oversight bodies or judicial proceedings. Therefore, as per UN guidance, it is good practice that the deletion of any such information is supervised by an external institution.[188]

Adjudication

Apart from ex-ante authorization, the judiciary has an essential function of adjudicating cases concerning the activities or legal basis of security services. Cases could be brought before a court by the target of surveillance (persons can find out about surveillance through ex-post notification procedures, whistleblowers and stories on the media or they may simply have a suspicion). Courts provide an avenue for persons to complain about infringement into their privacy and to seek a remedy. In this context judges establish whether the complainant's communications were indeed monitored, and if so whether the measures were lawful, necessary and proportional to the suspicion/threat posed. Challenges similar to the authorization processes apply here: judges should have the necessary experience, expertise and the power to access classified materials to examine the merits of the case. When low-level ordinary courts with limited access to confidential info are mandated, the services may be inclined to give 'neither deny nor confirm' responses. In this regard a good standard is to establish specialised tribunals,

184 ECtHR, Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 81
185 UN, Human Rights Council, Emmerson, B. (2014), para. 7
186 *EU FRA, Surveillance by Intelligence Services Vol 2, (2017)*, p.96
187 *ECtHR,* Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015,* para. 28
188 UN Compilation of Good Practices, Practices 24-25

where judges have the knowledge and expertise to decide on technical matters and are also allowed to access secret material. [189] The UK's Investigatory Powers Tribunal (IPT), a special judicial body with exclusive jurisdiction on handling complaints about surveillance and all human rights-related claims against the security services, which can investigate ongoing surveillance measures, is a good example of this standard.[190]

Courts also adjudicate on cases that were brought by NGOs or other relevant stakeholders, which are not necessarily based on a complaint, but rather challenging the legal basis or activities of the security services in more general terms. By adjudicating on such cases, the judiciary set important standards for the work of security services, which may even lead to changes to legislation or government policies.

This section briefly outlined the role of the judiciary in overseeing the security services, as well as explained some of the challenges associated with judicial authorization and litigation processes. Acknowledging such challenges, international actors have been increasingly calling for a multi-layered approach for the authorization of surveillance, including the executive, judiciary and expert oversight bodies covering different types and stages of surveillance. The next subsection provides an overview of country models.

189 *EU FRA Surveillance by Intelligence Services (2015)*, p.66

190 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015, p.53

CROATIA

Ex-ante authorization of targeted surveillance:

As per the Act on the Security Intelligence System of the Republic of Croatia (hereinafter the Law) in the authorization of targeted surveillance, the director of the security service (SOA) and the judiciary share competences. The following measures are authorized by the Director of the SOA: a) surveillance of telecommunication traffic data, b) surveillance of the location of the user *(a and b indicating metadata)* c) surveillance of international telecommunications d) secret purchase of documents and objects (art. 33 (3)). While the director approves such measures, he/she is also legally obliged to report to the Office of the National Security Council on a monthly basis. With respect to the secret purchase of documents and objects, the Director of the security service should also report on a monthly basis to the Chief Public Prosecutor (art.38(2)).

The following surveillance measures, which are more intrusive than those aforementioned above, require ex-ante judicial authorization: a) surveillance of the communication content, b) surveillance of posts, c) surveillance of facilities and closed spaces (bugging), and d) audio recording of communications between persons in open and public spaces.

In compliance with international standards, the Law stipulates in detail the required information for warrant requests, as well as the maximum duration for surveillance (Although it should be noted that the maximum duration (4 months) is longer than average) (art. 36 -37 of the Law). Surveillance measures are authorized by a judge of the Supreme Court of Croatia. When it comes to the extension of surveillance measures, Croatia represents best practice whereby extensions are authorized by a panel composed of three authorized judges of the Supreme Court. It is recommended to apply a stricter criteria and a higher level of control for requests on extending the duration of surveillance measures, in order to prevent the services from attempting to extend such intrusive measures unnecessarily.

Also in line with the international standards, surveillance without judicial authorization in extreme circumstances is limited to 24 hours (art 36(2) of the Law).

On-going oversight of surveillance measures: The Law does not give the judiciary the task of supervising the implementation of surveillance measures. Instead, the Council for Civic Oversight of Security and Intelligence Agencies, and the Croatian Personal Data Protection agency have the mandate to oversee the implementation of surveillance measures, through investigating complaints, launching thematic reviews or on-site inspections. Representing best practice, the decisions of the Croatian Personal Data Protection Agency are binding.[191]

191 See *EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.115*

Ex- ante authorization of targeted surveillance measures

Canada adopted a double approval system, whereby warrant applications drafted by the security service (CSIS) should be first approved by the Minister, and then submitted to the judiciary. The Canadian intelligence law has a comprehensive section, entitled 'Judicial Control' in which the ex-ante authorization processes are stipulated in detail. It should be noted that the law allows the CSIS to conduct surveillance operations both domestically and abroad. In any case, a judicial warrant is required. The CSIS Law[192] is an example of best practice since it stipulates in detail what a warrant request should include, namely: (section 21(2) of the Law)

- The facts relied on to justify the belief that a warrant would enable the CSIS to perform its duties;
- Justification that other less intrusive methods are failed or unlikely to succeed
- The type of communication proposed to be intercepted, the type of information, records, documents or things proposed to be obtained and the powers referred
- Identity of the subject of surveillance and the proposed period
- General description of place where Surveillance measures will be carried out
- Information on any previous application concerning the target of the surveillance

Surveillance measures that need judicial authorization include: interception of any communications or obtaining any information, record, document or thing and, for that purpose (i) entering any place or obtaining access to anything, (II) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing (III) to install, maintain or remove anything (section 21(3)).

In compliance with international standards, warrant applications are reviewed by a high level judge at the Federal Court. Renewal of warrants are also subjected to double approval by Minister responsible for CSIS and the federal court judge. The renewal of surveillance warrants that allow measures to reduce threats to the security of Canada is restricted; they can only be renewed twice (Section 22). This practice of limiting the renewal of surveillance measures for less concrete threats, can be considered as good practice.

In terms of protection of the rights of the surveillance target, the law does not have any provisions concerning a security cleared lawyer who would defend the target and critically question the basis of warrant requests at judicial hearings. However, civil society actors have been calling for the latter.[193]

Adjudication

Even though the Canadian law requires a double approval and a detailed warrant applications, there is always a risk that the security service misuses the surveillance powers obtained through the warrant. Adjudication of the Court ensures remedy and sets standards for the future. Upon complaint of an individual, the Federal Court reviewed the surveillance practices of CSIS and found that the CSIS did not accurately inform the Court on a powerful data collection program; which collected and retained metadata and non-threat related information of individuals over ten years. The Court has thus ruled that the retention of such data was illegal. Both the CSIS director and the Minister for Public Safety accepted the failure, and pledged to take all action necessary, including immediate blocking of access to the aforementioned data.[194]

192 Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23) available from: http://laws-lois.justice.gc.ca/eng/acts/c-23/index.html

193 https://ablawg.ca/wp-content/uploads/2016/12/Blog_CSIS_Warrants.pdf

194 See http://www.cbc.ca/news/politics/csis-metadata-ruling-1.3835472 https://www.documentcloud.org/documents/3213882-DES-Warrant-Nov-3-2016-Media-Summary-FINAL.html

Germany is one of the few countries in Europe, where the judiciary does not play a role in authorizing surveillance methods. Instead, Germany has established two quasi-judicial bodies in charge of inter alia, authorizing various types of surveillance. Both the BfV (domestic security service) and the BND (foreign intelligence service) are mandated to apply varying degrees of surveillance measures. The complex, yet fragmented system is very briefly outlined below:

Ex- ante authorization of targeted surveillance

Firstly, embodying good practice, the German G-10 law explicitly lists the categories of people who can be subjected to targeted surveillance. (G-10 Law, 1.3.11) The services (BfV and BND) draft a warrant request, and submits it to the Federal Ministry of Interior. If the Ministry finds that there are reasonable grounds for requesting surveillance measures, then it submits the request to the G-10 Commission. The G-10 Commission, a quasi-judicial body of the Parliament (for more information chapters 3.1. and 3.2.) gathers once a month and reviews the legality and necessity of all warrant requests. The surveillance measures can only be undertaken after the authorization by the G-10 commission. However, in emergency situations, surveillance measures can be implemented without G-10 commission's authorization, provided that retrospective authorization is sought without delay. Targeted surveillance measures last for a maximum of 3 months, and extension is subjected to the same procedures.[195]

Ex-ante authorization of strategic (mass) surveillance

Embodying best practice in the field, Germany has adopted detailed legislation regulating the BND's strategic surveillance practices. As a pioneer in this field, German legislation regulates not only domestic-foreign strategic surveillance (surveillance of communications, at least one –end of which takes place in Germany) but also foreign-foreign strategic surveillance (BND's surveillance of foreign-to foreign communications).

► Ex-ante authorization of domestic- foreign strategic surveillance

In this case, the BND drafts the warrant request, which includes the selectors (search terms to filter the mass data acquired) and submits the request to the Federal Ministry of Interior. The Ministry, after obtaining the consent of the Parliamentary Control Panel, submits the request to the G-10 Commission. Only after the Commission's review and its positive decision, can the strategic surveillance be applied. In emergency cases, surveillance measure can start before the G 10 Commission's approval but the data cannot be used[196], which represents best practice. With regards to mass surveillance, the G10 Commission also oversees the minimization of data obtained through surveillance measures.[197] As can be seen, German models adopts a multi-layered authorization system for mass surveillance, including the executive, parliament and the expert bodies.[198]

► *Ex-ante authorization of foreign-foreign strategic surveillance*

With the most recent intelligence reforms, Germany has amended its legislation to also regulate foreign-foreign strategic surveillance and for that purpose created a new quasi-judicial expert body (The Independent Committee, see sections 3.1. and 3.2) with exclusive mandate to authorize and oversee such surveillance measures. The BND submits surveillance requests to the Chancellery, which reviews and submits it to the Independent Committee for authorization. Composed of two judges and a public prosecutor, this quasi-judicial body gathers every three months, and with limited access to the proposed search terms, reviews the surveillance request. Foreign- foreign surveillance can only take place after the Committee's authorization.[199]

---

195 Hans de With and Erhard Kathmann, 'Annex A- Country Case Studies - Germany', p.223, in Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), Also see G-10 Law, article 10

196 *EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.99*

197 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.57

198 For more information, see Thorsten Wetzling, Germany's Intelligence Reform: More surveillance, modest restraints and inefficient controls' SNV Policy Brief (2017), p.8

199 Ibid.

Germany has not yet introduced the security –cleared lawyer system in either of the quasi judicial bodies, but the civil society has been actively calling for it.[200]

Ongoing and Ex-post oversight by quasi judicial bodies

Germany's both quasi-judicial bodies (G-10 commission and the Independent Committee) have the mandate to conduct ongoing and ex-post overview of the BfV and the BND. The G-10 Commission's supervisory powers shall covers the entire scope of collection, processing and use of the personal data. In line with international best practice, the G-10 Commission, at any point of its overview process, can decide on the immediate end of surveillance measures which it deems unlawful or unnecessary.[201]

The –G-10 law includes detailed provisions for the deletion of data. The BfV is obliged to review the accuracy and relevance of personal data it holds every 6 months. If data is found inaccurate or irrelevant, it should be deleted under the supervision of a staff member qualified to hold judicial office. The deletions should be logged, and the logged data can only be used in inspections by overseers (art 3b). Such detailed provisions concerning the oversight of the deletion of data represents best practice.

Complaints handling by quasi-judicial bodies and the judiciary

In Germany, individuals who have complaints against the services, can file complaints either to the quasi-judicial bodies (who have investigative powers and whose decisions are binding), or to the courts. Within the Court system, complaints regarding alleged surveillance practices are handled by the highest administrative court, complying with international standards. All other complaints against the services are handled by the local administrative courts.[202]

200 Thorsten Wetzling, SNV Policy Brief: 'The Key to Intelligence Reform in Germany- Strengthening the G-10 Commission's role to authorize strategic surveillance' 2016, p.3

201 G-10 Law, articles 3-5

202 German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.20

Belgium is another country where judicial oversight is largely carried out by quasi-judicial expert bodies instead of regular courts. Nevertheless courts play a key role in adjudicating on privacy/surveillance related cases and thus setting standards.

Ex-ante authorization of targeted surveillance: As mentioned in the first chapter, a progressive feature of the Belgian legal framework on surveillance is that the law makes a distinction between specific surveillance measures and exceptional surveillance measures. Specific surveillance measures are less intrusive such as requiring the cooperation of a communications operator, inspecting identification data, localisation and call-associated data of electronic communications. The director of the security service authorizes these measures; however the service is obliged to regularly report on the implementation of those measures to the expert oversight bodies.[203]

Exceptional surveillance measures are more intrusive measures which include not only the interception of communications but also observation in and searches of private dwellings; hacking into electronic systems; the and the use of human agents including through the creation of false identities. For the authorization of exceptional surveillance measures, the Security Service directly submits a written request to the Administrative Commission, the quasi –judicial expert oversight body (see Chapter 3.2). The Commission reviews the request, and in four days decide whether to approve or reject the request. Only after the request is approved, can the exceptional measures be implemented. However, even in the approval decisions, the Administrative Commission informs the Standing Committee I (the second quasi –judicial expert body in Belgium, see Chapter 3.2) ; which can overrule the Commission's authorization, and order an immediate secession of the surveillance measure.[204]

In compliance with international standards, in *emergency cases* the security service, with the approval of the head of the Administrative Commission, can implement exceptional measures for 48 hours, provided that justification for urgency is sent to the Commission immediately after.[205]

Complaint handling and adjudication:

On the basis of civil law, ordinary courts have the mandate to consider complaints concerning violation of human rights by security services. However such courts have limited expertise and may have restricted access to information. Instead, the Standing Committee I, which has full access to confidential information, and a mandate to receive and handle complaints with wide investigatory powers, and expertise on most technical surveillance measures is in a better position to handle complaints. Even though it cannot provide remedy itself like a court, it can refer the complainant to the body or service that has jurisdiction over in this regard.[206]

Setting aside the individual complaints, the Belgian Constitutional Court plays a crucial role in adjudicating on surveillance related measures. Recently the Court ruled that the Data Retention Act as unconstitutional. As a result, the Government drafted a new law, including strict safeguards and security measures, in response to the concerns raised by the Constitutional Court.[207]

3.4. OVERSIGHT BY THE CIVIL SOCIETY

In democratic societies, civil society plays an indirect, yet an important role in the accountability system. Compared to the other oversight actors such as the judiciary, parliament, independent oversight bodies and ombuds institutions; it does not have a 'formal' mandate to authorize, scrutinize or investigate activities of security services. However, civil society organizations exercise a number of functions, which make an important contribution to the

203 *EU FRA Surveillance by Intelligence Services (2015), p.69*
204 *EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.94*
205 Ibid. p.98
206 *EU FRA Surveillance by Intelligence Services (2015), P.69*
207 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), pp1-2

accountability of security services.

Key functions of civil society organizations in security services oversight:[208]

- **Monitoring legislative processes:** Civil society organizations (CSOs) analyze draft laws concerning the governance and oversight of security services, identify gaps in the legal framework, and develop recommendations for improvement. In some countries, they are invited by parliamentary committees to provide their expert opinion on draft laws. This is a key opportunity for the civil society to contribute to the development of legal framework, although in most countries, this is often done on an ad-hoc basis. Once the laws are adopted, CSOs monitor their implementation to identify discrepancies between the laws and practice.

- **Monitoring the activities of security services and launching critical litigation:** Considering that security services operate within a ring of secrecy, it is often not possible for CSOs to proactively monitor their activities, however CSOs usually pick up media reports on scandals/allegations of wrongdoing. Monitoring both the legal framework and the activities, CSOs play a key role in initiating lawsuits challenging problematic laws or practices of security services in both national courts and the ECtHR. By way of example, four French CSOs filed a lawsuit on radio surveillance, whereby the Constitutional Court ruled that the legal provision on such surveillance was contrary to the French Constitution. As a result, Article L.811-5 of the Internal Security Code was repealed.[209]

- **Developing informed public debate through research and advocacy:** Laws and policies concerning security services are often highly technical and complex for ordinary citizens to understand. However those laws and policies have a significant impact on fundamental human rights, in particular on privacy. It is important that the public comprehends the extent of security service powers and activities, as well as the potential impact on their daily lives. CSOs play a crucial role in raising awareness on surveillance, privacy related issues, and the need for accountability of security services through publishing research and articles addressing the general public and carrying out advocacy campaigns. Although this is not a direct form of oversight, visible public campaigns and fostering informed public opinion on these matters exert pressure on law- and policy makers to abide by international standards.

- **Contributing to norm setting at international level:** In the past decades there has been an increasing interest and efforts on the part of international society to develop norms and principles on the governance and oversight of security services. Although they are not legally binding, they do contribute to standard-setting; and encouraging states to comply with best practices. Examples of such normative instruments are Tshwane Principles (The Global Principles on National Security and the Right to Information) and Ottowa Principles on Anti Terrorism and Human Rights. Experts from civil society organizations around the world have contributed to the development of those instruments.

This is not an exhaustive list of all the way NGOs can contribute to the oversight of security services, but a brief overview of key functions. The effectiveness and scope of civil society organizations depend very much on the political culture, which includes the government's willingness to cooperate, transparency of security services, the public's involvement and interest in these matters, as well as availability of subject-matter expertise.

208 For more details, see *EU FRA, Surveillance by Intelligence Services Vol 2. (2017)* p.69

209 *France, Constitutional Court, Decision n. 2016-590 QPC, 21 October 2016*

GERMANY

Germany is one of the countries where the general public and the civil society is highly sensitive to- and involved in surveillance, data protection and privacy related matters; partly due to its history. There are several CSOs specialized in these matters, notable ones include Stiftung für Neue Verwaltung (SNV), Netzpolitik, Digitale Gesellschaft, and the Society for Civil Rights.

Developing informed public debate through research and advocacy The SNV has a specific program on 'Digital Basic Rights, Surveillance and Transparency', which carries out research and analysis on intelligence-related laws and practices and develops policy recommendations. The program publishes both research addressed towards expert community, and shorter articles and opinion pieces published in mass media, explaining in a plain language, problems with intelligence governance and risks to privacy rights.[210]

Launching critical litigation: Similar to their counterparts in other European countries, German NGOs have been active in challenging surveillance laws in courts. In 2013, the German branch of Reporters without Borders (RWB) brought an action against BND's (German Intelligence Agency) strategic surveillance of international communications. After several years of legal battles, in 2017, the case was brought before the Federal Constitutional Court chal- lenging, among others, the lack of remedies in case of strategic surveillance.[211]

210 Publications (including those in English), and information on activities of SNV can be accessed at: https://www.stiftung-nv.de/en/project/digital-basic-rights-surveillance-and-transparency

211 *EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.70*

***Monitoring legislative practices**:* Belgian CSOs that are specialized in issues surrounding intelligence governance and human rights closely follow legislative developments. Recently, several CSOs published a joint statement against a draft bill concerning the collection of metadata.[212]

***Launching critical litigation**:* French and German Speaking Bars (OBFG) of Belgium and other human rights NGOs took the 'Act on the Retention of Data' to the Belgian Constitutional Court, claiming that the law provides too much discretion, allowing for disproportional measures. In the end, the Court annulled the law, and ruled that the law's 'scope covered the personal data of every Belgian citizen, and was not limited to those suspected of posing a threat to public security or those related to a serious and specific offence'.[213]

212 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), p.3

213 Ibid. Also see (Belgium constitutional court, Case No. 84/2015, 11 June 2015.

Croatia adopted a progressive approach for ensuring civil society involvement in the oversight of security services. The legal basis of the expert body, 'Civilian Council for Security and Intelligence Oversight' allows for inclusion of academics, human rights experts and advocates to take part in the Council as a member.[214] Indeed, former members of the Council included CSO representatives.[215]

Another emerging good practice is that, since 2014 the Security and Intelligence Agency (SOA) has been publishing annual reports that are accessible to the public. In doing so, SOA presents the report to civil society organizations, and invite them to provide feedback.[216]

Monitoring legal basis and activities of security services: Some Croatian NGOs are actively engaged in monitoring security service's activities. Most recently, the Center for Peace Studies and an activist organisation 'Are You Syrius?', published a report analyzing the role of the security services (SOA) in vetting foreigners and asylum seekers in Croatia. After an analysis of individual case files and laws, the NGOs identified several problematic practices and developed policy recommendations.[217]

214 Article 110 of the SOA Law https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf

215 Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015), p.48

216 Gordan Bosanac, 'Legal Update Report: Croatia' National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016)

217 The report can be accessed: http://www.asylumineurope.org/news/04-05-2017/croatia-increasing-rejections-asylum-claims-based-classified-security-reasons

Monitoring legislative processes and developing informed public debate:

Canada has a vibrant civil society, which is very active in the fields of security and human rights. The Government's open attitude, and institutional mechanisms to collect NGOs input on legislation, further enhances civil society engagement in legislative processes. Recently, the Government launched a public consultation to collect public input to the Anti-Terrorism Act of 2015. Several Canadian civil society organizations, including (Openmedia, Canadian Journalists for Free Expression (CJFA), Canadian Civil Liberties Association) provided input outlining their concerns on mass surveillance, and launched massive public campaigns to inform the public about most problematic aspects of the law, and providing them with straightforward, accessible online tools to provide feedback to the government. [218]

218 See http://www.cbc.ca/news/politics/liberal-security-bill-opposition-1.4297316 , http://www.cjfe.org/6_reasons_why_you_should_participate_in_the_national_security_consultation and https://act.openmedia.org/security

CHAPTER 4: TRANSPARENCY OF SECURITY SERVICES

The balance between secrecy and transparency is one of the core debates concerning the governance of security services. While it is understandable that a certain degree of secrecy accompanies the work of security services, without adequate information, oversight actors would not be able to monitor the legality, effectiveness, and efficiency of the services' policies and activities. Over the last decades a set of standards on transparency have been developed at the international level, most notably the Global Principles on National Security and the Right to Information (The Tshwane Principles)[219] and the UN Compilation of Good Practices. This chapter will cover general standards on the transparency of security services, as well as the right to access one's own data.

4.1. GENERAL STANDARDS ON TRANSPARENCY AND ACCESS TO INFORMATION

- ***Publicly available laws:*** The most fundamental standard on transparency is that security services should be established through publicly available laws. Practice 4 of the UN Compilation of Practices states that: '*[A]ll intelligence services are constituted through, and operate under, publicly available laws that comply with the Constitution and international human rights law. Intelligence services can only undertake or be instructed to undertake activities that are prescribed by and in accordance with national law.*'

- ***Secret regulations:*** It is generally accepted that beyond publicly available laws, security services are regulated through subsidiary regulations (by-laws, ministerial directives etc.) that are withheld from the public access. Such regulations often include operational methods of security services, which would risk their operations, if disclosed to public.[220] However, as per UN guidance, the use of subsidiary regulations should be strictly limited, and such secret regulations should not serve as the basis for any activities that restrict human rights.[221] For instance the scope of surveillance conducted by the services should be regulated by laws and not by secret directives.

- ***Access to information laws:*** In democratic societies, freedom of information laws provide a basis for transparency. However such laws usually come with certain restrictions and limitations. It is good practice when security services are not completely exempted from such laws, but rather allowed to take advantage of narrowly described exceptions and restrictions, for the purposes of protecting national security.[222] In the EU, laws of all Member States allow for some form of limitation on the right to access to information based on a threat to national security and/or objectives of security services.[223]

- ***Restrictions on the access to information:*** It is crucial how the restrictions are defined by law. The Tshwane Principles established a comprehensive standard on such restrictions. Principle 3 states: '[N]o restriction on the right to information on national security grounds may be imposed unless the government can demonstrate that: (1) the restriction (a) is prescribed by law and (b) is necessary in a democratic society (c) to protect a legitimate national security interest; and (2) the law provides for adequate safeguards against abuse, including prompt, full, accessible, and effective scrutiny of the validity of the restriction by an independent oversight authority and full review by the courts.' This standard puts the onus of justifying the necessity of the restriction on the government, underlines the legitimacy of national security interests, and calls for effective external and judicial oversight of such restrictions.

- ***Information that legitimately may be withheld from the public:*** Since most of the restrictions to access to information are based on 'national security' grounds, there is no binding, authoritative list at the international level, on what kind of information should be withheld. Nevertheless, based on opinions of experts and international best practices, the Tshwane Principles developed a list of information that may be legitimately

---

219 The Tshwane Principles, available from https://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles

220 Aidan Wills, Understanding Intelligence Oversight,(DCAF.2010) p.14

221 UN Compilation of Good Practices, Practice 4.

222 Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, (DCAF: 2005), p.,.44

223 *EU FRA Surveillance by Intelligence Services (2015)*, p.62

restricted to public access:[224]

- Information about ongoing defense plans, operations, and capabilities for the length of time that the information is of operational utility.
- Information about the production, capabilities, or use of weapons systems and other military systems, including communications systems.
- Information about specific measures to safeguard the territory of the state, critical infrastructure, or critical national institutions against threats or use of force or sabotage, the effectiveness of which depend upon secrecy;
- Information pertaining to, or derived from, the operations, sources, and methods of intelligence services, insofar as they concern national security matters; and
- Information concerning national security matters that was supplied by a foreign state or inter-governmental body with an express expectation of confidentiality; and other diplomatic communications insofar as they concern national security matters.

- ***Classification of information:*** While it is agreed that certain information can be withheld from public, there are standards as to how states should classify information. First and foremost, what is classified should be the information, and not documents. This way, it would be possible to disclose documents by redacting the parts containing classified information, and making the rest of the document available to public.[225] Tshwane Principles include further detailed standards on classification, including, inter alia, the Government's duty to state reasons for classification (Principle 11), public access to procedures governing classification (Principle 12), time limits for period of classification, and periodic review of decisions to withheld information (principle 16).
- ***Annual Public Reports of Security Services:*** Although there is no internationally recognized standard for the content and the length of the annual reports of services, good practice suggest that it should include:[226]
  - Key priorities of the service;
  - Overview of major security threats;
  - Substantial changes to security/intelligence related policies;
  - Information and statistics on the accountability functions, including its response to requests for access to information.

4.2. STANDARDS ON THE RIGHT TO ACCESS ONE'S OWN DATA

An essential aspect of transparency is the right to access one's own data held by security services. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[227] is the first binding legal instrument which sets standards on data collection and processing and which explicitly recognizes the rights of data subjects (individuals whose data are collected). Article 8 of the Convention stipulates that:

'Any person shall be enabled:

a) to **establish the existence of an automated personal data file**, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

---

224 Tshwane Principles, Part II, Principle 9

225 Laurie Nathan, 'Intelligence Transparency, Secrecy and Oversight in a Democracy', p.55 in Born and Wills (ed.) *Overseeing Intelligence Services: A Toolkit* (DCAF: 2012)

226 Ibid, p.57

227 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

b) to **obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored** in the automated data file as well as **communication to him of such data** in an intelligible form;

c) to obtain, as the case may be, **rectification or erasure of such data if these have been processed contrary to the provisions of domestic law** giving effect to the basic principles set out in Articles 5 and 6 of this Convention;

d) to **have a remedy** if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.'

The provisions of this legally binding Convention provides for clear obligations for security services to respond to requests concerning the existence of personal data, to communicate the data to the data subject, to rectify or erase in case of an unlawful collection/processing. However Article 9 of the Convention allows for derogations from such obligations in the interests of 'protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;' as well as 'protecting the data subject or the rights and freedoms of others'.

These standards are not only recognized by the CoE Convention, but also the international soft-law instruments such as the UN Guidelines for the Regulation of Computerized Personal Data Files (Principle 4)[228], The Tshwane Principles (Part III), as well as the UN Compilation of Good Practices (Practice 26). In line with these European and International standards, most democratic countries have adopted laws and established mechanisms to protect and fulfill the right to access one's own data. There are essentially three main approaches in this respect:

Direct access by the data subject: Most countries have laws, which allow the data subject to apply directly to the security service and request access to his/her data. However such laws come with certain restrictions, allowing the services not to disclose the data in order to safeguard ongoing investigations and protecting sources and methods of the services.[229] An important standard in this regard is that such restrictions should be outlined by law, and the law should provide the data subject with the right to appeal against the decision in a judicial setting.[230]

Indirect access by an expert oversight body or DPA: As an attempt to balance restrictions to data subjects' access, some states allow their Data Protection Authorities and /or expert oversight bodies to access the data on behalf of the data subject. In this respect, it is good practice when these bodies are able to check whether the justification for restricting the data subject's access was reasonable, access and review the said data to see if it was collected lawfully, and order the destruction of the data if there was any violation of laws.[231] This approach has been adopted by 12 EU member states, including Austria, Belgium, Bulgaria, Cyprus, Finland, France, Hungary, Ireland, Italy, Luxembourg, Portugal and Sweden.[232]

Notification of the data subject by the security service: Lastly, an advanced, yet no so common approach is to oblige the security services to notify the data subject after the surveillance has ended, regardless of any request by the data subject and/or an expert oversight body.

The approaches above are not mutually exclusive and states may choose to combine them.

228 General Assembly Resolution 45/95 (1990), available from : http://www.refworld.org/pdfid/3ddcafaac.pdf

229 UN Compilation, para 40.

230 Laurie Nathan, 'Intelligence Transparency, Secrecy and Oversight in a Democracy', p.55 in Born and Wills (ed.) Overseeing Intelligence Services: A Toolkit (DCAF: 2012)

231 EU FRA, Surveillance by Intelligence Services ,Vol 2, (2017), p.110, Also see Hans Born and Ian Leigh, Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies, (DCAF: 2005)

232 EU FRA, Surveillance by Intelligence Services Vol 2, (2017), p.126

CROATIA

Publicly available laws and secret regulations: The Croatian security service (SOA) operates based on a publicly available law. In line with international standards, the law explicitly defines the surveillance and other covert information collection measures infringing upon human rights (articles 33-37 of the SOA Law), as well as authorization and oversight procedures. However, the following are governed by regulations and ordinances that are classified, and therefore withheld from public (articles 62-65 of the Law):

- Internal structure, scope of activities and management of internal units,
- The necessary number of employees, their job requirements, functions and tasks,
- Security –intelligence measures, procedures and means applied in the work of the SOA.

Access to information law and restrictions: In Croatia, access to information is regulated by the Law on the Right to Access to Information.[233] Article 15 of the law has a long list of conditions which would restrict public access to information, one of which is 'if the information is classified by public authorities'.

Information Classification: According to the 'Data Secrecy Act'[234], which regulates information classification, the director of the SOA is entitled to classify information whose disclosure would damage national security or functioning of state authorities (articles 6-9). In this framework, personal data relating to surveillance measures are classified as top secret, secret, confidential or limited – depending on the target of surveillance.[235] Given the SOA's wide powers to classify information, public access to information can be considerably limited.

Access to one's own data: Croatia has adopted the 'direct access by the data subject' approach. Article 40 of the SOA law states that SOA is obliged to inform the data subject within 15 days upon their request if measures of secret information collection have been applied against them, and allow access to the collected data at their request. However the same article provides for broad restrictions to this right, and allows SOA not to disclose the data if (i) the information would jeopardize the fulfillment of the agency tasks, (ii) the information could result in a threat to the security of another person, and (iii) the information could result in consequences harmful for the national security and the national interests of the Republic of Croatia. If the data subject would like to appeal the decision of SOA to not disclose information, he/she can apply to the Information Commissioner, who is entitled to review whether SOA has applied 'proportionality' test before classifying information. The Council for Civilian Oversight of Security and Intelligence Agencies (the expert oversight body) is also entitled to oversee how SOA classifies information, but so far it has never exercised that power. These legal restrictions, and the limitations of oversight institutions in practice make access to one's own data practically impossible.[236]

Annual Reports of the SOA: SOA publishes annual reports, available on its website. The reports are around 30 pages, including an overview of main security challenges, security vetting activities of SOA, information on international cooperation and very basic information on the budget.

233 http://www.revizija.hr/en/access-to-information/law-on-the-right-to-access-information
234 http://europam.eu/data/mechanisms/FOI/FOI%20Laws/Croatia/Croatia_Data%20Secrecy%20Act_2007.pdf
235 Gordan Bosanac, 'Legal Update Report: Croatia' National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.7
236 Ibid.

Publicly available laws and secret regulations: The Canadian Security Intelligence Service (CSIS) operates based on a publicly available law, in both official languages of Canada. The Law outlines in detail information collection measures that infringe upon human rights, which is in line with international standards. Although ministerial directions are not necessarily public, Canada embodies best practice by obliging CSIS to proactively send all directives to the Review Committee (see Chapter 2 on External Control).

Access to information: Canada has one of the most comprehensive freedom of information legislations. **The Access to Information Act**,[237] articles 13-16 stipulate the exemptions from the Government's duty to disclose information. However, the same law provides in detail the procedures for appealing the government institution's decision to refuse public access to information. The Information Commissioner is entitled to receive, handle and investigate complaints regarding government institutions' refusal to give access (art. 30-36). Based on the results of the investigation, the Commissioner issues recommendations to the government institution including appropriate actions to be taken (art 37). If the government institution does not provide access to information despite the Information Commissioner's recommendation, the complainant can take the case to the Federal Court (art 41). Thus, in line with international standards, the Canadian law provides strong remedies against refusal to access information.

Access to one's own personal data: The Privacy Act[238] regulates the procedures for access to personal information held by a government institution. The Act defines what is meant by personal data, the procedures for accessing personal data, as well as exemptions from access. If an individual is refused access, he/she can file a complaint with the Privacy Commissioner. Remedial procedures similar to the Access to Information Act apply, including a review by a Federal Court (art 41 of the Privacy Act).

Representing international best practice, the Canadian security service, **CSIS established an internal unit entitled 'Access to Information and Privacy'**. This unit receives and processes all access to information and privacy requests, and assists persons in formulating their requests among other tasks. The unit provides comprehensive information on their work annually, including detailed statistics on access to information requests they received, number of documents disclosed, exemptions invoked and so forth. This is an example of an intelligence agency actively promoting access to information and personal data and assisting individuals making such requests.[239]

Annual reports of the CSIS: CSIS's annual reports are exemplary, as it provides comprehensive information on the service. It publishes the number of employees, as well as statistics on diversity (the rate of minorities, women, persons with disabilities among the staff); as well as a general breakdown of the budget into operational costs and salaries. Furthermore, the report provides data on complaints received and reviews conducted by the SIRC (the expert oversight body) and other oversight actors. The report is highly interactive with videos, infographics and reader-friendly texts.[240]

237 http://laws-lois.justice.gc.ca/eng/acts/A-1/FullText.html
238 http://laws-lois.justice.gc.ca/PDF/P-21.pdf
239 The report of the unit can be accessed at: https://www.csis-scrs.gc.ca/tp/pblctns/2015-2016/nnlrprt-tp20152016-en.php
240 The report can be accessed at: https://www.csis-scrs.gc.ca/pblctns/nnlrprt/2014-2016/index-en.php#Unique

Publicly available laws: Both the BfV and the BND operate based on publicly available laws which outline information collection measures in detail.

Access to information: At the federal level, the right to access to information is regulated by the Freedom of Information Act[241] The Act has a long list of exceptions whereby public access to information can be refused federal authorities. These circumstances include, inter alia,

► where the information disclosed have detrimental effects on

a) International relations,

b) Military and other security-critical interests of the Federal Armed Forces,

c) Internal or external security interests,

d) Monitoring or supervisory tasks of the financial, competition and regulatory authorities,

e) Matters of external financial control,

f) Measures to prevent illicit foreign trade,

g) the course of current judicial proceedings,

► Where the information is subject to official secrecy,

► Where the information is related to security/intelligence agencies performing their security clearance duties (section 3 of the Act).

A good practice in the law is that when an authority refuses a request, it is obliged to notify the person as to whether and when partial or full access to the information is likely to be possible in the future(section 9(2)). Similar to the Canadian model, the German law provides for remedial routes. A refusal decision may be challenged by lodging an appeal to the Administrative Court (section 9(3)). Alternatively, anyone considering their right to access to information has been violated may appeal to the Federal Commissioner for Data Protection (section 12(1)).

Access to one's own data: Individuals' right to request information about their personal data held by the security services are regulated by the Federal Act on the Protection of Constitution[242] and the Act on the Federal Intelligence Service (BND Act) respectively. As for the BfV (the domestic security service), although the law recognizes the right to access to personal data in principle, the exercise of the right is interpreted very narrowly. The data subject should point to a 'specific situation' and justify a 'special interest' in requesting access. Even when these conditions are fulfilled, the BfV is not obliged to allow access if the disclosure of information: 'a) would threaten the implementation of its tasks, b) could put sources at risk or if there are reasons to fear that the request aims to investigate the state of knowledge or operational methods of the BfV, c) could threaten public security or would have detrimental effects on the well-being of the federation or a German state, or d) would conflict with the secret legal status or the secret nature of the information or the fact that it is being held, in particular if legitimate interests of third parties prevail'.[243] More or less the same rules apply to requesting information from the BND.

When their requests are refused, individuals can apply to Federal Data Protection Commissioner, who can approach the services on behalf of the data subject. However, different than the Canadian model, the executive (either the MoI for the BfV, or the Chancellery for the BND) can block the investigation of the Data Commissioner for national security purposes [244], which is a sub-optimal practice in comparison to the Canadian model.

241 https://www.gesetze-im-internet.de/englisch_ifg/englisch_ifg.html#p0021
242 https://www.gesetze-im-internet.de/bverfschg/
243 German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.14
244 Ibid.

Notification of the subject of surveillance: Germany adopted a novel approach, whereby the security services have a general obligation to inform the targets of surveillance, after the surveillance measure has ended.[245]However certain caveats apply:

- Regarding targeted surveillance, data subjects must be informed by the services about the surveillance measures within 12 months after their discontinuation, unless the information would jeopardize the purpose of the surveillance measures or harm the interests of the country (article 12 (1) of the G-10 Law).
- If the services decide not to notify a data subject after 12 months, the case should be reviewed by the G-10 commission, which decides for how long the information should be continued to be withheld.
- If the G-10 Commission unanimously finds that the risk of jeopardizing the purpose of surveillance or harming the interests of the country still applies five years after the termination of the measure, then no notification would be necessary. As per EU FRA statistics, in 2013, of 1,944 persons or institutions regarding which the surveillance measures were discontinued, 650 were informed. G 10 decided to not yet inform 1,079 persons/ institutions, and unanimously agreed 260 would never be informed.[246]
- Regarding strategic surveillance, same notification rules apply to the personal data which was processed, but not to the data which is immediately deleted after collection. Foreign-foreign strategic surveillance is completely exempt from notification requirement.[247]

As can be seen, Germany adopts all three approaches, direct access by the data subject, indirect access through the DPA and notification by the services.

Annual reports of the services: Although the Annual Report of the domestic security service BFV is voluminous (335 pages), however most of the report is dedicated to the detailed explanation of organizations /movements that pose a threat to the national security. Only a few pages are dedicated to the oversight of the BfV and unlike the Canadian example, no statistics regarding complaints are provided. Annual report of the BND is not available on its website.

245 G-10 Law Section 12

246 *EU FRA Surveillance by Intelligence Services (2015) p.64*

247 *EU FRA Surveillance by Intelligence Services Vol 2. (2017), p.126*

BELGIUM

Publicly available laws: Belgian security services are constituted through and operate based on publicly available laws.[248] The Standing Committee I publishes on its website not only the laws but also all relevant ministerial decrees on information classification, establishment of common databases, which represents good practice.

Access to information and one's own data: In Belgium, access to general information held by the services, as well as one's own data is regulated by the Act on the Transparency of Administration.[249] The law allows for direct access by the data subject to their own data, subject to certain restrictions. The security service is not obliged to disclose the data, if it deems safeguarding the interests of public order, public security, national defence and the safety of the population are more important than principle of transparency (art. 6 of the Transparency Act). However in practice, such broad exemptions result in almost all access requests to be denied. Moreover, unlike the Canadian model, the security service does not publish statistics on how many access to information requests are made.[250]

Indirect Access to Information: While direct access of the data subject is not effectively realized, the Belgian Privacy Act provides for indirect access to personal data that is processed for national security, state safety and national defence purposes. In such cases, the data subject can submit a request to the Privacy Commission, which reviews whether the security service complied with the law when handling the data subject's personal information. If there are any irregularities, the Privacy Commission can recommend changes to the data. After the review, the Commission informs the data subject, but it does not share the data held by the service.[251]

Indirect access to data can also be obtained through Standing Committee I, when the data subject files a complaint to the Committee and a legitimate and personal interest.[252]

Notification by the services: In 2011, the Belgian Constitutional Court stated that the security services should 'actively inform the person subject to a measure of surveillance as soon as such notification is possible without jeopardizing the purpose of the intelligence work'.[253] However, the laws have not yet been amended accordingly.

Annual reports of the service: Annual reports of the Belgian security service is not available on their website.

248 Organic Law on Security and Intelligence Services (1998).
249 *Loi relative à la publicité de l'administration, 11 April 1994*
250 Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),p.16
251 Belgium, Belgian Privacy Commission *(Commission vie privée/ Privacycommissie)*, 'La protection des données à caractère personnel en Belgique', Brussels, Privacy Commission, p. 20
252 Organic Law on the intelligence and security services Art 43 (4).
253 Judgement No. 145/2011, 22 September 2011, paras 88 to 92.

BIBLIOGRAPHY

Aidan Wills and Benjamin Buckland, *Access to Information by Intelligence and Security Service Oversight Bodies*, (DCAF/OSF, 2012), http://www.dcaf.ch/sites/default/files/publications/documents/Access_information_oversight_bodies_draft.02.12.pdf

Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, (DCAF: 2010), http://www.dcaf.ch/guidebook-understanding-intelligence-oversight

Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2456151

Council of Europe, *Democratic and Effective Oversight of National Security Services*, (2015): https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

Canadian Security Intelligence Agency, Annual Report 2016: https://www.csis-scrs.gc.ca/pblctns/nnlrprt/2014-2016/index-en.php#Unique

Croatian Council for Civilian Oversight of Security and Intelligence Agencies, Fact Sheet, available from http://www.sabor.hr/0060

Committee I, Activity Report 2014-2015, http://www.comiteri.be/images/pdf/Jaarverslagen/Activity_Report_2014_15.pdf

DCAF, Parliamentary Brief: Safeguards in Electronic Surveillance, available from: https://dcaf.ch/resources?type=publications

European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Mapping Member States' legal frameworks,* (Luxembourg, 2015), http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU*- - Volume II: field perspectives and legal update (Luxembourg, 2017), http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and/publications

German Federal Ministry of the Interior, Report on the Protection of the Constitution (2016),: https://www.verfassungsschutz.de/en/about-the-bfv

German Institute for Human Rights, Legal Update Report: Germany, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016),: http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu

Global Principles on National Security and the Right to Information (Tshwane Principles), available from: https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf

Gordan Bosanac, 'Legal Update Report: Croatia' National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016): http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu

Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, (DCAF: 2005), p., available from: http://www.dcaf.ch/making-intelligence-accountable

Hans Born and Aidan Wills (ed.) *Overseeing Intelligence Services: A Toolkit* (DCAF: 2012) http://www.dcaf.ch/sites/default/files/publications/documents/Born_Wills_Intelligence_oversight_TK_EN_0.pdf

Hans de With and Erhard Kathmann, 'Annex A- Country Case Studies - Germany', in Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011)

Laura Jacques, Legal update report: Belgium, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies (EU FRA, 2016), http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu

Lauren Hutton, 'Overseeing Information Collection', Tool 5, in Born and Wills, *Overseeing Intelligence Services – A Toolkit*, (DCAF: 2012)

The Paris Principles, http://www.ohchr.org/EN/ProfessionalInterest/Pages/StatusOfNationalInstitutions.aspx

Thorsten Wetzling, 'Germany's Intelligence Reform: More surveillance, modest restraints and inefficient controls' SNV Policy Brief (2017), available from: https://www.stiftung-nv.de/en/project/digital-basic-rights-surveillance-and-transparency/publikationen

Thorsten Wetzling, SNV Policy Brief: 'The Key to Intelligence Reform in Germany- Strengthening the G-10 Commission's role to authorize strategic surveillance' 2016, https://www.stiftung-nv.de/en/project/digital-basic-rights-surveillance-and-transparency/publikationen

UNODC, 'Current practices in electronic surveillance in the investigation of serious and organized crime' (New York, 2009) https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf

UN General Assembly Resolution 45/95 (1990), http://www.refworld.org/pdfid/3ddcafaac.pdf

UN Human Rights Council, *Compilation Of Good Practices On Legal And Institutional Frameworks And Measures That Ensure Respect For Human Rights By Intelligence Agencies While Countering Terrorism, Including On Their Oversight* (*UN Compilation of Good Practices*), A/HRC/14/46 para , http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf

Venice Commission, *Report on the Democratic Oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session* (2007), http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx

Venice Commission , *Report on the Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session,* CDL-AD (2015) 011: http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)011-e,

Wauter Van Laetham, The Belgian Civil Intelligence Service: Roles, Powers, Organisation and Supervision , EJIS, Volume 2, (2008) http://www.comiteri.be/index.php/en/publications/specialized-literature

National Laws

Belgium

Act on Security and Intelligence Services, (Loi Organique des Services de Renseignement et de Securite) (18 decembre 1988), available from : http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032

Loi relative à la publicité de l'administration, 11 April 1994, http://www.mumm.ac.be/Downloads/bmdc_LOI-WET_11_04_1994.pdf

Canada

Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23) available from: http://laws-lois.justice.gc.ca/eng/acts/c-23/index.html

National Security and Intelligence Committee of Parliamentarians Act (S.C. 2017, c. 15),: http://laws.justice.gc.ca/eng/AnnualStatutes/2017_15/page-1.html

Security of Information Act (R.S.C., 1985, c. O-5), available from http://laws-lois.justice.gc.ca/eng/acts/O-5/

Access to Information Act http://laws-lois.justice.gc.ca/eng/acts/A-1/FullText.html

Privacy Act http://laws-lois.justice.gc.ca/PDF/P-21.pdf

Croatia:

Act on the Security Intelligence System of the Republic of Croatia https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf

Data Secrecy Act: **http://europam.eu/data/mechanisms/FOI/FOI%20Laws/Croatia/Croatia_Data%20Secrecy%20Act_2007.pdf**

Decree on the Right of Security and Intelligence Agency Officials to Bear and Use Firearms, available from: https://www.soa.hr/UserFiles/File/Decree_bear_and_use_firearms.pdf

Act on the Right to Access to Information: , http://www.revizija.hr/en/access-to-information/law-on-the-right-to-access-information

Germany

Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution https://www.gesetze-im-internet.de/bverfschg/

Act on the Federal Intelligence Service, https://www.gesetze-im-internet.de/bndg/

Code of Criminal Procedure, as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I p. 410) https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html

Act on the Parliamentary Control of Federal Intelligence Services Art.4.1, http://www.gesetze-im-internet.de/pkgrg/BJNR234610009.html

G-10 Act, https://www.gesetze-im-internet.de/g10_2001/index.html

Freedom of Information Act, https://www.gesetze-im-internet.de/englisch_ifg/englisch_ifg.html#p0021

ECtHR Court Cases
Klass and Others v. Germany, No.5029/71, 6 September 1978.
Leander v. Sweden, Application No.9248/81, 26 March 1987.
Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016,
Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015,*
United Communist Party of Turkey and Others v. Turkey, 19392/92, 30 January 1998
Zana v. Turkey, 18954/91, 25 November 1997