LEGAL ASPECTS OF THE EUROPEAN INTELLIGENCE SERVICES' ACTIVITIES

Scientific Editor Piotr Burczaniuk

LEGAL ASPECTS OF THE EUROPEAN INTELLIGENCE SERVICES' ACTIVITIES

Scientific Editor **Piotr Burczaniuk**

LEGAL ASPECTS OF THE EUROPEAN INTELLIGENCE SERVICES' ACTIVITIES

Scientific Editor **Piotr Burczaniuk**

Warsaw 2022

Reviewers
Prof. Artur Kotowski (Cardinal Stefan Wyszyński University in Warsaw)
Prof. Marcin Wielec (Cardinal Stefan Wyszyński University in Warsaw)

Editors
Magdalena Liebner (Poltext)
Marcin Nowiński (Internal Security Agency)
Julita Kisielewska (Internal Security Agency)

Cover design
Aleksandra Bednarczyk

Typesetting
Camélia Dizajn

ISBN: 978-83-964225-0-7

Publishing House of the Internal Security Agency
Central Training and Education Centre named after Major General Stefan Rowecki ‘Grot’
ul. Nadwiślańczyków 2, 05-462 Wiązowna, Poland

Contact
e-mail: wydawnictwo@abw.gov.pl
www.abw.gov.pl/pub/

Contents

Foreword

The Internal Security Agency (the ABW) that I have the honour of leading is the biggest Polish intelligence and security service, possessing the most comprehensive scope of tasks and competences among the other intelligence and security services. In consequence, the ABW is one of the pillars of the security system of Poland and, as demonstrated by the Russian aggression on Ukraine, along with the intelligence and security services of the Western and Central European states and the United States of America, one of the core elements guaranteeing the security of the Western civilisation.

24 May 2022 marked the 20th anniversary of the creation of the ABW on the basis of the legislative decision of the Parliament of the Republic of Poland. The ABW was separated from the State Protection Office (UOP), established in 1990. This anniversary became the opportunity to reflect on the role of this institution in safeguarding security, both in its internal dimension and in its external dimension, understood as the security of the Euro-Atlantic community.

As far as the first dimension is concerned, the years 1990 and 2002 mark important stages in the process of shaping the model of the Polish intelligence and security services which have been profoundly modified during the last 30 years. This fundamental transformation has been conditioned by the change of the political system and the transition from the communist system to the principle of the democratic state ruled by law which is enshrined in Article 2 of the Constitution of the Republic of Poland of 2 April 1997. In the security dimension, this transformation is illustrated by leaving the Warsaw Pact and joining the NATO structures.

These structural changes triggered the need to redefine the perception of threats to the very existence of Poland and to outline the role and tasks of the new established institutions responsible for national security, including the intelligence and security services, safeguarding its respective components. In the external dimension, the geopolitical fluctuations that we experienced both after the fall of the Iron Curtain and at the dawn of the 21st century, redefined the Euro-Atlantic security paradigm and shaped the tasks and powers of the intelligence and security services which are some of its core elements.

In this context, as far as the Polish perspective is concerned, our membership in NATO from 12 March 1999 and in the EU from 1 May 2004 laid the foundations of the security policy and correlated the activities exercised by the Polish services with their European counterparts in order to effectively safeguard the security of the Euro-Atlantic area.

From such a perspective, this publication, the basic idea of which is to present institutional models of the Euro-Atlantic intelligence and security services to European readers, is of particular value.

It continues a series of legal monographs devoted to the problems concerning intelligence and security services initiated in 2017 by Prof. Piotr Pogonowski – the then Head of the Internal Security Agency – published by the Publishing House of the Internal Security Agency. The previous publications, including the monograph *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego* [The Legal Aspects of the Functioning of the Intelligence and Security Services on the Example of the Internal Security Agency], because of its thematic scope and the fact that it was published in Polish, was addressed to the public in Poland. In this context, this monograph, presenting an overview of the tasks and powers of the intelligence and security services of 19 European countries (Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Estonia, France, Greece, Spain, the Netherlands, Lithuania, Latvia, Germany, Poland, Romania, Slovakia, Hungary, Italy and Sweden) and its publication in English, targets a broader public, including European lawyers and practitioners interested in various issues concerning the intelligence and security services.

In my opinion, the value of this publication is evidenced by the fact that it was written by a sizeable group of authors of individual chapters, i.e. 26 legal experts representing the aforementioned 19 European countries. Furthermore, substantive supervision was assumed by the University of Cardinal Stefan Wyszyński in Warsaw. All these aspects make this monograph a valuable component of the European literature on intelligence and security services.

Col. Krzysztof Wacławek
Head of the Internal Security Agency

Warsaw, 20 October 2022

Preface

This multi-authored legal monograph which I have edited from the academic point of view aims to provide an overview of the organisational models of the intelligence and security services in certain European countries, sharing the common Western civilisational heritage.

The idea of preparing the present monograph emerged during the editorial works on another legal monograph published in Poland in October 2021 – *The Legal Aspects of the Functioning of the Intelligence and Security Services on the Example of the Internal Security Agency*. That publication sought to systematise 'the doctrinal and theoretical considerations on the intelligence and security services and the need to confront these considerations with the experiences shaped by, among others, judiciary and administrative practice of the twenty years since the adoption of the Act of 4 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency which constitutes the essential element of all the legal provisions applicable to the abovementioned organs in Poland.'[1] The analysis and evaluation of the Polish provisions in this area presented in that monograph pointed to the legitimacy and significant value that a comparison of these regulations with legislative solutions adopted in other countries, irrespective of whether they are similar or diverging, may bring. Such a comparison would be of particular value taking into account the systemic cooperation of the European intelligence services which implement security policy formulated by international organisations, in particular the EU and NATO. Unfortunately, both at the Polish and European levels, there are no publications either analysing such solutions comparatively or presenting them in a comprehensive manner, which could provide a starting point for such research. In my opinion, many European universities have identified similar problems.

This publication is therefore intended to fill the aforementioned gaps, presenting organisational models of the intelligence and security services in selected European countries.

I invited 26 legal experts from 19 Central and Western European countries to cooperate on this project. Each of them, based on his or her expertise in the field of the legal systems

[1] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (ed.), ABW, Warszawa 2021, p. 9.

of their respective countries, wrote, individually or within a research team, one chapter devoted to each country, using a single methodological scheme.

To facilitate the comparative analysis, I assumed that the description of each model should consist of two main parts: first, concerning the role and place of the intelligence and security services in the national institutional architecture, and second, discussing their statutory tasks and powers. As far as the first part is concerned, the authors focused on the legal definition of the intelligence and security services, their position within the public administration system, tasks, supervision and control, and the legal status of their officers. With regard to the second part, the main assumption was to discuss the main types of tasks performed by these organs: investigatory, intelligence gathering, and analytical tasks as well as their responsibilities in the area of ICT security, protection of classified information, international cooperation and protection of personal data. At the same time, I allowed certain divergences in the respective chapters which result mainly from structural differences between the legal systems or their specific features.

With such defined research objectives and methodology, this study characterises regulatory models of the intelligence and security services of 19 countries – Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Estonia, France, Greece, Spain, the Netherlands, Lithuania, Latvia, Germany, Poland, Romania, Slovakia, Hungary, Italy, Sweden. Furthermore, this publication contains an additional chapter discussing national security clause in the European Union law and its implications for intelligence and security services.

I would like to express my gratitude to all the Authors for their willingness to participate in this project and their commitment and the highest professional standards they demonstrated during our cooperation. I am perfectly aware that this work would not have been published without your participation. I seize this opportunity to emphasise my highest appreciation to the academic staff of the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw, in particular to Professor Artur Kotowski and Professor Marcin Wielec – the publishing reviewers of this monograph.

I hope that this monograph will prove to be useful in the field of legal theory and would be well received by the practitioners interested in the problems concerning the intelligence and security services. I believe that the material gathered in this publication may be used for further research on the organisational models of these institutions.

Piotr Burczaniuk, PhD

Warsaw, 20 October 2022

CHAPTER I

Austria

Omar Haijawi-Pirchner

1. POSITION OF THE SERVICE IN THE DOMESTIC LEGAL SYSTEM

1.1. Legal Definition of Special Services

In Austria, there are three organisational units that are entrusted with intelligence tasks domestically and abroad.

The Directorate State Protection and Intelligence (DSN) is the security authority responsible for the protection of the constitution within the Federal Ministry of the Interior and has the characteristics of an intelligence service.

The Strategic Intelligence Agency (HNA) and the Armed Forces Security Agency (HAA) belong to the Federal Ministry of Defence. The tasks of the Strategic Intelligence Agency (HNA) and the Armed Forces Security Agency (HAA) are governed in the Military Powers Act (MBG).

The Austrian Strategic Intelligence Agency (HNA) is responsible for gathering strategic foreign intelligence. Its purpose is the procurement, processing, evaluation and presentation of information about foreign countries, international organisations or other intergovernmental institutions concerning military facts and other related facts, activities and projects.

The Armed Forces Security Agency (HAA) is responsible for the aversion of threats to military security. Its purpose is the self-protection of the military through the procurement, processing, evaluation and presentation of information on endeavours and activities that can be expected to lead to intentional attacks against the legal interests of the military and aim to impair military security.

The purpose of the protection of the constitution is to protect constitutional institutions and their capacity to act; representatives of foreign states, international organisations and other subjects of international law in accordance with the obligations under international

law; the critical infrastructure and the population against crimes driven by terrorist, ideological or religious motives and against threats from espionage, by means of intelligence activities and through proliferation, as well as to carry out key functions in international cooperation in these areas.

1.2. Position and Role of the Services in the Public Administration System

In Austria, the protection of the constitution is carried out by the Directorate State Protection and Intelligence Service (DSN) and the organisational units of the provincial police directorates responsible for State protection in the Austrian federal provinces. They are an organisational unit of the Directorate General for Public Security of the Federal Ministry of the Interior.

Due to domestic legal provisions, Austria does not have an intelligence service per se. The protection of the constitution is performed in the exercise of the security police.

State police matters thus fall within the area of responsibility of the security police and serve to maintain public peace, order and security. Both the Directorate State Protection and Intelligence Service (DSN) and the organisational units of the provincial police directorates responsible for state protection are organisational units of the security authorities pursuant to Article 78a of the Federal Constitutional Law (B-VG).

The DSN was established on 1 December 2021. In terms of organisation, it is clearly separated into the areas of state protection and intelligence service. The state protection area is responsible for the preventive protection against attacks endangering the constitution, danger aversion pursuant to the Security Police Act and the performance of criminal police investigations. The intelligence service area is responsible for the collection and analysis of information as well as extended threat investigation.

The State Protection and Intelligence Service Act (SNG) forms the legal basis for the protection of the constitution, which serves as an umbrella term for the separate areas of the responsibility of state protection and intelligence service within the organisation. In addition to the responsibilities and organisation of the authorities responsible for the protection of the constitution, this act governs the tasks and powers of the said authorities as well as the processing of personal data and it contains special provisions for legal protection.

The State Protection and Intelligence Act contains provisions concerning the area of the responsibility and organisation of the authorities responsible for the protection of the constitution, regulations concerning the training of employees working in these authorities and concerning the high sensitivity with regard to the information security, confidentiality and integrity necessary in this area.

The SNG determines the DSN's central functions (e.g. operational coordination centre for reports of any form of attack on the computer systems of constitutional institutions or critical infrastructure, security vetting and reliability examinations, as well as the Reporting Office for National Socialist Activity and the Reporting Office for Extremism and Terrorism).

Furthermore, the State Protection and Intelligence Service Act standardises the tasks that are exclusively performed by the authorities responsible for the protection of the constitution. The state protection area encompasses the prevention of attacks endangering the constitution as well as the performance of tasks pursuant to the Security Police Act and the Code of Criminal Procedure in connection with attacks endangering the constitution. The intelligence service area comprises the collection and analysis of information for the purposes of the protection of the constitution as well as extended threat investigation for the surveillance of a group. Furthermore, the State Protection and Intelligence Service Act (SNG) contains special powers for the purpose of performing the tasks of the authorities responsible for the protection of the constitution.

Moreover, the SNG comprises the appropriate legal protection for the special tasks and powers, an increased parliamentary control through comprehensive obligations to report and the establishment of an independent control commission not bound by instructions for the structural control of the authorities responsible for the protection of the constitution.

The Security Police Act (SPG), which forms the legal basis for the security police tasks of the police forces, contains the central tasks and the corresponding powers as well as provisions on legal protection that are essential for the work of the authorities responsible for the protection of the constitution.

The Security Police Act includes tasks of relevance to state protection, such as danger aversion, the protection of constitutional institutions and their ability to act, foreign representatives, international organisations and other subjects of international law in accordance with international obligations as well as the protection of critical infrastructures.

If the state protection area acts as criminal police for the purpose of law enforcement, the main legal provisions are standardised in the Code of Criminal Procedure (StPO). The criminal police activities of the state protection area are based on the provisions standardised in the StPO.

1.3. Scope of Activities of the Services

State police matters fall within the area of the responsibility of the security police, which is responsible for maintaining public peace, order and security. The authorities responsible for the protection of the constitution, which includes both the Directorate State Protection and Intelligence Service (DSN) as well as the organisational units of the provincial

police directorates responsible for state protection, constitute organisational units of the security authorities pursuant to Article 78a of the Federal Constitutional Law (B-VG).

The Directorate State Protection and Intelligence Service (DSN) was established on 1 December 2021 when the State Protection and Intelligence Service Act (SNG) came into force. The areas of the responsibility of the authorities whose task is to protect the constitution are standardised in the State Protection and Intelligence Service Act.

The protection of the constitution includes:

- the protection of constitutional institutions and their capacity to act as well as the representatives of foreign states, international organisations and other subjects of international law in accordance with international obligations
- the protection of critical infrastructures
- the protection of the population against crime based on terrorist, ideological or religious motives, threats emanating from espionage, intelligence activities and proliferation
- the performance of key functions in the field of international cooperation in these areas.

The clear division between the areas of state protection and intelligence services is an essential element of the protection of the constitution.

The state protection area comprises the preventive protection against attacks endangering the constitution as well as the performance of tasks pursuant to the Security Police Act and the Code of Criminal Procedure in connection with attacks endangering the constitution. The intelligence service area is responsible for tasks related to extended threat investigation, i.e. the surveillance of a group if, considering its existing structures and current developments in its environment, it is to be expected that criminal activity involving a serious threat to public security, particularly ideologically or religiously motivated violence, will occur; and the collection and analysis of information for the purposes of the protection of the constitution.

The above-mentioned matters are performed by the Directorate State Protection and Intelligence Service, which is an organisational unit of the Directorate General for Public Security (Directorate), and the organisational units of the provincial police directorates responsible for state protection in the Austrian federal provinces.

State Protection

In Austria, the tasks related to the area of state protection fall within the competence of the State protection area within the Directorate State Protection and Intelligence Service (DSN) and the organisational units of the provincial police directorates.

The state protection area encompasses the prevention of attacks endangering the constitution as well as the performance of tasks pursuant to the Security Police Act and the Code of Criminal Procedure in connection with attacks endangering the constitution.

The core responsibilities of the state protection area are as follows:

- combatting Islamism and Islamist terrorism
- combatting left-wing extremism, right-wing extremism and subversive associations
- combatting beconomic crimes in connection with the protection of the constitution
- combatting espionage, proliferation and international trafficking of arms, and maintaining and strengthening the areas of protection
- cybersecurity
- prevention
- close protection and physical security
- critical infrastructure protection
- security vetting.

Intelligence Service

The organisational unit responsible for the area of intelligence service within the DSN is particularly in charge of investigating, evaluating and analysing intelligence comprehensively and at an early stage, and of continuously assessing all threat scenarios that are of relevance to the protection of the constitution in Austria, using criteria-based evaluation systems and the corresponding information.

This includes, among other things, protection against crimes based on terrorist, ideological or religious motives and the aversion of threats from espionage, intelligence activities and proliferation. Furthermore, the intelligence service area is responsible for extended threat investigation, which is the surveillance of a group if it is expected that this group will engage in criminal activity involving a serious threat to public security. Apart from specific investigation powers, there are particular methods of intelligence collection available, in order to perform the tasks for the purpose of the protection of the constitution in the best possible manner. In this way, extensive knowledge on the current situation, developments and future scenarios are generated, serving as an early warning system to develop adequate strategies for action.

Another central task covers the strategic area of prevention comprising the coordination, control and promotion of national cooperation. This area comprises the development of strategies and approaches as well as the coordination and implementation of measures in the field of prevention in connection with the protection of the constitution. Moreover, intelligence services regularly communicate and exchange information with other services and cooperate with security-relevant actors both domestically and abroad. Furthermore, the classical scope of responsibilities includes the special protection of sensitive and secret information. In addition, the protection of computer-based systems, cybersecurity and the aversion of cyberespionage constitute essential security tasks of the intelligence service area.

1.4. Control and Supervision Over the Services

Control Within the Scope of the Parliamentary Right of Interpellation

The National Council and the Federal Council are entitled to monitor the administration of affairs by the Federal Government, to query its members on all executive matters and to request all relevant information (Article 52 of the Austrian Federal Constitutional Law – B-VG). This right of control exists vis-à-vis the Federal Government and its members and therefore also vis-à-vis the Federal Minister of the Interior. The right to ask questions is exercised through written, oral and urgent requests as well as during the debate on matters of topical interest.

Review of measures for the protection of the constitutional institutions and their capacity to act by the Standing Subcommittee of the Committee on Internal Affairs.

For the purpose of reviewing measures for the protection of the constitutional institutions and their capacity to act, the Committee on Internal Affairs elects a Standing Subcommittee. The Standing Subcommittee is authorised to request from the Federal Minister of the Interior all relevant information and inspection of the relevant files (Article 52a B-VG).

Independent Control Commission for Constitutional Protection

The control commission is an independent institution not bound by instructions, which was established for the control of the lawfulness of the administration within the meaning of Article 20 § 2(2) B-VG in order to guarantee that the authorities responsible for the protection of the constitution fulfil the tasks that they are entrusted with by law. It is responsible for exercising the accompanying structural control over these authorities. It can become active on its own initiative or at the request of the Federal Minister of the Interior or the Standing Subcommittee.

Control of Public Accounts and Administration of Public Funds by the Court of Audit

The Court of Audit is responsible for the examination of the administration of public funds (Article 121 B-VG). Accordingly, within the scope of the examination of the administration of public funds of the Federal Ministry of the Interior, the Court of Audit is responsible for monitoring the protection of the constitution. The examination shall extend to the accuracy of numbers, compliance with the law, thrift, economic efficiency and expedience.

Control by the Ombudsman Board

As an independent supervisory body, it is the task of the Ombudsman Board to examine alleged maladministration by the federal government. Anyone can lodge complaints with

the Ombudsman Board against maladministration, provided that this person is affected by such maladministration and insofar as legal remedies are not or no longer available. Any such complaint must be investigated by the Ombudsman Board. The Ombudsman Board may investigate its own suspicions in connection with maladministration by the Federation *ex officio* (Article 148a B-VG).

Legal Protection Officer of the Federal Ministry of the Interior

The Legal Protection Officer is an independent institution not bound by instructions, whose independence is preserved to the highest degree through the appointment process and the legal guarantee for the stability of the constitution.

The Legal Protection Officer of the Federal Ministry of the Interior is responsible in particular for the performance of provisional legal protection for individuals who are subjects of covert measures by security authorities (§ 91a et seq. of the Code of Police Practice (SPG) and § 14 et seq. of the State Protection and Intelligence Service Act (SNG)). If the legal protection officer notices that the processing of personal data has infringed the rights of data subjects who have no knowledge of this processing of data, it is the legal protection officer's duty to inform the data subjects or, if this is not possible because it might jeopardise measures that have already been initiated, lodge a complaint with the data protection authority.

Pursuant to § 14 para. 1 SNG, the legal protection officer ensures special legal protection for the tasks pursuant to § 6 para. 1 (extended threat investigation in the intelligence service area) and 2 (prevention of attacks endangering the constitution by a person in the state protection area) SNG and monitors the processing of data according to § 12 para. 6 SNG. Prior to the performance of any of these tasks and if there is intention to set special investigative measures pursuant to § 11 SNG, the authorisation of the legal protection officer shall be obtained.

The legal protection officer shall be granted access to all the necessary documents and records as well as insight into the processing of data according to § 12 para. 1 and 1a SNG at any time, hand over transcripts (photocopies) of individual documents from the archives to him or her free of charge and provide all the information required; in this respect, the claim for official confidentiality cannot be made against him or her. However, this does not apply to information regarding the identity of individuals in accordance with § 162 of the Code of Criminal Procedure (StPO).

The legal protection officer must be given the opportunity to monitor the execution of the measures referred to in § 14 para. 2 at any time, as well as to enter any rooms in which recordings, images or other results of surveillance processes are kept. Furthermore, his or her professional duties also include monitoring the compliance with the obligation to rectify or delete data according to § 13.

The legal protection officer shall submit a yearly report to the Federal Minister of the Interior by 31 March of the following year at the latest, describing his or her activities and any observations made during the performance of his or her duties under this federal act.

Data Protection Authority Within the Scope of the Data Protection Act

The collection of information and processing of personal data is essential for the performance of the tasks of the authorities responsible for the protection of the constitution. The primary task of the Data Protection Authority is to monitor the protection of personal data.

(Administrative) Judicial Legal Protection

According to the SPG, any individual has the right that security police measures against this individual are only carried out in compliance with legal requirements. Following a complaint, the administrative courts may examine the activities of the authorities responsible for the protection of the constitution (Article 129 et seq. B-VG).

1.5. The Legal Status of the Personnel of National Security Services

The employees working in the field of the protection of the constitution include both administrative officials as well as officers of the public security services, i.e. law enforcement officers who are authorised to issue direct orders and execute coercive measures and who perform law enforcement tasks based on the Security Police Act.

Legally speaking, the administrative officers are subdivided into civil servants and contract staff. Pursuant to § 1 para. 1 of the Civil Servants Act (BDG), the civil servants are employees who are employed by the federal government under public law. The civil servants are appointed to their posts by an official notification. Pursuant to § 1 of the Contract Staff Act (VBG), the contract staff are employed by the federal government under a private law service contract. Depending on the type of employment, the employees have different rights and obligations. This includes, for instance, matters relevant to disciplinary law, administrative law and pension law. Regarding their activity in the civil service in general, but also in the area of the protection of the constitution, no distinction is made between the civil servants and the contract staff.

The division into the state protection area and the intelligence service area within the DSN accentuates the distinction between administrative officers and law enforcement staff. In the state protection area, both the administrative officers and the law enforcement staff are employed, whereas the tasks of the intelligence service area are not carried out by the law enforcement staff. The tasks of the intelligence service area are exclusively performed by the administrative officers, who do not have executive powers pursuant to the Security Police Act (SPG). However, § 11 para. 1 SNG provides that in the intelligence service area, suitable and particularly trained staff may perform investigations on the basis of the SNG, which means

that these individuals may carry out the investigative measures listed in § 11 para. 1. Furthermore, it is laid down by law that every staff member of the Directorate State Protection and Intelligence Service shall undergo a reliability examination before taking up his or her duties. The reliability examination is intended to check an individual's reliability based on personal data, which indicates whether there is any reason to believe that the individual might pose a risk to the state protection office.

The reliability examination shall be carried out upon the consent and a declaration of the employee regarding his or her past and current personal circumstances, including information on his or her parents, spouse, registered partner, civil partner and individuals above the age of 18 years living in the same household as the employee (reliability declaration). The matters that form the subject of the reliability examination are laid down in a regulation. Moreover, every employee shall undergo a security check for the 'top secret' level in order to access classified information.

Pursuant to § 2b para. 2 SNG, other suitable and particularly trained staff members employed in the field of the protection of the constitution (administrative officers employed in the intelligence service area) may be provided with service weapons for cases of justified self-defence to defend a human being in the exercise of their official duties and service obligations if, in the course of the performance of their tasks, there may be situations in which they may have to exercise self-defence or defend others by using a service weapon.[1]

2. TASKS AND MANDATE

2.1. Investigative Powers, the Role in Criminal Procedure and Intelligence Tasks

The State Protection and Intelligence Service Act (SNG) regulates the protection of the constitution in Austria. The protection of the constitution is performed as the exercise of the security police. The various tasks and related powers of the authorities responsible for the protection of the constitution and its organs are not only laid down in the SNG. Moreover, the Security Police Act (SPG) and the Code of Criminal Procedure (StPO) govern various tasks of the security authorities and the related powers of the authorities and institutions for the individual areas of responsibility.

In Austria, the authority responsible for the protection of the constitution consists of the areas of state protection and intelligence service. The state protection comprises the preventive protection against attacks endangering the constitution. In addition to that, this area exercises the tasks pursuant to the Security Police Act (SPG) and the Code of Criminal Procedure (StPO) when it comes to preventing attacks endangering the constitution. Therefore, in addition to performing the tasks of the SNG, the state protection area also

[1] See government bill concerning Federal Law Gazette I 148/2021, § 2b para. 2 SNG.

becomes active pursuant to the SPG and the StPO. The intelligence service is responsible for the collection and analysis of information for the purpose of the protection of the constitution and for extended threat investigation. Consequently, the tasks and powers of the intelligence service area are exclusively based on the regulations of the SNG.

In the framework of the Security Police Act (SPG), i.e. in the performance of tasks laid down in the SPG, numerous powers are available to the security authorities and their organs (which normally become active as organs of the public security services) to perform their duties. This requires the existence of concrete tasks pursuant to the Security Police Act (SPG). By its nature, the Security Police Act (SPG) is strongly preventive. The purpose of the Security Police Act is to avert threats. To this end, this act equips the security authorities with various powers. Pursuant to § 21 SPG, the security authorities are responsible for the aversion of general threats. The security authorities must stop dangerous threats immediately. Within the meaning of § 16 SPG, a general threat is defined as a dangerous attack or a criminal association.

A dangerous attack is the threat posed to a legal interest by the unlawful realisation of the elements of a judicially punishable act, which is committed intentionally and is prosecuted not only at the request of the person injured. A dangerous attack also refers to any conduct that is aimed at and appropriate to prepare such a threat as long as it is conducted within a short period of time of the intended realisation of the offence.

If a circumstance corresponding to such a threat arises in the area of the responsibility of the Directorate State Protection and Intelligence Service – meaning that a task pursuant to the Security Police Act (SPG) arises – the respective powers may be exercised by the area of state protection. The same holds true for the protection of constitutional institutions and their capacity to act as well as the protection of representatives of foreign states, international organisations and other subjects of international law, the official and private premises available to them, as well as the staff assigned to them, as provided for through obligations under international law, and for the protection of critical infrastructure.

In the framework of the Security Police Act, the following powers shall be mentioned as examples:

- stopping dangerous attacks
- identity checks
- go-away orders
- the search of premises and persons
- the seizure of objects
- addressing persons considered a threat to public safety for the purpose of deradicalisation
- surveillance
- undercover investigation.

If an individual is suspected of committing a punishable act pursuant to § 22 para. 3 SPG, the provisions of the Code of Criminal Procedure (StPO) shall apply. In parallel, the powers of the SPG and the SNG may be invoked if the respective prerequisites are met.

The Code of Criminal Procedure (StPO) serves to clarify criminal offences and to enforce the state's right to impose punishment. The StPO regulates various tasks and powers of the criminal police, the public prosecutor's office and the courts. For the investigation of crimes, i.e. in the exercise of tasks falling within the remit of the criminal police, the security authorities (within the meaning of § 18 StPO) act as the criminal police.

The StPO also provides for numerous powers, among them:

- seizure
- search
- surveillance
- undercover investigation
- arrest.

The formal requirements for enforcement vary depending on the severity of the encroachment on fundamental rights. The criminal police may partly exercise powers 'on its own initiative'. Most frequently, however, an order of the public prosecutor's office or an additional authorisation by a court is required.

The Federal Act on the Organisation, Tasks and Powers of the Protection of the Constitution (State Protection and Intelligence Service Act – the SNG) defines the tasks of the authorities responsible for the protection of the constitution.

This act defines the following tasks for the two areas:

State protection:

- Preventive protection against attacks endangering the constitution by a person, provided that there is a reason to suspect that the danger of such an attack exists.
- The security police tasks in connection with attacks endangering the constitution.
- The criminal police tasks in connection with attacks endangering the constitution.

Intelligence Service:

- Extended threat investigation; this is the surveillance of a group if, considering its existing structures and developments to be contemplated in its environment, it is to be expected that criminal activity involving a serious threat to public security, particularly ideologically or religiously motivated violence, will occur.
- The collection and analysis of information for the purpose of the protection of the constitution within the meaning of § 1 para. 2 in order to assess threat scenarios that are of relevance to the protection of the constitution.

2.2. Protection of Classified Information

In Austria, the Federal Regulation on Classified Documents (GehSO) regulates the handling of national classified information. Concerning international classified information, the provisions of the Information Security Act (InfoSiG) and the Information Security Regulation (InfoSiV) apply. In terms of content, both regulations essentially follow the same system and lay down uniform standards for the access, handling, storage and transmission of classified information. The federal ministries are responsible in their respective areas for the compliance with and implementation of the provisions of the Information Security Act (InfoSiG), the Information Security Regulation (InfoSiV) and the Federal Regulation on Classified Documents (GehSO). Key standards are developed and adapted in cooperation with the Federal Chancellery as the seat of the Austrian Information Security Commission. Each ministry has an Information Security Commissioner whose primary function is to act as an advisor and who monitors the compliance with and implementation of the legal requirements. As regards the Federal Ministry of the Interior, the function of the Information Security Commissioner forms part of the DSN.

2.3. International Cooperation

The international cooperation of the authorities responsible for the protection of the constitution is based on the provisions of the Police Cooperation Act (PolKG), the EU-Police Cooperation Act (EU-PolKG) and on bilateral and multilateral agreements.

As the central agency in the field of state protection, the DSN is in charge of international cooperation.

The Police Cooperation Act (PolKG) regulates international cooperation within the framework of the security police, criminal justice (criminal police), passport matters, the foreigners police and border control. International mutual police assistance is defined as the mutual assistance in the fulfilment of tasks and cooperation in the joint fulfilment of tasks. The assistance takes place between security authorities and (international) security organisations or foreign security authorities.

Security organisations are defined as international organisations that serve the purpose of police cooperation, i.e. Europol, Interpol or other organisations that have been declared security organisations by decree of the Federal Minister of the Interior.

The Police Cooperation Act (PolKG) provides regulations regarding the performance of administrative assistance, the use of administrative assistance, the legal requirements regarding the transmission of personal data and the intervention of security authorities abroad and foreign security authorities in the federal territory.

The EU-Police Cooperation Act (EU-PolKG) regulates the police cooperation between the security authorities and security authorities of other EU member states as well as the

necessary specifications, in particular regarding the cooperation with Europol pursuant to the Europol regulation.

In addition, there are numerous agreements on police cooperation with other states.

2.4. Personal Data Protection

Pursuant to § 1 para. 1 of the Austrian Data Protection Act (DSG), which has a constitutional status in Austria, every individual shall have the right to the confidentiality of personal data concerning the individual, especially with regard to the respect for the private and family life of the said individual, insofar as that individual has an interest which deserves such protection. The existence of such an interest is ruled out if data cannot be subject to the right to confidentiality due to its general availability or because it cannot be traced back to the data subject.

In Austria, the entry into force of the General Data Protection Regulation (DSGVO) was accompanied by the adoption, or rather the amendment, of the Data Protection Act (DSG). This regulation contains the necessary implementing provisions for the DSGVO. Furthermore, it transposed Directive (EU) 2016/680 into national law.

The processing of personal data for the purposes of the security police, including the protection of the constitution, the self-protection of the military, the resolution and prosecution of criminal offences, the enforcement of sentences and the enforcement of precautionary measures involving the deprivation of liberty is governed by §§ 36 et seq. of the Data Protection Act (DSG).

In addition, the individual acts concerning the protection of the constitution – the State Protection and Intelligence Service Act (SNG), the Code of Police Practice (SPG) and the Code of Criminal Procedure (StPO) – contain numerous specific data protection regulations.

CHAPTER II

Belgium

Hilde Lemmens, Kristof Juchtmans

1. POSITION OF THE VSSE IN THE DOMESTIC LEGAL SYSTEM

1.1. Legal Definition of Special Services

The Organic Act[1] provides concepts relating to the duties, activities and procedures applicable to the VSSE.[2] For example, various threats to national interests have been outlined in the Belgian law.

However, certain other legal notions essential to the VSSE work remain largely undefined in Belgian legislation. For instance, the central concept of 'national security' has not been comprehensively established in the Belgian legislation.

1.2. Position and Role in the Public Administration System

Belgian law provides for only two national intelligence and security services, the VSSE being the civilian service and the ADIV/SGRS being the military intelligence service.[3] The VSSE is considered a domestic civilian intelligence service and has no foreign equivalent.

There are no other Belgian intelligence services, neither on the federal level nor on the regional or local level.

Law enforcement services are organised by federal law and comprise the federal police force and the local police forces among other entities.[4]

---

1 Act of 30 November 1998 regulating the intelligence and security services (Organic Act).

2 For more details, see: *Scope of Activities*.

3 Article 2(1) Organic Act. ADIV stands for *Algemene Dienst Inlichting en Veiligheid*. SGRS is short for *Service Général du Renseignement et de Sécurité*. This translates into 'General Intelligence and Security Service'.

4 Article 3 and Article 4 Act of 7 December 1998 organising an integrated policy force structured at two levels.

The VSSE is working under the responsibility of the federal Minister of Justice,[5] [6] whereas the ADIV/SGRS operates under the authority of the federal Minister of Defence.[7] The VSSE enjoys more autonomy than other divisions of the Ministry of Justice but has no separate legal personality.

The VSSE is independent of the military intelligence service ADIV/SGRS and the law enforcement authorities. Nevertheless, operations are at times conducted in coordination with these entities[8] and (intelligence) information may be shared, as permitted by legislation on classified information,[9] [10] the need-to-know principle and the third-party rule.

1.3. Policy

Several entities are involved in political decision-making which might concern the VSSE:

- The National Security Council,[11] presided over by the federal Prime Minister, the federal deputy Prime Ministers, the federal ministers in charge of Justice, Defence, Interior and Exterior Affairs. The Head of the VSSE will be invited if necessary. The National Security Council determines the national intelligence and security policy.
- The Strategic Committee and the Coordinating Committee for intelligence and security[12] are supporting the National Security Council in preparing and implementing its chosen policy. The Strategic Committee members are representatives of the National Security Council, plus the Coordination Committee's president. The Coordination Committee brings together the heads of service of all government departments and agencies (including the VSSE) involved in intelligence and security policy.

1.4. Control and Supervision

Parliamentary Control

The VSSE operates under the authority of the federal Minister of Justice, who is held accountable by the Belgian Federal Parliament. Members of the Federal Parliament have the right to:

---

5 Article 4 Organic Act.

6 The VSSE Head of Service and Deputy Head of Service are placed under the direct authority of the Minister of Justice by Article 7 Royal Decree of 14 January 1994 creating the status of Administrator General and Deputy Administrator General of the VSSE and by Article 2 Royal Decree of 5 December 2006 on the general administration and the support cell with the VSSE.

7 Article 10 Organic Act.

8 Article 20 Organic Act.

9 Article 19 Organic Act.

10 Article 8 Act of 11 December 1998 regarding the classification and the security clearances, certificates and advice (Classification Act).

11 Royal Decree of 28 January 2015 establishing the National Security Council.

12 Royal Decree of 2 June 2015 establishing the Strategic Committee and Coordinating Committee for intelligence and security.

- interrogate the Minister (via oral or written questions)[13]
- hear the VSSE Head of Service, VSSE Directors or the VSSE staff, or any other civil servants[14]
- start a parliamentary inquiry commission on topics of their own choice (e.g. in response to a national security crisis), with far-reaching judicial powers.[15]

Some of these prerogatives also apply to the Members of Parliament of the federated regions in Belgium.[16]

A dedicated parliamentary commission[17] guides the Standing Intelligence Agencies Review Committee (hereinafter referred to as 'the Review Committee'). This commission is formed by Members of Parliament without a security clearance. This implies that they are entitled to receive only non-classified information from the Review Committee.

External Inspection

a) Review Committee

The Review Committee is the most important supervisory authority for the VSSE.[18]

The Review Committee is both an administrative and a judicial body under the authority of and funded by the Belgian Federal Parliament.[19] It functions completely independently from the VSSE in legal and operational terms. The Review Committee consists of three working members (including one magistrate),[20] the Investigations Department[21] and the Secretariat.

As the principal external supervising authority competent for the VSSE and the ADIV/SGRS, the Review Committee will send the VSSE questions, request (classified) documents or ask to be informed of the VSSE internal procedures. The Review Committee can also directly consult with the Minister of Justice.[22]

---

13 Articles 123–124, Article 127 Rules of the House of Representatives.

14 Occasionally, senior civil servants of government departments or agencies are invited to a hearing organised by a parliamentary commission, on matters that concern that department or agency. The commission can send a report of the hearing to Members of Parliament. Article 32 Rules of the House of Representatives.

15 Article 56 Belgian Constitution. Act of 3 May 1880 concerning parliamentary inquiries.

16 Article 40 Special Act of 8 August 1980 on the reform of institutions.
Flemish Parliament Decree of 1 March 2002 organising parliamentary inquiries.
Walloon Parliament Decree of 15 September 1982.
Order of 16 June 2017 of the United Assembly of the Joint Community Commission (Brussels).

17 Article 66bis Act of 18 July 1991 regulating the supervision of police and intelligence services and of the Threat Analysis Coordination Body (Inspection Act). Rules of Procedure regarding the Guidance Commission adopted by the Belgian Parliament on 26 March 2015.

18 'Comité permanent R' / 'Vast Comité I', Article 33 Inspection Act.

19 Article 28 Inspection Act.

20 Article 28 Inspection Act.

21 Article 40 Inspection Act.

22 Article 33 Inspection Act.

Its legal powers allow the Review Committee to act on its own behalf, as requested by the Parliament, by the Minister concerned or in liaison with the Public Prosecutor's Office.[23]

The Review Committee's competences include:

- **Overall supervision**

The Review Committee supervises the VSSE's compliance with the Belgian law and, more broadly, with the constitutional rights and fundamental freedoms of Belgian citizens.[24]

It also oversees the internal functioning of the VSSE and the collaboration with the ADIV/SGRS[25] and it shall examine any complaints made by members of the general public or other parties concerned.[26] This is considered an administrative competence.

- **Approval of intelligence operations**

Certain methods of intelligence gathering are subject to subsequent control by the Review Committee.[27] Among the Review Committee's powers are imposing the discontinuation of an operation and ordering the erasure of information gathered.[28] No appeal against the Review Committee's decisions is available under the Belgian law.[29] This is regarded as the judicial competence of the Review Committee.

- **Data Protection Authority**

When the VSSE processes personal data, a distinction needs to be made between situations where the General Data Protection Regulation (GDPR) is applicable and where it is not. See *Personal Data Protection* below for a more detailed explanation on the role of the Review Committee.

- **Other competences**

The Review Committee issues advice on draft legislation.[30] Its president is a member of the Appeal Body deciding on procedures against security clearance decisions taken by the VSSE.[31]

Further, the Review Committee's Investigations Department is entitled to inspect the VSSE and its individual staff members concerning criminal acts, disciplinary measures or complaints received.[32] Certain Investigations Department members have powers of criminal prosecution.[33]

---

23 Article 38 Inspection Act.
24 Article 2(1) Organic Act.
25 Article 33 Inspection Act.
26 Article 34 and Article 56 Inspection Act.
27 Article 43/2 Organic Act.
28 Article 43/6 Organic Act.
29 Article 43/8 Organic Act.
30 Article 33 Inspection Act.
31 Article 3 Act of 11 December 1998 establishing the appeal body regarding security clearances, certificates and advice.
32 Article 40 Inspection Act.
33 Article 21 Inspection Act.

Lastly, the Review Committee will report – periodically and ad hoc – to the Belgian Federal Parliament. A yearly report is published on the Review Committee's website.

b) Commission

A dedicated Special Intelligence Methods Commission (hereinafter referred to as 'the Commission') inspects certain intelligence methods operated by the VSSE. It intervenes in authorising, evaluating, modifying and suspending privacy-intrusive methods.[34]

The Commission is an administrative body under the authority of and funded by the Belgian Federal Parliament.[35] It functions completely independently from the VSSE in legal terms. The Commission is composed of three members, all of whom are magistrates. A number of the VSSE staff undertake a secondment to the Commission for administrative support.[36]

See *TASKS AND MANDATE* and *Intelligence Gathering* below for more details.

c) Financial Inspection

The Court of Audit (*Rekenhof / Cour des comptes*) is a Belgian parliamentary institution competent to audit the VSSE budget, bookkeeping and financial transactions.[37] It has autonomous investigative and judicial powers. The Court publishes an annual report on its website.

Internal Inspection

a) Security Clearance

Top Secret clearance is legally mandatory for all VSSE personnel, regardless of their duties.[38] The background checks prior to granting clearance concern the VSSE staff member, their partner and any adults living at the same address. This investigation needs to be repeated every 5 years.

b) Professional Secrecy

All VSSE personnel are legally bound by professional secrecy and an obligation to exercise discretion about their position and their work. This applies to all VSSE staff regardless of their duties. Individuals violating their professional secrecy are liable to prosecution and sanctioning under Belgian criminal law.[39] Professional secrecy will remain applicable after the staff member has left service.[40]

---

34 Article 43/1(1) Organic Act.
35 Article 43/1(1) Organic Act.
36 Article 43/1(5) Organic Act.
37 Act of 29 October 1846 establishing the Court of Audit.
38 Article 2/1, Article 35 and Article 52 Royal Decree of 13 December 2006 on the status of the VSSE field agents.
39 Article 458 Criminal Code.
40 Article 36 Organic Act. In theory, professional secrecy is likewise transferred onto any person cooperating with a VSSE staff member, Article 37 Organic Act.
Article 12 Royal Decree of 13 December 2006 on the status of the VSSE field agents.

c) Database Management

- Mandatory linking of all information to one or more legal duties of the VSSE, in the internal VSSE database.
- Auditing of the VSSE and non-VSSE databases accessed by the VSSE staff (e.g. the National Registry, the criminal record system, the vehicle registration database): monthly checks of random user logs.
- Need-to-know principle: information access is granted by least privilege according to user profile/role.[41]

d) Chain of command

The VSSE Heads of Unit have a reporting duty to their superiors following the chain of command. The Belgian law of criminal procedure requires that all federal government officials (including the VSSE staff members) report certain criminal offences, of which they become aware during their work, to the Public Prosecutor's Office.[42]

e) Disciplinary Law

A Royal decree governs the disciplinary proceedings involving the VSSE personnel.[43] In addition, the VSSE has adopted several internal working guidelines applicable to all staff.

Certain infringements are subject to an investigation and can result in disciplinary sanctions. An appeal against disciplinary decisions or sanctions can eventually be lodged with the Belgian State Council (*Conseil d'Etat / Raad van State*), a dedicated legal court.[44]

f) Data Protection

Data subjects can exercise their legal rights with the competent Data Protection Authorities, but not with the VSSE directly. The VSSE has appointed a Data Protection Officer, who reports to the Head of Service. See *Personal Data Protection* below for more details.

g) Security Officers

Within the VSSE, several Security Officers (*Veiligheidsofficieren / Officiers de Sécurité*) are appointed by the Minister of Justice. One officer is designated as Head of the VSSE Security Bureau.

---

41 Article 2(1) Organic Act and Article 75(3) Data Protection Act.

42 Article 29 Code of Criminal Procedure.

43 Articles 190–223 Royal Decree 13 December 2006 on the status of the VSSE field agents. Articles 77–97 Royal Decree of 2 October 1937 on the status of government staff.

44 Preliminary procedural steps before a disciplinary council and an appeal council apply in certain cases. Article 221 Royal Decree of 13 December 2006 on the status of the VSSE field agents. Article 94 Royal Decree of 2 October 1937 on the status of government staff. Article 14(1) State Council Coordinated Act of 12 January 1973.

Among the duties of the Security Officers are:

- overseeing background (re-)checks
- managing security clearances
- registering and securing classified documents
- organising physical security of the VSSE premises
- training and advising VSSE security clearance holders, and evaluating their compliance.

1.5. Legal Status of the Officers/Employees

The majority of VSSE employees are civil servants who have been individually appointed by Royal Decree under Belgian administrative law.[45] Temporary ICT staff and all cleaning staff have an individual labour contract under civil law.

The VSSE employees are divided in two main categories, depending on whether they mostly work in the field or at the office.

- Field agents are directly involved in intelligence operations, working either outside the VSSE premises or at their desk managing case information or technical procedures to deploy intelligence methods.
- Office employees include analysts handling the information gathered as well as employees in HR, administrative, training and legal or finance roles.

The legal differences between these categories pertain to recruitment, pay, promotion, disciplinary rules and the carrying of arms, among other work aspects.

A limited number of ad-hoc roles exist such as: Security Officer, Data Protection Officer, member of the Intervention Team[46] or Special Accounting Officer. These roles will be filled (temporarily) by selected VSSE employees as a result of exam procedures or by appointment.

Top management members (including Head of Service, Deputy Head of Service and Directors[47]) are assigned for a temporary renewable mandate by the federal Minister of Justice. The federal Minister of Interior Affairs will co-sign the VSSE Head's appointment decision.[48] The delegation of authority from management to officers is regulated by Ministerial Decree.[49]

---

45 Article 2 Royal Decree of 2 October 1937 on the status of government staff. Article 2 Royal Decree of 13 December 2006 on the status of the VSSE field agents.

46 Members of the VSSE selected and trained for the protection of the premises and personnel of the VSSE. Article 22 Organic Act.

47 Head of Service and Deputy Head of Service: Article 2 and Article 4 Royal Decree of 14 January 1994 creating the status of Administrator General and Deputy Administrator General of the VSSE.
Director of Operations: Article 115(1) Royal Decree of 13 December 2006 on the status of the VSSE field agents,
Director of Analysis and Director of Staff Services: Article 4 *quinquies* Royal Decree of 4 September 2014.

48 Article 6 Organic Act.

49 E.g. delegation of signature in public procurement decisions: Ministerial Decree of 16 October 2018 regarding the internal organisation, transfer of powers and authorisation to sign with the VSSE, concerning order placement and execution of public contracts and concerning various expenses.

2. TASKS AND MANDATE

2.1. Investigative Powers and the Role in Criminal Procedure

The VSSE has no general law enforcement tasks.[50] These competences are reserved for law enforcement authorities. However, VSSE intelligence work can take place in parallel to criminal investigations by these authorities.

Whenever VSSE intelligence operations or analysis could risk interfere with such an ongoing criminal investigation, the VSSE has to follow convergence management procedures.[51] These procedures are designed to safeguard the precedence of criminal investigations over intelligence activities. Following these rules, the VSSE will consult with the Public Prosecutor's Office, the Commission and the Review Committee.

All Belgian civil servants are under the legal obligation to report crimes of which they become aware during their work.[52] Specifically for the VSSE, in case intelligence operations would indicate the existence or imminence of a criminal offence, the Commission and the Public Prosecutor's Office need to be informed.[53]

2.2. Intelligence Gathering

Gathering intelligence is considered to be the core business of the VSSE. The provision of the Organic Act listing the VSSE's legal duties features collecting information as the first element,[54] thereby arguably indicating its precedence over other duties.

The Belgian Organic Act has shaped an elaborate legal framework which offers a broad spectrum of intelligence gathering methods to the VSSE. Because the legal wording is technology-neutral, the VSSE field agents will find legal ground for employing a widening range of human and technical intelligence gathering methods. However, in practice, budget constraints, staffing or recruitment limitations, management priorities and the necessities of each case will influence the choice of methods deployed.

Scope of Activities

The Organic Act defines the scope of VSSE activities.[55]

Firstly, the VSSE gathers intelligence on activities which pose a real or potential threat to any of the following interests:

---

50 As an exception to this rule, members of the VSSE Intervention Team are legally mandated to use physical force, including using firearms, in order to protect the VSSE personnel and property. Articles 30 and 31 Organic Act.

51 Article 13/5 Organic Act.

52 Article 29 Code of Criminal Procedure.

53 Article 19/1 Organic Act.

54 Article 7/1 Organic Act.

55 Article 7 Organic Act.

- the domestic national security
- the continuation of the democratic and constitutional order
- the foreign national security
- the international relations of Belgium
- the scientific or economic potential of Belgium.

Threats are further defined as any of the following activities, whether undertaken by an individual or a group in Belgium or abroad:

- espionage
- interference in decision-making
- terrorism
- extremism
- nuclear, biological or chemical weapons proliferation
- harmful sects
- criminal organisations, if linked to any of the above activities.

Moreover, the VSSE is tasked with gathering intelligence on the activities of foreign intelligence services on Belgian territory. Other tasks can be assigned to the VSSE by law.

Competences

The intelligence methods available to the VSSE are arranged in two categories: traditional methods and more privacy-intrusive methods. Explicit legal rules, limitations and procedures are laid down for each category.

Supervision

On the one hand, many traditional methods can be deployed without case-by-case supervision of the Commission. These methods include working with human sources,[56] conducting observation in public,[57] searching government databases,[58] requesting user identification with telecom operators and financial institutions[59] and collaborating with public or private sector entities.[60]

On the other hand, the Commission will need to be involved when the VSSE personnel are involved in more intrusive methods, such as:

---

56 Article 18 Organic Act.
57 Article 16/1 Organic Act.
58 Article 14 Organic Act. Examples include the Automated Number-Plate Recognition database and the Passenger Name Record database.
59 Article 16/2 Organic Act.
60 Article 14 and Article 16 Organic Act.

- observation and searches in public or private places/using equipment[61]
- telecom data requests with telecom operators and capture via technical means: traffic, location and payment method data of communications[62]
- interception of telecom data[63]
- financial data requests: identification of customers and of services used, all transaction details of bank accounts, investment accounts, safe deposit boxes etc., to be obtained from financial institutions[64]
- identification and interception of postal letters and parcels[65]
- accessing public or private IT systems, including by hacking, password cracking and malware deployment[66]
- incorporating legal entities[67]
- travel data requests: all passenger information, including individual movements, to be obtained from private travel companies.[68]

VSSE agents can use a false name or assume a fictitious identity[69] when performing an operation. New legislation regulating infiltration is currently being drafted. These supporting measures are technically not considered to be intelligence methods.

Committing offences during intelligence operations remains formally prohibited, but agents who do so in their line of duty can receive criminal immunity.[70] Conditions apply, such as the necessity and the proportionality of their acts with regards to their mission, the intervention of the Commission in certain cases and the prohibition to physically harm persons.[71]

Procedures

Essentially, depending on the degree of intrusiveness of the intelligence operation, merely notifying the Commission or obtaining its upfront approval before method de-

61 Public places: Article 18/4 and Article 18/5 Organic Act.
Private places: Article 18/11, Article 18/12 and 18/17 Organic Act.

62 Article 18/7 Organic Act.

63 Identification and location data: Article 18/7 Organic Act.
Traffic data: Article 18/8 Organic Act. Note that the current legal provision on data retention has been annulled by the Belgian Constitutional Court further to the Court of Justice Judgment of 6 October 2020 (La Quadrature du Net et al. v. Premier ministre et al., C-511/18). This provision is now being amended.
Content data: Article 18/17 Organic Act.

64 Article 18/15 Organic Act.

65 Article 18/6 and Article 18/14 Organic Act.

66 Article 18/16 Organic Act.

67 Article 18/13 Organic Act.

68 Article 18/6/1 Organic Act.

69 Article 13/2 Organic Act.

70 Article 13/1 Organic Act.

71 Article 13/1 Organic Act.
Note that an exception applies to members of the VSSE Intervention Team, who are legally mandated to use physical force, including firearms. The VSSE Intervention Team members are charged with protecting the VSSE personnel and property. Articles 30 and 31 Organic Act.

ployment is required.[72] These notification and approval procedures are subject to strict legal deadlines.

The VSSE must provide the Commission with regular status reports on certain ongoing operations.[73]

If the Commission decides to suspend or disallow an intelligence method, this will interfere with VSSE operations (planned or in progress).[74]

No appeal procedure against the Commission's decisions is afforded by Belgian law. Yet, the Commission is required to provide the Review Committee with documentation of its decisions and any other relevant information that the Committee would need.[75] The Review Committee has the power to suspend a deployed method and order the destruction of any information gathered by the VSSE.[76]

2.3. Analysis

Analysis of compiled information is the second essential task of the VSSE specified in the Organic Act.[77] All intelligence work is understood to have a clear goal: informing the Government about threats to national security.[78] Thus, when analysis work generates an intelligence product, the VSSE can make a written report available to the competent authorities following the rules on information classification,[79] the need-to-know principle and the third-party rule.

2.4. Administrative Tasks

These tasks relate primarily to security vetting, including security clearance, certificates and advice as well as contributing information.[80]

Security Vetting for the VSSE's Purposes

The VSSE has no general duty[81] to oversee all Belgian security vetting procedures. The competent authority in this domain is the National Security Authority.[82] This authority is a collegiate body with representatives of various government departments and agencies.

---

72 Article 18/10(1) Organic Act.
In extremely urgent cases, the VSSE Head of Service can obtain authorisation directly from the Minister of Justice, Article 18/10(4) Organic Act.

73 Article 18/3(4) Organic Act.

74 Article 18/3(6) Organic Act.

75 Article 18/3(6) and Article 18/10(7) Organic Act.

76 Article 43/6(1) Organic Act.

77 Article 7/1 Organic Act.

78 Explanatory memorandum to the Bill of the original Organic Act, Article 7(2), DOC 49 - 0638/001.

79 For more details, see *Protection of Classified Information*.

80 Article 7(2) Organic Act.

81 See *Protection of Classified Information*.

82 Article 24 Royal Decree of 20 March 2000 implementing the Act of 11 December 1999 regarding the classification and the security clearances, certificates and advice.

Nevertheless, the VSSE remains the competent security authority to issue security clearances to the VSSE personnel.[83] Each person seeking employment with the VSSE will be subjected to security vetting. With obtaining and maintaining Top Secret security clearance being a formal job requirement,[84] all VSSE staff will undergo renewal vetting every five years.[85]

Commissioned Security Vetting for Other Authorities

In a number of security vetting contexts where the National Security Authority is competent for issuing security clearances, certificates or advice, the VSSE carries out administrative tasks in a support role. For instance, the VSSE will provide information to public authorities or private organisations requiring security vetting of their personnel.

Providing Information to Other Authorities

As a matter of principle, the VSSE will solely provide information to the authorities, who are themselves competent to deliver advice. The VSSE will not formally issue positive or negative advice as to the opportunity of the decision.

Examples include:

- informing the Belgian Federal Parliament or Public Prosecutor's Office when they decide on requests by individuals seeking Belgian citizenship[86]
- informing the federal Minister of Interior Affairs when licensing commercial security firms[87]
- informing the federal Government on official requests made by religious communities to be considered a recognised cult.[88]

2.5. ICT security

The VSSE has no collective legal duty to manage or advise other parties on ICT security matters. The VSSE will be responsible for ICT security only within the limits of its own organisation, a task achieved by the VSSE Security Bureau.

The overall duty to supervise, coordinate and monitor the application of the Belgian cybersecurity strategy falls to the Centre for Cybersecurity Belgium.[89]

---

83 Article 4(4) Royal Decree of 20 March 2000 executing the Act of 11 December 1999 regarding the classification and the security clearances, certificates and advice.

84 Article 2/1, Article 35 and Article 52 Royal Decree of 13 December 2006 on the status of the VSSE field agents.

85 Article 15 Organic Act. Article 26 Royal Decree of 20 March 2000 executing the Act of 11 December 1999 regarding the classification and the security clearances, certificates and advice.

86 Article 21 Belgian Nationality Code of 28 June 1984.

87 Article 18 Act of 2 October 2017 regulating private and special security activities.

88 Article 3(1) Federal and regional cooperation agreement regarding the recognition of cults.

89 Article 3 Royal Decree of 10 October 2014 establishing the Center for Cybersecurity Belgium.

2.6. Protection of Classified Information

The VSSE has no collective legal duty to protect classified government information or to issue and manage security clearances. This is the task of the National Security Authority.

Still, as part of its core activities VSSE will be sending intelligence products, possibly including classified information, to competent authorities. Therefore, the VSSE is legally required to secure and protect its intelligence products and other classified information handled by VSSE staff.[90] This includes applying security measures to protect classified information concerning its own personnel, such as security vetting files.[91]

The fact that in practice the VSSE's intelligence products often include classified information creates several challenges.

Firstly, no person may receive classified information from the VSSE unless they hold an appropriate security clearance.[92] This can result in not all persons involved in policy or legislative projects having access to VSSE intelligence products, even if these persons are the lead contacts.

Further, other public authorities on occasion rely on VSSE intelligence products to corroborate their administrative decisions, which are possibly disadvantageous to persons concerned. When these decisions are appealed against, classified information may have to be withheld from parties or their lawyers. This may create tension between the non-disclosure of classified information as evidence and the principle of fair trial (including equality of arms, public character of proceedings).[93]

2.7. International Cooperation

The VSSE entertains regular and fruitful relations with its international counterparts. A general provision for international cooperation is included in the Organic Act.[94] Additionally, the National Security Council has issued guidelines in this matter.

2.8. Personal Data Protection

When the VSSE processes personal data, a distinction needs to be made between situations where the GDPR is applicable and where it is not.

---

90 Articles 8–20 Royal Decree of 20 March 2000 implementing the Act of 11 December 1999 regarding the classification and the security clearances, certificates and advice.

91 Article 13/1 Classification Act.

92 Article 8 Classification Act.

93 Indeed, following recent press reports on court cases regarding the refusal to grant the Belgian nationality and visa revocation, reforms in this area are being discussed.
Relevant jurisprudence of the European Court of Human Rights in the sphere of intelligence services may include:
ECHR Judgment of 19 September 2017 (Regner v. the Czech Republic, 35289/11).
ECHR Judgment of 17 December 2013 (Nikolova et Vandova v. Bulgaria, 20688/04).
ECHR Judgment of 16 April 2013 (Fazliyski v. Bulgaria, 40908/05).

94 Article 20(1) Organic Act.

The GDPR Is Not Applicable

Any processing of personal data by the VSSE, when fulfilling its legal duties imposed by the Organic Act, will generally be out of scope for GDPR purposes.

The Belgian Data Protection Act[95] puts in place Belgian legal restrictions allowed under Article 23 GDPR to safeguard national security.[96] The act regulates certain areas in which the GDPR has left the initiative for further legislation to member states.

As a result, the Data Protection Act creates a stand-alone legal framework for personal data processing by the VSSE. These rules are still inspired by the GDPR but curb the rights that data subjects can exercise towards the VSSE, among other restrictions.

Examples of restrictions created by the Data Protection Act include:

- introduction of 'useful processing'[97] in addition to 'adequate, relevant and limited processing' covered by the GDPR data minimisation principle[98]
- indirect exercise of data subjects' rights with the Review Committee and not with the VSSE directly[99]
- scaled-down powers of the Review Committee as competent authority[100]
- removal of the obligation to keep records of processing activities, replaced by the obligation to keep records of databases used[101]
- the optional character of Data Protection Impact Assessments or advice from the Data Protection Officer or competent authority, which can never be a mandatory preliminary condition to processing.[102]

Notwithstanding these provisions, several other typical GDPR components have not been fully replicated in the Data Protection Act.[103]

The competent Authority is the Review Committee,[104] which has published several advisories in this new capacity on its website.

---

95 The Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (Data Protection Act).

96 Title 3(1) Data Protection Act.

97 Article 74/3 Data Protection Act.

98 Article 5(1)(c) General Data Protection Regulation (GDPR).

99 Article 79 and Article 80 Data Protection Act, Article 51/1 Inspection Act.

100 Article 51/3 Inspection Act. The Standing Committee has fewer advisory, investigative and corrective powers than those listed under Article 58 GDPR.

101 Article 90 Data Protection Act.

102 Article 92 Data Protection Act.

103 This raises a number of legal questions:
- Is the VSSE acting as data processor on behalf of other public or private entities acting as data controller (e.g. the VSSE's administrative support requested by third parties in certain vetting procedures)?
- Which information security safeguards are required when the VSSE – acting as a data controller – appoints data processors (e.g. domestic or foreign companies providing EU/non-EU based cloud services)?
- Are written data sharing agreements mandatory when the VSSE collaborates with other government departments, agencies or private organisations? Which minimal security requirements apply to any exchanges of personal data in such cases?

104 Article 95 Data Protection Act, Article 33 Inspection Act.

The GDPR Is Applicable

Whenever the VSSE processes personal data for other purposes than those duties laid down in the Organic Act, the GDPR will in principle apply.

Examples:

- HR management including recruitment, training, job evaluation and promotion
- ICT management, including digitalisation, security and working from home
- disciplinary procedures, sanctions and litigation
- public relations, networking activities, presentations, talks and events
- public correspondence and public enquiries, including requests to see recorded information held by public authorities.[105]

In these cases, the Minister of Justice as a data controller will need to ensure that the VSSE takes technical and organisational measures to ensure lawful and secure personal data processing in accordance with the GDPR. This entails drafting its own security policies, training and supervising its personnel, executing its multiannual information security plan and responding to security incidents or data breaches.[106]

The competent Authority will not be the Review Committee, but the Belgian Data Protection Authority.[107]

In conclusion, the Data Protection Act does not entirely exclude the GDPR from being applicable to the VSSE activities.

---

105 Such information requests are governed by the Act of 11 April 1994 regarding the publicity of government. Article 6 of this Act compels the VSSE to turn down such requests whenever the protection of national security outweighs the importance of publicity. Nonetheless, dealing with such requests is not imposed by the Organic Act, hence the GDPR will in principle apply to the VSSE's processing of personal data.

106 To this effect, the appointed the VSSE Data Protection Officer will cooperate with the VSSE Security Bureau and Heads of Unit. Article 91(1) Data Protection Act.

107 Article 4(1) Act of 3 December 2017 establishing the Data Protection Authority.

CHAPTER III

Bulgaria

Greta Nikolova, Kristiyana Velinova

1. POSITION OF SERVICES IN THE DOMESTIC LEGAL SYSTEM

1.1. Position and Role of the SANS in the Public Administration System

The State Agency for National Security (SANS) is the counterintelligence (internal) security service of the Republic of Bulgaria.

The agency is a central body of the executive power under the Bulgarian Administration Act and more specifically, a specialised body to the Council of Ministers for the implementation of the policy for national security protection. The SANS is part of the government bodies performing diplomatic, defence, intelligence, counterintelligence, operational and tracing, law enforcement and security guard activities under the Act on the Management and Functioning of the System of National Security Protection (AMFSNSP).

The SANS is headed by a chairperson who is assigned by a Decree of the President, following a proposal by the Council of Ministers.

The Chairperson of the Agency is a member of the Security Council under the Council of Ministers (SCCM), along with the heads of all other security bodies, the Minister of Finance and the Minister of Foreign Affairs and representatives of the President of the Republic of Bulgaria. The Security Council analyses the state of the system for the protection of national security, draws up assessments and proposes solutions and actions to the Council of Ministers. The SCCM also proposes to the Council of Ministers objectives and priorities in the field of national security protection.

The Chairperson of the Agency is also *ex officio* a member of the National Security Consultative Council (NSCC), headed by the President of the Republic of Bulgaria. Members of the NSCC are the Prime Minister, Minister of Defence and the Minister of Interior, the heads of security bodies and members of the Parliament. The NSCC draws up opinions and proposals for issues of the foreign and domestic policy related to national security.

The SANS, the State Intelligence Agency (SIA), the Defence Information Service, the Secretary of the SCCM and the Secretary General of the Ministry of Interior comprise the Bulgarian Intelligence Community, which has serious prerogatives in the field of national security protection, including to draw up proposals to the Council of Ministers to amend and supplement laws and regulations. The authorities of the Community systematically analyse the specificities and dependencies in the security environment, with a view to issuing early warnings, apply measures to exclude, mitigate and prevent risks, and counteract threats and encroachments.

1.2. Oversight and Supervision of the Service

As far as the SANS is concerned, the Bulgarian national legislation envisages certain forms of external oversight.

Under the Act on the Management and Functioning of the System of National Security Protection, parliamentary, administrative, judicial and public oversight is exerted over the activities and bodies of the national security protection organisations, among which is the SANS. The National Assembly exerts oversight over the activities of the State Agency for National Security, the State Intelligence Agency, the Defence Information Service – the Ministry of Defence and over the National Service for Protection via a permanent committee.

Under the SANS Act, the parliamentary oversight over the agency activities is exerted by a special standing committee to the National Assembly and that the chairperson, deputy chairpersons and the officers of the agency are obliged to appear following an invitation in front of the National Assembly or the committee and to present the requested information.

Administrative oversight of the agency is carried out by the Council of Ministers, since the SANS is a security service and a part of the executive power.

The judicial oversight of the agency is related to control regarding offences committed in relation with the agency's activity. The control regarding the application and use of special intelligence means under the Special Intelligence Means Act and requests for access to traffic data stored by providers of electronic communications networks and/or services under the Electronic Communications Act can also be considered as part of the judicial oversight. These acts introduce comprehensive regulations of the procedure for obtaining court permission for the use of special intelligence means and permission to receive traffic data.

The compulsory administrative measures imposed by the Chairperson of the SANS under the Foreigners in the Republic of Bulgaria Act and under the European Union Citizens, Who Are Not Bulgarian Citizens, and Members of Their Families Entry and Residence in and Departure from the Republic of Bulgaria Act, are also subject to judicial oversight.

The public (civilian) oversight is mostly declarative, as it is reduced to the provisions of the Access to Public Information Act, which regulates the social relations pertaining to the right of access to public information. It enables members of the public to form their

own opinion regarding the operation of the entities obligated by law. This act does not allow for access to classified information, with the SANS Act also containing further restrictions for the provision of specific information to individuals.

Despite the fact that the citizens do not have oversight of the SANS' activity, they may submit proposals and signals to the SANS in relation its activities. The procedure for review, forwarding of the documents according to the competence of the respective bodies, checking and resolution of the proposals and signals are determined by an ordinance of the Chairperson of the Agency.

In view of the above, parliamentary oversight remains the main external tool for oversight of the security services.

1.3. Legal Status of the Personnel of the State Agency for National Security

'The personnel of the State Agency for National Security shall consist of civil servants under the SANS Act, civil servants under the Civil Servants Act, and hired employees.

Candidates for appointment as civil servants with the Agency must:

- have Bulgarian citizenship only
- be of legal age
- not be placed under legal disability
- have no prior conviction for a premeditated crime of a general nature, regardless of whether they have been rehabilitated since; nor have been acquitted of criminal liability for a premeditated crime of a general nature
- not be barred from holding certain positions in the civil or public service
- not have been arraigned as suspects or defendants in a criminal case of a general nature
- not have been previously dismissed from office for disciplinary reasons
- meet all general and specific requirements for holding the position applied for.'[1]

Similar requirements are stipulated in the SANS Act regarding the candidates for appointment as hired employees.

Noting the specific activities performed by the State Agency for National Security, the SANS Act regulates some restrictions in performing some basic rights towards all or certain categories agency's officers.

The officers of the agency are not allowed to be members of political parties or coalitions, or of organisations with political purposes; they are not allowed to carry out political activity or to undertake other activities as servants which violate their political neutrality. The agency personnel shall have no right to strike.

[1] SANS Act (SG 2007), Article 53, p. 1.

The civil servants of the agency shall have no right to join trade unions or to engage in trade union activities.

The agency personnel shall have the right to associate among themselves for the performance of activities of mutual interest outside their official duties, without thereby violating the established internal order in the agency and the principle of unity of command.

The subject of the activity of such associations shall not comprise the functions already performed by the agency.

The agency personnel are not military, but civil servants.

2. TASKS AND MANDATE

The State Agency for National Security is Bulgaria's primary counterintelligence structure and its main functions include the identification of risks to national security and to the collective security of the EU and NATO (both internal and external) and maintaining an integrated system for prevention, counteraction and minimisation of harmful consequences.

'The State Agency for National Security independently or jointly with other state bodies performs counter-intelligence activities for the surveillance, detection, counteraction, prevention and interception of plotted, prepared or perpetrated encroachments against national security, including within the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army.'[2]

2.1. Investigative Powers and the Role in Criminal Procedure

Currently, the SANS does not have investigative powers.

2.2. Analytical Tasks

The agency performs functions pertinent to information analysis, forecasts, control, coordination and technical assistance, using their own information or information supplied by other government authorities, of significance to national security.

The agency performs operative search, operative-technical, information and analytic activities pertinent to surveillance and monitoring of persons, facilities and activities.

Its functions include countering threats for the national security of Bulgaria connected with:

- hostile intelligence activities
- sovereignty and territorial integrity of the state and the unity of the nation
- unconstitutional activities
- internal and international terrorism
- economic and financial security

[2] SANS Act (SG 2007), Article 4, p. 2.

- environmental security
- disruption of the proper functioning of the National System for the Protection of Classified Information
- critical infrastructure security
- communication and information systems
- proliferation and international arms trade
- illegal migration processes.

According to Article 4 of the SANS Act, the agency performs activities for the protection of the national security and the sovereignty of the Republic of Bulgaria, its territorial integrity, the fundamental rights and freedoms of the citizens, the democratic functioning of the state and the public institutions and the functioning in the country of the constitutional order.

In view of the above fields, the SANS has the following roles:

- **Counterterrorism**

The agency is a coordination centre and a focal point for counterterrorism issues, including risks related to crossings of foreign fighters, attempted creation of terrorist cells on our territory, plans for terrorist acts in Bulgaria or abroad, radicalisation of individuals and groups, anti-constitutional activity, attempted use of force or of items of hazardous nature to political ends.

The National Counterterrorism Centre functions within the SANS, carrying out operational cooperation and 24/7 information exchange with the Ministry of Interior, the State Intelligence Agency, the Defence Information Service in the Ministry of Defence as well as with the partner services and structures engaged in countering terrorism from all EU and NATO member states.

A national unit to gather and process air passenger name records (PIU) was established within the SANS, in the implementation of Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

- **Counterintelligence**

Under the SANS Act, the agency works on the detection, prevention and neutralisation of the risks and the limitation of the potential vulnerabilities of the Bulgarian national security and the collective security of the EU and NATO evolving from the activities of foreign special services.

- **Military Counterintelligence**

The establishment of the SANS in 2008 led to the integration of the civil and the military counterintelligence (MCI). The MCI units of the agency perform tasks counteracting encroachments against national security within the Ministry of Defence, whose structures

are directly subordinated to the Minister of Defence and the Bulgarian Army, as well as tasks related to the protection of the defence interests of the EU and NATO.

- **Risk Migration**

One of the priorities of the SANS is to limit the risk of infiltration in the migration influx of individuals related to terrorist groups and foreign security services and of granting legal resident status to risk individuals. The agency has exclusive rights to the implementation of the control activities on the stay of foreign nationals in Bulgaria by issuing an obligatory position regarding entering the country as well as regarding any change of the status of foreign nationals in Bulgaria.

- **Counterproliferation**

The SANS counteracts encroachments related to the international trade in weapons and dual-use products or technologies as well as the manufacture, storage, distribution and use of weapons of mass destruction. The prevention of violations of the EU, UN and OSCE sanctions is a priority. The agency established the National Counterproliferation Coordination Centre in order to exchange information with competent Bulgarian authorities and foreign partner cervices and to coordinate the counterproliferation activities.

- **Financial Security**

The focus is on negative impact on the financial and credit system, attempted tax and social insurance system fraud and money laundering as well as on the illegal absorption of EU funding. The national financial intelligence unit (FIU) of the Republic of Bulgaria is a part of the SANS and it implements the national legislation and the international agreements against money laundering and the measures against the terrorism financing.

- **Economic Security**

The focus is on the protection of facilities or activities of a strategic nature in the general government, energy, transport, communications, healthcare, production and dissemination of food, ecology, science and technology.

- **Counteraction to Harmful Impact on Communications and Information Systems and Strategic Sites**

The focus is on those built and maintained in strategic installations and on securing strategic activities relevant to the national security. This includes vetting procedures for granting access to strategic installations and activities.

Together with the State Agency for Technical Operations, the SANS is authorised to apply special intelligence means (SIMs) and to carry out technical checks about the presence and usage of unregulated SIMs within premises of the state authorities.[3]

[3] Special Intelligence Means Act, Classified Information Protection Act, SANS Act, Regulation of the system of measures, tools and means for the physical security of the classified information and the terms and order for their use, adopted with a Decree of the Council of Ministers No. 52 of 2003 (Promulgated, SG No. 22/2003).

2.3. Administrative Powers

In order to perform the activities described above, SANS officers have a number of powers. Operative search activities are among the major activities performed by the agency and they are carried out through:

- 'taking statements from citizens
- the performance of searches in databases in respect of individuals engaged in criminal activities, as they may constitute a threat to national security
- taking samples for comparative testing
- the marking of sites or objects
- the investigation of objects or documents
- surveillance
- the identification of persons or objects
- gaining entry into and performing investigations of premises, buildings, transport vehicles or parts of localities
- the monitoring of postal, telegraphic or other correspondence
- the monitoring of telephone calls
- information gathering from technical communication channels
- operative infiltration
- operative experiment
- making verbal or written warnings to discontinue violations of the legal order, as they may constitute a threat to national security
- the operative verification of the evidence gathered and its recording
- the performance of cross-checks on the basis of documents
- the monitoring of the radio frequency spectrum
- the setting up and usage of not-for-profit legal entities or commercial companies subject to terms, conditions and procedure as provided by law.'[4]

The SANS Act empowers its officials to carry out the surveillance and monitoring of persons, facilities and activities related to encroachments upon and threats to national security, as well as to gather, process, store and use data obtained from the investigation of facts, persons and facilities related to the security of the Republic of Bulgaria. In this regard, the SANS Act regulates the powers related to processing personal data, where collecting information about citizens only on racial signs or ethnic origin, political, religious or philosophical beliefs and membership in political parties, organisations, associations with religious, philosophic, political or syndic purposes, as well as information about the well-being of the person or his or her sexual life, is strictly forbidden.

---

[4] SANS Act (SG 2007), Article 20, p. 1.

In performing their duties and in case of proved operational need, the SANS officials could be appointed to undercover positions in the state administration, in legal entities, civil associations, as well as freelancers, except for lawyers' activities. The undercover process and the activities of the SANS officers are carried out while respecting the principles of lawfulness and conspiracy. The undercover agents carry out counterintelligence work and operative search activities in order to protect the national security.

The operative search activities could be carried out through the services of citizens who have voluntarily undertaken to cooperate with the bodies of the agency in the discharge of their functions. The recruitment and functions of the persons are carried out in compliance with the principles of 'voluntary recruitment, hiring and discharge; protection in the course of, or pertinent to, such collaboration; keeping in the strict confidentiality of the identity and other personal data of such persons, as well as the nature of their activity.'[5]

For the purpose of doing activities in countering terrorism and risk migration, the SANS bodies could carry out interviews with foreign nationals who illegally entered or are illegally residing on the Bulgarian territory.

In order to guarantee the effective undertaking of activities countering terrorism, the SANS officers are authorised to detain a person known by them to have committed a criminal offence in relation to terrorism or a terrorist-related crime for a period of 24 hours.

The officers of the agency have the right to detain a person who breached the security and the rules for entering the area of a protected agency site.

Detainees are transferred to the officers of the Ministry of Interior (MoI) who convoy the detained persons to a detention facility within the structures of the MoI.

In relation to the detention powers of the SANS officers, there are also those regarding the body search of detained persons.

In relation to protecting the national security and for the purpose of the prevention and detection of serious crimes, in the frames of their competence, the SANS officers use and deploy special intelligence means subject to the terms, conditions and procedure as per the Special Intelligence Means Act. They are also granted access to traffic data according to the Electronic Communications Act.

Along with the powers mentioned above, for the purpose of undertaking the activities related to the security of Ministry of Defence and the structures directly subordinate to the Minister of Defence and the Bulgarian Army, the SANS officers:

- provide for and assure the counterintelligence capabilities of the Bulgarian troops participating in operations and missions outside the territory of the Republic of Bulgaria and of the national military formations made available as collective defence capabilities and for the purposes of NATO operations

5 SANS Act (SG 2007), Article 23, p. 3.

- have access to bases and facilities of the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army
- receive directly from the commanders and base commanders of the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army, the information necessary for the discharge of their powers and duties and for assuring the security of the armed forces
- perform functions pertinent to the protection of the classified information of the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army, pursuant to the Classified Information Protection Act
- provide opinions in respect of decisions, plans, materials and others relevant to the security of the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army
- issue binding instructions for action in case of an emerging threat to the combat readiness, the information, economic and financial security, as well as in case of endangering the security of the facilities and activities of the Ministry of Defence, the structures directly subordinate to the Minister of Defence and the Bulgarian Army.

The officers of the agency may issue verbal or written warnings to persons, in the case of whom there is sufficient evidence to suggest that they may commit criminal offences or other acts endangering the national security.

In discharge of their duties, the SANS officers may demand information of the government authorities, institutions, legal entities and private individuals as well as the officers of the agency can summon members of the public to their offices. In this regard, the law envisages a sanction (a fine) for an officially summoned person who fails to appear without a valid reason.

In the discharge of their duties, the officers of the agency have the right to carry firearms as well as to use physical force and auxiliary devices only when this is absolutely necessary.

2.4. Protection of Classified Information

Counteraction to encroachments against the National System for the Protection of Classified Information, with a focus on the physical, documental, personal and industrial security as well as on the security of information systems and networks for classified information.

The SANS functions as a national authority for cryptographic security and a national authority for the accreditation of automated information systems/networks. In its capacity as an authority responsible for the developing and exploiting the Unified Secure Communications and Information System and the Unified Cryptographic Network for Electronic Systems, the agency conducts the electronic exchange of official correspondence between the structures of the state government of the Republic of Bulgaria and it also administers

and maintains the points of presence of the Republic of Bulgaria along the communications and information systems for the secure exchange of EU information.

Taking into account its responsibilities for protecting classified information, the SANS conducts security vetting within all state structures and the agency itself (with the exception of the security and law enforcement structures), which in turn expands our capabilities for acquiring information.

CHAPTER IV

Croatia

Daniel Markić

1. POSITION OF THE SERVICE IN THE DOMESTIC LEGAL SYSTEM

1.1. Legal Definition of Special Services

The Security-Intelligence Agency (hereinafter referred to as 'the SOA') is a state body established by the Act on the Security Intelligence System of the Republic of Croatia[1] (ZSOS) of July 2006 for the purpose of systematic gathering, analysis, processing and evaluation of information relevant for the national security, with the aim of detecting and preventing activities, by individuals or groups, directed against the viability, independence, integrity and sovereignty of the Republic of Croatia, aiming at the violent overthrowing of the state authority structures; threatening to violate human rights and basic freedoms established by the Constitution and the legislation of the Republic of Croatia and to endanger the fundamentals of the economic system of the Republic of Croatia, required for reaching decisions that are relevant for the successful achievement of national interests in the field of national security. The SOA is both a security and an intelligence agency.

The same act establishes the Military Security Intelligence Agency (hereinafter referred to as 'the VSOA').

1.2. Position and Role of the Services in the Public Administration System

The SOA is part of the security intelligence system of the Republic of Croatia. The system is made up of the Office of the National Security Council (UVNS), the SOA, the VSOA, the Operation Technology Centre for Telecommunication Surveillance (OTC) and the Institute for the Information Systems Security (ZSIS).

[1] Act on the Security Intelligence System of the Republic of Croatia, Official Gazette, Nos. 79/06 and 105/06 – amendment.

The National Security Council is at the top of the system's hierarchy; it is co-chaired by the President and the Prime Minister and it is in charge of facilitating cooperation between the President and the government by providing guidance for the work of security and intelligence agencies. The operational coordination of the work of security intelligence agencies falls under the purview of the Council for the Coordination of Security Intelligence Agencies, which is chaired by the Deputy Prime Minister in charge of national security. The National Security Advisor to the President and directors of the SOA, the VSOA and the UVNS also sit on the Council.

The UVNS performs expert and administrative functions for the National Security Council and the Council for the Coordination of Security Intelligence Agencies, performs functions which facilitate the National Security Council to analyse the reports of security intelligence agencies and to evaluate the fulfilment of the objectives set for security and intelligence agencies, to evaluate the implementation of the decisions of the President of the Republic and the Prime Minister on directing the work of the security intelligence agencies, and the functions facilitating the President of the Republic and the Prime Minister to supervise the performance of the security intelligence agencies.

The UVNS also integrates the reports and the information received from the security intelligence agencies, drafts periodic reports covering different areas of security intelligence activity and analyses as well as evaluates the security-related information relevant for the national security of the Republic of Croatia and essential for the execution of constitutional powers of the President of the Republic and the Prime Minister.

The UVNS is the central state authority body responsible for determining and implementing activities relating to the application of information security measures and the adoption of information security standards in state authority bodies in the Republic of Croatia, and for the coordination of activities with respect to the application of the information security measures and standards in the exchange of classified information between the Republic of Croatia and foreign countries and organisations.

The ZSOS also establishes the OTC for the purpose of the activation and management of the measures of the secret surveillance of telecommunication services, activity and transmissions and in order to enable the operational/technical coordination between the legal and the natural persons operating public telecommunication network and providing public telecommunication services and access services in the Republic of Croatia and the bodies authorised to apply the measures of the secret surveillance of telecommunications pursuant to the ZSOS and the Criminal Procedure Act. In cooperation with the bodies authorised for the application of the measures of the secret telecommunication surveillance in accordance with this act and the Criminal Procedure Act,[2] the OTC is authorised to su-

[2] Act and the Criminal Procedure Act, Official Gazette, Nos. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19.

pervise the work of the telecommunication services providers, i.e. their fulfilment of the obligations provided by the ZSOS.

The ZSOS also establishes the ZSIS which performs functions in the fields of information systems and networks security, of security accreditations for the information systems and the networks in the state authority bodies, of handling of the crypto materials used in the classified data exchange between the state authority bodies of the Republic of Croatia and foreign countries and organisations, and of the coordination of the prevention and the removal of problems related to the security of computer networks in the state authority bodies. The ZSIS also conducts research and works on the development and testing of technologies intended for the protection of classified data, and issues certificates for the use thereof.

1.3. Scope of Activities of the Services

The SOA performs the functions from its scope of work pursuant to: the national security strategy, defence strategy, annual guidelines for the work of security intelligence agencies, laws, requests submitted by certain legally authorised state authority bodies or requests by the users of the results produced by security intelligence agencies, in accordance with the Croatian Constitution, laws and other regulations.

On the territory of the Republic of Croatia, the functioning of the SOA is directed against activities or actions aimed at threatening the constitutional order, the safety of state authority bodies, that of citizens and of the national interests through:

- terrorist acts and other forms of violence
- intelligence activity of foreign intelligence services, organisations and individuals
- organisation of extremist activities of groups and individuals
- endangering the safety of top state officials and protected facilities and areas
- organised and economic crime
- unauthorised access to protected information and communication systems of the 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
- other activities aimed at endangering national security.

The SOA collects, analyses, processes and assesses the political, economic, scientific/technological and security-related information concerning the foreign countries, organisations, 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.

The SOA's mission is to collect and analyse data pertinent to national security in order to identify, investigate and comprehend threats and challenges to the national security, thus providing the government and other bodies a reliable basis for decision-making and action in protecting the national security, interests and welfare of Croatia's citizens.

The SOA's vision is a modern, efficient and responsible security and intelligence agency adapted to current demands and focused on fulfilling its mission and top performance, with a significant national and regional reach and distinguished abilities, top quality workforce and strong partnerships.

The VSOA is a structural unit of the Ministry of Defence intended to provide planning and implementing support to the Ministry of Defence and the Armed Forces in their performance of duties in the area of the protection of the viability, sovereignty, independence and territorial integrity of the Republic of Croatia. The VSOA collects, analyses, processes and assesses information on the armies and defence systems of other countries, on external pressures which might influence the defence security and on the international activities directed against the defence security of the country. On the territory of the Republic of Croatia, the VSOA collects, analyses, processes and evaluates information regarding the intentions, potentials and plans for actions by certain persons, groups and organisations in the country, the objective of which is to threaten the defence capabilities of the state, and takes measures aimed at identifying, monitoring and combating such activities.

1.4. Control and Supervision of the Services

The oversight of the SOA's work is five-fold: parliamentary, professional, civil, judicial and internal.

The parliamentary oversight is conducted by the Croatian Parliament directly or through the Parliamentary Committee for Internal Affairs and National Security.

In the effectuation of the oversight, the Croatian Parliament may request:

- from the SOA, reports on the actions and measures that it implements
- from the President of the Supreme Court of the Republic of Croatia, reports on the measures of secret information gathering or on such measures applied to certain persons
- from the SOA, reports on the implementation of the measures of secret information gathering or on the implementation of the measures of secret information gathering applied to certain persons
- reports on whether the security intelligence agencies collect information regarding any members of the Parliament or any person from their family households.

In the effectuation of the oversight, the Croatian Parliament or the Parliamentary Committee competent for national security may request that the UVNS submits a report and information and/or performs a professional inspection of the SOA.

In addition to the foregoing, the Committee of the Croatian Parliament competent for national security is also authorised to summon the SOA Director and the officers to hearings regarding the illegality of the application of certain measures and actions by the agencies, to discuss the SOA's financial management, to review the Ombudsman's reports on the protection of the constitutional and legal rights of citizens in the procedures undertaken by the SOA and to look into its work with respect to the foreign policy of the Republic of Croatia.

Information disclosed to the Croatian Parliament or the Parliamentary Committee competent for national security may not include information on the persons, with whom the SOA has collaborated in the performance of its functions, or information obtained from foreign intelligence and security services/agencies without their prior authorisation, or a decision by the National Security Council.

The UVNS conducts professional oversight of the SOA. Within the framework of its professional oversight functions, the UVNS:

- monitors and controls the legality of the work
- monitors and controls the attainment of prescribed objectives and purview
- monitors and controls the effectiveness and usefulness of the work
- controls the application of the measures of secret information gathering that restrict the basic rights and freedoms guaranteed by the Constitution
- controls the use of financial resources
- supervises the coordination and the cooperation between the SOA and the corresponding services of other countries.

When conducting oversight, the UVNS may have access to the reports and other documents of the SOA and it may interview its Director and officers.

The SOA is obliged to permit the officers of the ONSC, at their request, to have access to the data concerning the sources of the agency only if that is necessary for the fulfilment of the final goals of the inspection control undertaken for a specific case, and in case of an explicit disagreement with the request, the SOA Director shall request the decision on the specific case to be made by the National Security Council.

When, in the performance of the professional oversight, the UNVS establishes that actions of the SOA have been, or are, violating the Constitution and the laws of the Republic of Croatia, the Head of the UVNS must undertake measures for the immediate removal of the detected irregularities and inform the President, the Prime Minister and the Speaker of the Croatian Parliament about it if the inspection was performed at the request of the Croatian Parliament or the Parliamentary Committee competent for the national security.

The Council for the Civilian Oversight of the Security Intelligence Agencies conducts the civil oversight of the SOA's work. This council performs the following functions:

- It monitors the legality of the work of security intelligence agencies.
- It monitors and controls the implementation of the measures of secret information gathering that restrict basic rights and freedoms guaranteed by the Constitution.
- It delivers, in the form of a piece of information, the obtained information and data referred to in the previous items, to the National Security Council, the Speaker of Croatian Parliament, the President of the Parliamentary Committee competent for national security and to the SOA Director.
- It provides information about the procedure for the submitting of the request referred to in Article 112 of the ZSOS.

When conducting oversight, the Council may have access to the reports and other documents of the SOA and interview its Director and officers.

The Council performs the oversight pursuant to the programme adopted by the Parliamentary Committee competent for national security, based on the requests submitted by citizens, state authority bodies and legal persons, regarding the observed unlawful actions or irregularities in the SOA's work, especially in cases of violations of basic freedoms and human rights guaranteed by the Constitution.

The information regarding the conducted oversight inspection is reported to whoever had submitted that request. In its reply to the submitted request the Council shall refer only to the remarks listed in the request, where, in the conducted oversight, it is established that there have been some unlawful acts, the chairman of the Council shall notify the President of the Republic of Croatia, the Speaker of the Croatian Parliament, the Prime Minister and the Chief Public Attorney about the results of the oversight. At the request of the Speaker of the Croatian Parliament, and at least once every six months, the Chairman of the Council submits reports on the work of the Council.

The Council is composed of a chairman and six members, all appointed by the Croatian Parliament. For the legality of their work, the chairman and the members of the Council are responsible to the Croatian Parliament. The chairman and the members of the Council are obliged to keep the secrecy of the information they have learnt while performing the functions in the Council. They shall be obliged to do so even when they leave the Council.

The SOA's work is also subject to internal oversight. The judicial oversight of the SOA's implementation of the secret information collection measures is carried out by the Supreme Court which approves measures of covert data collection, which temporarily restrict certain human rights and basic freedoms guaranteed by the Constitution. Proposals for the application of secret information collection measures are submitted by the SOA Director, who is required to justify the validity of the proposed measures.

Additionally, in some cases, for instance, those concerning citizens' rights, such as security vetting, issues related to foreigners' status etc., the oversight of the SOA may be carried out by competent Croatian courts.

1.5. Legal Status of the Officers/Employees

The ZSOS defines the legal status and powers of SOA officers. In matters not regulated by this act, the provisions of the Act on Civil Servants[3] or the Act on the Obligations and Rights of State Officials[4] apply to the officials and employees of the SOA, the VSOA, the UVNS, the ZSIS and the OTC, whereas the provisions of the Act on Service in the Armed Forces of the Republic of Croatia[5] apply to the employees of the VSOA who are in active military service.

Particular provisions applying to the SOA employees also concern hiring. The public announcement of vacancies in the SOA is not mandatory. Persons admitted to work in the SOA, in addition to common requirements stipulated by the Act on Civil Servants, must also satisfy specific requirements for the admission and assignment to certain jobs (specific education and profession, working experience, special skills and training, special health and psychical capabilities etc.), stipulated by the SOA ordinances on the internal order. The persons hired must also comply with the security requirements, which is established through a security vetting procedure. Security vetting is conducted with the approval of the person that is being hired and it covers the vetted persons' spouses and persons living with them in the same household. If the person being hired does not give his or her approval for the security vetting procedure, the employment contract cannot be concluded with him or her. Persons may not be hired if there are impediments to their admission to civil service. If a person was not hired due to the non-compliance with the conditions or due to the presence of impediments to the admission, the SOA is not obliged to explain the reasons for such denial. The employment of the persons who were hired as trainees may be terminated during the period of their traineeship if, in the course of the traineeship, it is assessed that they do not display capabilities necessary for the performance of work in the SOA.

Furthermore, the ZSOS defines particular obligations for the staff in the SOA. The SOA officers are obliged to perform the work at the work posts to which they are assigned, even in situations where their lives, health or property are at risk. In addition, if ordered by their superior officer, they are obliged to perform their duties after working hours if

---

3 Act on Civil Servants, Official Gazette, Nos. 92/05, 140/05, 142/06, 77/07, 107/07, 27/08, 34/11, 49/11, 150/11, 34/12, 38/13, 37/13, 1/15, 138/15, 102/15, 61/17, 70/19, 98/19.

4 Act on the Obligations and Rights of State Officials, Official Gazette, Nos. 101/98, 135/98, 105/99, 25/00, 73/00, 30/01, 59/01, 114/01, 153/02, 163/03, 16/04, 30/04, 121/05, 151/05, 141/06, 17/07, 34/07, 107/07, 60/08, 38/09, 150/11, 22/13, 102/14, 103/14, 03/15, 93/16, 44/17, 66/19.

5 Act on Service in the Armed Forces of the Republic of Croatia, Official Gazette, Nos. 73/13, 75/15, 50/16, 30/18, 125/19.

that is necessary for the successful and timely completion of the official duty, for which they are entitled to financial compensation or to days off, pursuant to the SOA ordinance on the internal order.

The SOA employees are forbidden to apply for membership in political parties, to participate in activities thereof, to act on behalf of any political party within the SOA or to perform any other public or professional function. They are also forbidden to apply for membership in executive or managing boards of companies or of corresponding bodies of other legal persons. Furthermore, they are not allowed, without the approval of the Council for the Coordination of Security Intelligence Agencies, to make public statements or to make comments on the work of the service and of other bodies and persons in the field of national security or to disclose the SOA information and documents to unauthorised persons.

The SOA Director and staff who had access to information and documents of the SOA or of other bodies within the security intelligence system are obliged to keep the secrecy of legally classified information and documents, regardless of the way that they were disclosed to them until, pursuant to the same legal act, they are free from keeping the secrecy thereof. These persons may not misappropriate documents belonging to the SOA or to other bodies of the security intelligence system. Failure to comply with these obligations will result in dismissal. The SOA employees have the duty of confidentiality even after they leave the service.

On the other hand, the ZSOS also provides for special protection of the SOA staff, who are guaranteed specific rights other than those enjoyed by other civil servants. In this sense, the SOA and other bodies of the security intelligence system are obliged to maintain the secrecy of the identity of the SOA employees, secret collaborators, persons assisting the SOA and that of other sources of information and to protect the manner in which the information is obtained.

If criminal proceedings have been initiated against the SOA officers for acts committed in the performance of the SOA functions, the agency shall ensure that they receive legal assistance unless the proceedings were initiated based on the criminal report submitted by the SOA.

The SOA concludes life insurance contracts for their employees or the insurance for cases of death or work-related loss of working abilities and the work-related property losses.

On the basis of the decision of the SOA Director, upon the termination of service due to the requirements of the service, the employees of the SOA may exercise their right to an old age pension, regardless of their age, when they have completed 30 years of the pension insurance, of which at least 15 years of the pension insurance on duties or functions where the actual work performed is counted as an extended period of pension insurance, pursuant to the provisions of the Act on the Pension Insurance Rights of Active Servicemen, Police Officers and Civil Servants with Official Powers.[6]

[6] Act on the Pension Insurance Rights of Active Servicemen, Police Officers and Civil Servants with Official Powers, Official Gazette, Nos. 128/99, 16/01, 22/02, 41/08, 97/12, 118/12.

The SOA employees whose employment is terminated due to the fulfilment of the conditions for the retirement are entitled to severance pay. The SOA Director and officers are entitled to an extended 'bonus period of pension insurance', meaning that each 12 months of actual service or employment are counted as 15, 16, 17 or 18 months of pension insurance.

The ZSOS also defines special instances of abuse of office for the SOA employees. The following constitute minor breaches of official duty, in addition to the minor breaches of official duty defined by the Act on Civil Servants:

- unprofessional conduct by the SOA employees towards the citizens or the employees of other state authority bodies
- disclosing information relative to the scope of work of a SOA structural unit to unauthorised employees of other structural units.

The following constitute major violations of official duty, in addition to the violations of official duty as defined by the Act on Civil Servants:

- irregular spending of allocated funds or spending for unintended purposes
- making false statements concerning the SOA
- taking, or failure to take, any action, with a view to preventing or curbing the performance of SOA functions
- making false or incomplete statements to bodies of oversight
- disclosing SOA information to unauthorised persons, regardless of its classification level
- taking a classified document out of the agency's working facilities, unless authorised to do so by an immediately superior officer.

For major violations of official duty or for disciplinary offences, the SOA employees may, in addition to punishments for violations of the official duty stipulated by the Act on Civil Servants, be pronounced a disciplinary punishment of termination of the employment, conditionally, in the duration of 3 to 12 months.

For minor breaches of official/working duty or for disciplinary breaches, the proceedings are conducted and decisions passed, at the recommendation of a superior person, by the SOA Director or persons designated by them. For major violations of the official/working duty, at the recommendation of the Director or persons designated by them, the proceedings are conducted and the decisions are reached by special disciplinary courts.

The ZSOS also regulates particularities concerning the departure from service. In addition to the cases of termination of service defined by the Act on Civil Servants, the service of the officers of the SOA shall be terminated if it is established that, by negligent performance of their functions or by violation of rules and regulations regulating the work of

the SOA, they have obstructed the performance of functions from the scope of activities of the SOA. Obstructing the performance of functions includes overstepping one's powers or failure to exercise them, as a result of which damage is incurred to natural or legal persons, the SOA, state authority bodies or the Republic of Croatia.

In addition to the cases where the service of officers of SOA is terminated *ex lege*, as laid down by the Act on Civil Servants, the service is also terminated *ex lege*:

- when the competent body establishes that he or she has met the conditions for the retirement on account of general or professional incapacity
- when it is established that the employee has given false information at the time of admission to service
- when an officer is convicted for a criminal offence prosecuted *ex officio*, except for the offences relating to transport security
- if an officer refuses a legal relocation
- when it is discovered that the officer has acted contrary to the provision forbidding him or her from taking an active part in politics or other public or professional duty
- when it is learnt that he or she has acted contrary to the previsions of keeping the secrecy of legally classified information and documents.

On the basis of the decision of the SOA Director, for those employees of security intelligence agencies who have completed 20 years of social insurance, of which they have spent at least 10 years on duties or functions where active work is counted as a prolonged period of pension insurance, and who, through an appropriate procedure, have been found incapable of further professional growth, service may be terminated due to professional incapacity for work, with an entitlement to a disability pension.

2. TASKS AND MANDATE

2.1. Investigative Powers and the Role in Criminal Procedure

The SOA has neither investigative nor law enforcement powers. The Criminal Procedure Act stipulates that personal data collected by the SOA and used to identify the defendant may, in some cases, be used as evidence in specific criminal cases involving terrorism and terrorism financing.

2.2. Intelligence Gathering

Within the scope of its activities, the SOA gathers information from publicly available sources, through communication with citizens and requesting data from state authority bodies, local authority bodies and regional self-government, legal persons, including through access to registers and databases and to the official documentation and by applying secret procedures and measures.

When the SOA officers gather information through communication with citizens, making formal inquiries or requesting other forms of assistance, the officers are obliged to identify themselves by presenting their official identification cards and badges. Interviews in the official premises of the SOA may be conducted with citizens only with their expressly stated consent. Such interviews are recorded by technical means and, by signing the minutes, citizens confirm the voluntary nature of the interviews and verify the authenticity and the integrity of the recorded conversations.

The SOA has an obligation to protect the identity of persons registered as secret collaborators and, if necessary, ensure their physical safety and the safety of their families and the security of their property.

The officials and employees of the state authority bodies and those of local (regional) self-government bodies and of legal persons with public authority are obliged to comply with the requests of the SOA regarding the data available to them within their respective scope of activity.

State authority bodies, units of the local (regional) self-government and legal persons as well as the members of the Ministry of Defence and the Armed Forces may maintain records of all effectuated accesses to their respective databases, registers and documentation, which may include only the numbers of badges or the numbers of the official identification cards of the SOA officers. Records of the numbers of the badges or the identity cards of the officers of security intelligence agencies shall be kept separate from other records. The officials and employees of these bodies must keep the secrecy of all knowledge disclosed to them on the matters of interest to the SOA.

The SOA may apply measures of secret information gathering, which temporarily restrict certain constitutional human rights and basic freedoms. The measures of secret information collection, which temporarily restrict certain constitutional human rights and basic freedoms, may be applied if the information cannot be obtained in any other way or the collection thereof is linked with disproportionate difficulties. In cases where a choice between several different measures of secret information collection is possible, the one that is less invasive to constitutionally protected human rights and basic freedoms shall be applied.

The measures of secret information gathering include:

a) Secret surveillance of telecommunication services, activity and traffic:
   - secret surveillance of the communication content
   - secret surveillance of the telecommunication traffic data
   - secret surveillance of the location of the user
   - secret surveillance of international telecommunications.
b) Postal censorship
c) Secret surveillance and technical recording of the interior of facilities, closed spaces and objects

d) Secret surveillance and monitoring, with recording of images and photos of persons in the open and public spaces
e) Secret surveillance and monitoring, with audio recording of the content of communication between persons in the open and public spaces
f) Secret purchase of documents and objects.

Depending on the measure, its application is approved either by the Croatian Supreme Court or the SOA Director.

The Supreme Court approves the following measures:

- secret surveillance of the communication content
- postal censorship
- secret surveillance and technical recording of the interior of facilities, closed spaces and objects
- secret surveillance and monitoring, with audio recording of the content of communication between persons in open and public spaces.

These measures may last up to four months, but they may be renewed based on the decision of a council composed of three authorised judges of the Supreme Court.

The SOA Director approves the following measures:

- secret surveillance of the telecommunication traffic data
- secret surveillance of the location of the user
- secret surveillance of international telecommunications
- secret surveillance and monitoring, with recording of images and photos of persons in open and public spaces
- secret purchase of documents and objects.

2.3. Analytical Tasks

The SOA uses the information collected to draft appropriate analytical reports within its scope of work, concerning specific security challenges and illegal activities of individuals and groups.

Reports and analyses provide a comprehensive overview of specific security challenges relevant to national security and national interests. The reports also contain current and long-term forecasts. The SOA circulates reports containing intelligence to authorised structures.

All relevant information collected in their work and the assessments of the security situation are reported by the SOA to the President of the Republic of Croatia, the Speaker of the Parliament, the Prime Minister and the UVNS. Ministers and other state officials receive reports relating to their respective areas of responsibility. When the collected intel-

ligence indicates that a criminal act which is prosecuted *ex officio*, is being planned or committed, the security intelligence agencies shall notify the Public Attorney's Office thereof.

Annual reports on the SOA activity are submitted to the President of the Republic of Croatia, the Speaker of the Croatian Parliament, the Chairman of the Parliamentary Committee competent for national security, the Prime Minister and the Head of the UVNS and, at their request, they also receive special reports about the national security situation in their respective scopes of activity.

2.4. Administrative Tasks

Administrative tasks at the SOA are in charge of legal, HR and finance departments. They entail issues regarding the legality of the SOA activities, constructive HR management aiming at ensuring the excellence of its workforce, employee rights, daily operation and resources needed to meet its objectives.

In addition, it should be noted that the SOA establishes and maintains databases and registers of personal data, and other records of the collected information and documents with the data related to its scope of activity as well as other records relating to their functions and activities. In this sense, the SOA is obliged to inform the citizens, within 15 days at their request, in writing, if measures of secret information collection have been applied to them or if files with their personal data are kept, and to allow them access to the collected data, at their request. Documents inspected by the citizens must not contain information on the employees of the security intelligence agencies or any information about the sources of the security intelligence agencies or any third persons. The SOA is not required to do so if the information would jeopardise the fulfilment of the agency tasks and the information could result in a threat to the security of another person. As soon as these reasons cease to exist, the SOA is obliged to proceed in the manner stated above. Also, if the information could result in consequences harmful for the national security and the national interests of the Republic of Croatia, the SOA does not have to comply with the request before the expiry of a period of 10 years following the date of the termination of the application of the measure.

2.5. ICT Security

Information system security is an area of information security defined by the Information Security Act.[7]

An information system is a communicational, computer or other type of electronic system within which information are processed, stored or transmitted in such a way that they are available and applicable to authorised users.

---

[7] Information Security Act, Official Gazette, No. 79/07.

The UVNS and the ZSIS are central state authorities in charge of information security.

The UVNS coordinates and harmonises the adoption and implementation of information security measures and standards in the Republic of Croatia and in exchange of classified and unclassified data with foreign countries and organisations. The UVNS shall adopt ordinances on personnel security standards, physical security standards, standards of the security of information, an ordinance on the INFOSEC organisation and management standards and on industrial security standards.

The ZSIS is in charge of the technical aspects of INFOSEC in bodies and legal persons using classified and non-classified data. The aspects include: information systems security standards, information systems security accreditations, managing crypto materials used in the exchange of classified data and coordination of prevention and response to security threats to the information systems security.

2.6. Protection of Classified Information

On the territory of the Republic of Croatia, the functioning of the SOA is against the activities or actions aimed at threatening the constitutional order, the safety of state authority bodies, that of citizens and the national interests through, among other things, the disclosure of classified information by state officials or the employees of state authority bodies, scientific institutions and legal persons with public authority.

It should be noted that the Criminal Code also provides for a prison sentence to whoever makes secret intelligence entrusted to him or her available to unauthorised persons.

The SOA carries out the operational aspect of security vetting required for certificates allowing access to classified information, counter-surveillance inspections and must, like all other state agencies, adhere to regulations regarding the protection of classified data and information security in general, as enacted by the UVNS and the ZSIS.

Classified information is also protected by the obligation of the officials and employees of the SOA and other bodies of the security intelligence system, who had access to their information and documents, to keep the secrecy of legally classified information and documents, regardless of the way that they were disclosed to them until, pursuant to the same legal act, they are free from keeping the secrecy thereof.

2.7. International Cooperation

Based on their international commitments, the SOA may cooperate with foreign security, intelligence and other corresponding services through the exchange of information, equipment, through jointly conducted activities from their respective scopes and through the education of employees. The establishment and the suspension of the cooperation with each foreign service are approved by the National Security Council on the basis of the recommendations of the directors of the security intelligence

agencies and the previously obtained opinion of the Council for the Coordination of Security Intelligence Agencies.

The SOA may communicate to the appropriate foreign services the information on a citizen of the Republic of Croatia if they have been provided with relevant data indicating that such a person is a threat to the national security of the state, to which the data are supplied, or to values protected by the international law. The information will not be provided if that would be contrary to the interests of the Republic of Croatia or if the protection of the interests of the person concerned is of greater value. Classified information may only be shared with countries and international organisations which signed the agreement on mutual protection of classified data with the Republic of Croatia. Classified information may also be shared with international partners as part of the classified information exchange.

When the SOA conducts security vetting requested by a foreign service or an international organisation of a person seeking employment in the state authorities of foreign states or in the bodies of international organisations, it shall be conducted upon the receipt of a written consent of the vetted person.

2.8. Personal Data Protection

In the national security system, personal data are handled exclusively as classified. Their protection and right of access, as well as sanctions for abuse thereof is defined by the law.

Para. 16 of the preamble to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), states, *inter alia*, that the Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security.

Furthermore, Article 2(2) of that Regulation states that the 'Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law.'

Furthermore, the General Data Protection Regulation's Article 23 (Restrictions) provides that 'Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard', *inter alia*, national security.

Article 1(2) of Croatia's Act on the Implementation of the General Data Protection Regulation[1] states that the Act does not apply to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, nor does it apply to the areas of national security or defence.

1 Act on the Implementation of the General Data Protection Regulation, Official Gazette, No. 42/18.

CHAPTER V

The Czech Republic

Michal Koudelka

1. POSITION OF THE SERVICE IN THE DOMESTIC LEGAL SYSTEM

1.1. Position and Role of the Services in the Public Administration System

In the Czech Republic, there are three intelligence services – the BIS, the Office for Foreign Relations and Information (UZSI – a foreign intelligence service) and the Military Intelligence.

The Security Information Service (hereinafter referred to as 'the BIS') was established as an armed intelligence service of the Czech Republic on the day when Act No. 154/1994 Coll. on the BIS entered into force, i.e. on 30 July 1994. It is a counterintelligence service active within the Czech Republic. The BIS builds on its post-1990 predecessors, the Office for the Protection of the Constitution and Democracy within the Federal Ministry of Interior, the Federal Information Service within the Federal Ministry of Interior, the Federal Security Information Service and the Security Information Service of the Czech Republic. The BIS is also governed in its activities by the Constitution of the Czech Republic, the Charter of Fundamental Rights and Freedoms, international treaties and other legal regulations of the Czech Republic.

The Director of the BIS is appointed by the government, following a discussion by the respective committee of the House of Deputies responsible for security matters. In matters regarding the execution of his or her responsibilities, the BIS Director reports to the government, which also has the authority to dismiss him or her. Within the organisation of public administration, the BIS falls under the government.

The Military Intelligence, just like the BIS, is governed by individual legislation, in this case, Act No. 289/2005 Coll. on the Military Intelligence, and it is a military foreign and counterintelligence service. Legal provisions concerning the status, scope of powers

and responsibilities, coordination, cooperation and oversight of the intelligence services, their tasking and their reporting duties and the provision of information to the intelligence services are stipulated in Act No. 153/1994 Coll. on the Intelligence Services of the Czech Republic. Legal provisions concerning the use of specific means of acquiring information and personal data records kept by the BIS and the Military Intelligence are stipulated by Act No. 154/1994 Coll. on the BIS as well as by Act No. 289/2005 Coll. on the Military Intelligence. These acts also regulate the status of service members and their contract of service.

More specific and detailed provisions concerning the contract of service of BIS and UZSI officials can be found in Act No. 361/2003 Coll. on the Service Contract of Members of the Security Forces or in Act No. 221/1999 Coll. on Professional Soldiers in the case of Military Intelligence officials. All three intelligence services are headed by directors and are legally defined as state agencies for the acquisition, collection and evaluation of information important for protecting the constitutional order, major economic interests, security and defence of the Czech Republic.

Since 1 July 2021, the Military Intelligence, which is part of the Ministry of Defence, has been contributing to the defence of the Czech Republic in cyberspace to the extent stipulated by Act No. 289/2005 Coll.

Apart from the legally defined scope of powers and responsibilities, intelligence services also complete other tasks defined by special legislation or international treaties by which the Czech Republic is bound. The internal structure of the intelligence services and a more specific scope of their activities are defined by intelligence services statutes approved by the government. The government is responsible for the activities of intelligence services and coordinates them.

The BIS is one of the seven security forces listed in Act No. 361/2003 Coll. on the Service Contract of Members of the Security Forces together with the Police of the Czech Republic, the Fire Rescue Service of the Czech Republic, the Customs Administration of the Czech Republic, the Prison Service of the Czech Republic, the Inspectorate General of the Security Forces and the UZSI, which falls under the Ministry of Interior. Security forces together with armed forces, rescue corps and emergency services ensure the security of the Czech Republic, as stipulated by Section 3(1) of constitutional Act No. 110/1998 Coll. on the Security of the Czech Republic. Other bodies obliged to participate in safeguarding the security of the Czech Republic are state authorities, bodies of self-governing territorial units and natural and legal persons. The BIS cooperates with state authorities and institutions – most often ministries, central administrative offices, security forces or armed forces.

The income and expenditures of the BIS are defined in a separate chapter of the state budget.

1.2. Scope of Activities of the Services

The UZSI acquires, collects and evaluates information of foreign provenance important for the security and protection of the foreign political and economic interests of the Czech Republic.

The Military Intelligence acquires, collects and evaluates information of foreign provenance important for the defence and security of the Czech Republic, on the intelligence services of foreign powers in the area of defence, on schemes and activities directed against the safeguarding of the defence of the Czech Republic and on activities endangering classified information concerning the defence of the Czech Republic.

The BIS acquires, collects and evaluates information (i.e. carries out mainly operational and analytical activities) on:

- schemes and activities directed against the democratic foundations, sovereignty and territorial integrity of the Czech Republic
- the intelligence services of foreign powers
- activities endangering classified information
- activities the consequences of which may jeopardise the security or major economic interests of the Czech Republic
- organised crime and terrorism.

As for the activities falling under the first point, the BIS monitors phenomena, opinions or activities aimed against the system, i.e. the ones which, directly or in their consequences, endanger the state's democratic foundations (mainly its constitutionality, protected values, declared human rights and civil freedoms) or those aimed at destabilising the existing democratic, political and socio-economic system, replacing it by an antagonistic system (totalitarianism, dictatorship, anarchy) and conducting deliberate destructive activities against the existing system. Thus, the BIS looks into the activities of entities that openly or covertly profess ideologies incompatible with the legal system and democratic foundations of the Czech Republic, entities engaging in politically, economically or socially motivated activities which instigate actions against the democratic system of the Czech Republic, promote the use of violence against representatives of the democratic system of the Czech Republic, their ideological opponents and other groups of citizens or call for the limitation of the rights of certain groups of citizens. The BIS also monitors related phenomena that may, mainly in the long term, increase tensions within the society and contribute to citizens' distrust in the democratic principles and the legal system of the Czech Republic.

In the field of counterintelligence, the BIS looks into activities undertaken by foreign powers and by natural or legal persons acting in the interest of foreign powers or foreign intelligence services. The counterintelligence activities of the BIS have two major functions – to inform legally stipulated addressees about the activities, interests and inten-

tions of foreign powers in the Czech Republic (the informative function) and to suggest or adopt measures aimed at hindering or disrupting foreign intelligence operations in the Czech Republic (the preventive function). Therefore, the main aim of the BIS in this field is to avoid leaks of classified and sensitive information and devices to foreign powers, to openly or discreetly hinder the activities of foreign intelligence services as well as to detect and disrupt operations extending the influence of foreign powers (disinformation, manipulation, deceit, propaganda).

In terms of protecting classified information, the BIS is tasked with protecting people and entities who work with classified information and with evaluating and highlighting key points where there is a danger of disclosure. If the BIS identifies warning indications of an attempt at a breach of information security, it takes action to eliminate it.

The activities of the BIS which fall under the fourth point include cybersecurity, protection of the state's economic interests and countering proliferation. As for cybersecurity, the BIS, for instance, looks into various types of cyberattacks affecting the protected interests of the Czech Republic or in general gathers and analyses information on real and potential threats and risks that endanger strategic information and communication systems, since the destruction or disruption of such systems could seriously impact the security or economic interests of the Czech Republic. These systems include systems run by state offices, public administration authorities and other legal persons, also from the private sector, that require increased security protection, given their importance or their potential inclusion on the list of critical infrastructure entities of the Czech Republic. In order to ensure cybersecurity, the BIS also keeps track of various online discussion boards used to trade personal data or other sensitive information or those used as a market for supplying and demanding different types of cyberattacks and exchanging know-how. In terms of major economic interests, the BIS informs authorised state representatives about risks threatening those economic interests of the Czech Republic in order to ensure that they have all relevant information for their key economic decisions, e.g. information on external attempts to influence these decisions, on the plans of entities posing a threat or on covert interests tied to these plans. In the field of major economic interests, the BIS focuses mainly on power engineering, transport, public health, telecommunications, banking or tax collection and on phenomena endangering these economic interests, such as negligence within the state, legal but harmful business activities, incorrect lobbying or illegal activities. The BIS aims to prevent direct financial losses and threats to energy security or other important infrastructure. Within the field of countering proliferation, the BIS focuses on the activities of state and non-state actors and their procurement networks aimed at obtaining strategic materials, devices, individual components, technologies and know-how that may be used for the research, development and production of weapons of mass destruction. Countries of proliferation concern perceive the Czech Republic as a country with developed industry,

a high-quality and accessible education system and a wide scientific base. In this context, there are several thousand entities active in the Czech Republic that could potentially be involved in proliferation activities.

In terms of organised crime, the BIS focuses mainly on informal non-institutionalised structures taking form of lobbyist and clientelistic networks or creating parallel power structures. These structures use illegal or illegitimate methods in order to threaten or disrupt the legality and independence of state power and the legitimacy of decisions made by state authorities, harm public budgets and assets and in consequence weaken public trust in state authorities. Legally stipulated powers and responsibilities of the BIS state that the BIS is not responsible for investigating specific (organised) criminal activities and imposing criminal sanctions. The main role of the BIS is to discover and offset the negative impacts of organised crime on the exercise of state power, the state's constitutional, political and social stability and on its international perception and inform legally stipulated addressees. As for terrorism, the BIS has been appointed the central intelligence service responsible for processing analytical and field intelligence related to the security of the Czech Republic, especially fighting against terrorism. Given that nowadays, terrorism is above all an international phenomenon affecting the whole world, the BIS focuses on international cooperation in this area. Its fight against terrorism is characterised by a pragmatic approach to assessing potential threats to the interests of the Czech Republic or evaluating the possibility of an attack on buildings, citizens or interests of other states being carried out in the Czech Republic. The BIS is also interested in activities aimed at recruiting new members, obtaining financial or logistic support for terrorism and promoting radical interpretations of ideologies or religions which support terrorist activities.

1.3. Oversight and Supervision of the BIS

The activities of the BIS are subject to oversight by the government, the Parliament and the Independent Authority for the Oversight of Intelligence Services of the Czech Republic (hereinafter referred to as 'the Independent Oversight Authority'). The Independent Oversight Authority has not been established yet, but it has been agreed that it shall not be able to enquire into the activities of the BIS which took place prior to 1 January 2018 (when Act No. 325/2017 Coll. entered into force). As a result, the Independent Oversight Authority is allowed to investigate matters which took place before its establishment, but not before 1 January 2018.

The scope and manner of the oversight of the BIS are partly provided for in the Act on the Intelligence Services of the Czech Republic and partly in the Act on the BIS. Even though the law does not describe the exact extent or specific manner in which the oversight by the government should be carried out, the government's oversight powers are based on

its entitlement to assign tasks to the BIS and to assess their fulfilment. This means that the oversight by the government focuses on all activities of the service.

The activities of the BIS are also supervised by the House of Deputies, which sets up a special supervision body, which is the Standing Oversight Commission for the oversight of the BIS.[1]

The Standing Oversight Commission is composed of at least seven members; at present, the Commission has nine members. The House of Deputies decides on the number of the Commission's members in a way that all political groups established by deputies of individual political parties or movements for which they stood in the elections are represented. The members of the Commission may enter the facilities of the BIS when accompanied by the Director or an officer designated by the Director for this purpose. The Director submits to the Commission the statutes of the BIS, a draft budget and other documents needed for inspecting the correct budget implementation, written terms of reference for assignments issued by the government or the President of the Czech Republic, internal regulations on the use of specific means of acquiring information, information regarding the types of records kept by the service and their administration. Following a request by the Commission, the Director of the BIS also submits a report on the activities of the service, a report on the use of intelligence means, the number of cases in which the BIS is carrying out its activities with the usage of intelligence technology, summary information and the number of cases and matters in which the BIS is still active, the number of cases investigated by the BIS in which a bank or similar institution was requested to provide a report (see Section 1.4.: *Legal Status of the Officers/Employees* for further information) and a report on the use of such requests. Should the Commission be of the opinion that the activities of the BIS unlawfully undermine or damage the rights and freedoms of citizens, it is authorised to request a due explanation from the Director. The Commission is obliged to notify the Director and the Supreme State Prosecutor (Attorney General) of each breach of law by members of the BIS, which it identifies during the performance of its function.

The above-mentioned mechanisms constitute what can be seen as the direct oversight of the BIS. The law also provides for indirect oversight, as the government informs the House of Deputies, i.e. the Standing Oversight Commission about the activities of the intelligence services once a year and whenever it is requested to do so, as well as each time when information is obtained which is important for the protection of the constitutional order, major economic interest security and defence of the Czech Republic.

Following a complaint from one of the responsible oversight bodies, the Independent Oversight Authority investigates the work of the BIS on the territory of the Czech Republic in terms of legality and respect for fundamental rights and freedoms.

---

1 http://www.public.psp.cz/en/sqw/snem.sqw?id=1563

As mentioned earlier, no members of the Independent Oversight Authority have been appointed yet, although the Authority has been established by the law. The Independent Oversight Authority is composed of five members who are nominated by the government and elected by the House of Deputies for a period of 5 years.

The members of the Independent Oversight Authority are not allowed to have served in or worked for a security force of the Czech Republic or to have worked or served as professional members in the armed forces of the Czech Republic in the 3 years prior to taking their office. The members of the Authority exercise their powers independently while being bound only by the Code of Administrative Procedure of the Czech Republic; they exercise their powers impartially and only to the extent permitted by the law and they refrain from any action which might undermine trust in their impartiality, which means in particular that they should not let themselves be influenced by the interests of political parties or movements, public opinion or by the media.

When performing its duties, the Independent Oversight Authority is authorised to request necessary information from the BIS regarding its work in connection with the enquiry conducted by the Authority.

The BIS is not required to provide the Independent Oversight Authority with information which might:

- undermine the objectives of an ongoing operation; the intelligence service shall not provide such information only with the prior consent of the Prime Minister
- reveal the identity of officers of the BIS
- reveal the identity of persons acting in favour of the BIS
- put other persons whose safety constitutes a major interest pursued by the BIS in danger
- contravene the requirement made by intelligence services of foreign countries in terms of disclosure of information to third parties.

Should the Authority come to the conclusion that the work of the BIS constitutes an illegal breach of fundamental rights and freedoms or a breach of law, it is authorised to request a due explanation from the Director of the BIS. Based on its enquiry into the work of the BIS, the Authority shall produce a written report which shall clearly say whether and in what way the case in question constituted an illegal breach of fundamental rights and freedoms or a breach of law by the BIS. The Authority shall submit its written report to the Standing Oversight Commission on whose complaint it opened its enquiry and also to the Director of the BIS. The conclusion made by the Independent Oversight Authority regarding possible breaches of fundamental rights and freedoms or possible breaches of law shall be made public in a way enabling remote access. Should it establish that the BIS is responsible for an illegal breach of fundamental rights and freedoms or a breach

of law, the Authority shall provide the Director of the BIS, the Prime Minister or relevant cabinet ministers with recommendations to be made in order to remedy any shortcomings.

The Independent Oversight Authority is required to notify the Prosecutor General's Office of any suspected criminal acts committed by BIS officers, which were uncovered during an enquiry. The Authority is required to notify the Director of the BIS of opening an enquiry.

Oversight regarding the service's management of state assets and of the funds allocated to the BIS from the state budget is carried out by responsible national authorities, such as the Supreme Audit Office. Other oversight activities regarding the BIS can be undertaken only if approved by the Director of the BIS. If the approval is not granted, the BIS arranges for such oversight activities within its scope of powers and responsibilities and submits a report on such activities to the oversight body which requested the approval. If the BIS is not able to arrange for such oversight activities within the scope of its powers and responsibilities, it is obliged to allow for their execution by the oversight body. The service may reserve special conditions regarding the manner in which the oversight activities are to be carried out.

It should also be noted that on its own initiative, the BIS publishes an annual report on its activities for the general public, containing non-classified information on the most notable issues and cases regarding intelligence work. The report includes general statistical data,[2] providing the public with an insight into intelligence activities and allowing it to participate in supervising the work of the BIS.

1.4. Legal Status of the Officers/Employees

In the execution of their responsibilities, the officers are obliged to act in such a way as to avoid prejudicing the respectability and dignity of other persons as well as their own and to make sure that by their activities they do not cause damage or other unreasonable injury to any person. The character of the BIS is of an armed security force, with hierarchy based on the superiority/subordination system and with officers who carry out the orders and instructions from the commanding superiors in the service.

The contract of service of BIS officers is regulated by Act No. 361/2003 Coll. on the Service Contract of Members of the Security Forces. The officers establish their affiliation with the BIS by presenting their service card with a registration number and by an oral declaration, i.e. by saying the words: 'Security Information Service'. The crest of the BIS consists of the greater coat of arms of the Czech Republic, which is positioned on the breast of an eagle, which is a symbol of astuteness, vigilance, speed, tenacity and authority. The service's motto in Latin – *Audi, vide, tace* – is placed at the top of the crest, capturing

[2] Annual Report of the Security Information Service for 2020. See http://www.bis.cz/annual-reports/

the principal qualities of good intelligence officers, who have to be good listeners with a perceptive mindset and keep silent about their work. All BIS officers take the following pledge on the first day of service: 'I pledge on my honour and conscience that I will not be biased in fulfilling my service duties; that I will observe legal and service regulations, follow the orders of my superiors and never abuse my position. My behaviour will never jeopardise the good reputation of the service. I will fulfil my service tasks properly and dutifully and will not hesitate to risk my life in order to protect the interests of the Czech Republic.' Should the officer fail or refuse to take the pledge or should the officer take the pledge with any reservations, the contract of service cannot be concluded.

The officers of the BIS are entitled to hold and carry service firearms and use them in case of legitimate self-defence or in distress. The BIS also employs a number of people who are not officers but work under a contract of employment, as provided for in Act No. 262/2006 Coll., the Labour Code, and who constitute a special category of employees with extra duties, such as the obligation of secrecy, limitations to private business activity, a prohibition against accepting gifts and other benefits or limited membership in a range of organisations.

On top of that, the BIS has the power to conduct a security clearance process – i.e. it issues or cancels security clearance – when it comes to the service's officers, employees and those applying for a position within the service.

Additionally, the BIS and the UZSI act as health insurance authorities with regard to the rights and duties of their respective officers in health-related matters (the Ministry of Defence assumes the same responsibilities with regard to the Military Intelligence).

The officials of the BIS and the UZSI are responsible for matters concerning the contract of service of their respective officers, including any misdemeanour committed by the officers.

According to the Code of Criminal Procedure, law enforcement authorities are courts, public prosecution and police authorities. The police authorities include a designated body within the BIS, the Inspection Department of the BIS, which prosecutes crimes committed by the BIS officers. The department's main task is to uncover and investigate these crimes by finding the leads and gathering evidence.

2. TASKS AND MANDATE

2.1. Limits to the BIS Powers

The Czech intelligence services are intelligence services without executive powers. They cannot arrest or interrogate citizens. It is not the responsibility of the intelligence services to gather evidence enabling arrests and leading to criminal prosecutions. The Czech intelligence services identify threats, issue early warnings and take steps to eliminate the threats. In this respect, the work of the services differs from that of the police, who do not intervene

before a criminal offence is committed. If an intelligence service approaches a citizen with a request, it is entirely up to the citizen whether he or she will grant its request or not.

Even though no legislation prohibits the use of intelligence findings in legal proceedings, the case-law of the Constitutional Court indicates that information obtained by means of interfering with the rights and freedoms of citizens cannot be used as evidence, since there is no legal basis for doing so. This rules out the possibility of using intelligence findings in proceedings carried out by courts as well as by administrative authorities.

The topic of creating a legislative framework for the use of intelligence findings as evidence in criminal proceedings is currently open and being discussed.

2.2. Informing the State Authorities

The government and the President of the Czech Republic have the right to task the intelligence services within the scope of the services' powers and responsibilities. The President is entitled to task the BIS with the knowledge of the government. Furthermore, each intelligence service submits a report on its activity to the President and the government annually or whenever requested.

The President, the Prime Minister and relevant cabinet members also receive reports from the intelligence services on urgent findings as they emerge. Furthermore, the intelligence services provide findings to state and police authorities, provided that such information falls within their powers and responsibilities and that sharing this information does not jeopardise a major interest pursued by the service. The BIS submits reports and information via its Director, who also transmits tasks assigned to the BIS. Information can be shared with the President, the Prime Minister and relevant cabinet members as well as with state and police authorities only with the knowledge of the Director of the BIS.

2.3. Intelligence Gathering

In compliance with its powers and responsibilities, the BIS may request that public administration bodies provide necessary assistance and information stored by these bodies in relation to fulfilling state administration tasks. The public administration bodies shall provide their assistance and information as requested without undue delay and for free unless otherwise provided for by specific legislation. The intelligence services are also authorised to request information obtained in relation to tax administration and data from the relevant information systems of administrative authorities in a way which enables constant and, if technically possible, remote access. The intelligence services are authorised to request information to the extent necessary for fulfilling a specific task or for undertaking measures related to registered data protection.

The BIS is authorised to submit a written request to banks and branches of foreign banks, savings and credit cooperatives or other entities authorised to provide payment services on

commercial basis to provide a report on matters related to their clients subject to bank secrecy or other data of a similar type. The BIS is authorised to make written requests for such reports also with regard to a future period of time. In both cases, it can only do so in order to fulfil a specific task falling under its powers and responsibilities and only in cases in which obtaining necessary information using other means would be ineffective, substantially more difficult or, in a given case, impossible. The BIS is authorised to request such a report or reports only after obtaining a warrant issued by the Chairman of the Panel of Judges of the High Court in Prague. The provision of future reports may be authorised only for the absolutely necessary period of time, which may in no case exceed 3 months. Based on a new request, the judge can repeatedly prolong this period, but each time it is for no more than 3 months. If the ruling applies to a future period, the BIS is obliged to regularly inform the judge whether the reasons for providing the reports still exist. The judge is authorised to request this information and may cancel the warrant permitting the provision of reports at any time.

The law allows the BIS to use specific means of acquiring information, which include so-called intelligence means and persons acting in favour of the BIS (agents). The conditions and methods for the use of the specific means are determined by internal regulations issued by the Director of the Service. The intelligence means include intelligence technology, cover means and cover documents and surveillance. The BIS is obliged to secure the protection of the intelligence means against their exposure, abuse, damage, destruction, loss and theft.

The intelligence technology is taken to mean technical (especially electronic, phototechnical, chemical, physical-chemical, radio-technical, optical and mechanical) means and equipment or their sets, used in a covert manner for the following purposes if it involves infringement upon the fundamental rights and freedoms of citizens.

The BIS may use the intelligence technology when a prior warrant to this effect is issued in writing by the Chairman of the Panel of Judges of the High Court in Prague and on the condition that the exposure or documentation of the activity for which the intelligence technology is to be used would be ineffective, substantially more difficult or in the given case impossible through other means. The use of the intelligence technology may not exceed the limits of the judge's warrant and it may not interfere with the rights and freedoms of citizens beyond the necessary extent.

The use of the intelligence technology may be warranted only for the necessary period of time which may in no case exceed 4 months. When issuing a permit for the use of the intelligence technology, the judge also issues a warrant to this effect which contains the essential identification data and a statement on whether the inviolability of the privacy of home may be infringed upon during the use of the intelligence technology. If the judge rules for the request for a warrant permitting the use of the intelligence technology to be rejected, the ruling includes a statement of the reasons for the decision.

The judge has the authority to request from the BIS information needed for assessing whether the reasons for the use of the intelligence technology still persist. Should the judge find out that the reasons for the use of the intelligence technology have ceased to exist, the judge withdraws the warrant for its use. The BIS informs the judge without delay in writing about the termination of the use of the intelligence technology.

To the extent needed for fulfilling a specific task, the BIS is entitled to the following from legal and natural persons administering public communication networks or providing a publicly accessible electronic communication service:

- to set up or secure an interface for connecting a terminal telecommunication device for the tapping or recording of messages in specified points of their networks
- to provide traffic or location data in a manner, form and extent specified by a specific legal provision.

A cover document shall mean any document used to conceal the true identity of an officer of the BIS or to conceal this officer's affiliation with the BIS or to conceal the activities or facilities of the BIS. What is not allowed to be used as cover documents is the identification cards of deputies, senators, members of the bank board of the Czech National Bank, members of the Supreme Audit Office and judges of the Constitutional Court, service identification cards of judges and prosecutors or identification documents of living individuals. Cover documents shall be supplied and issued by the BIS upon a decision of its Director. Cover means shall mean any object which is not a document, any space or any activity used to conceal the true identity of an individual or to conceal the activity of the BIS. Cover means shall be supplied or created by the BIS upon a decision of its Director.

The BIS keeps a record of supplied or created cover documents and means.

Another essential intelligence means is surveillance. The use of surveillance and its documentation are subject to the decision of the Director or the head of an organisational unit designated by the Director for this purpose. The BIS has the right to request that technical provisions for the surveillance of persons and things and employing security and decoy technology for its own needs are also made by other agencies authorised to carry out these activities. In this case, the BIS is obliged to present evidence that the use of surveillance of persons and things as well as security and decoy technology has been warranted in compliance with Act No. 154/1994 Coll.

In the execution of its tasks, the BIS is authorised to use services provided by persons acting in its favour. For the purposes of this act, a person acting in favour of the BIS is taken to mean a natural person older than 18 years of age, who voluntarily and in a covert manner provides the BIS with services in the execution of its tasks. The BIS is obliged to protect persons acting in its favour against their exposure, against injury to their honour, lives or property which might arise from the provision of these services or in connection to it.

The state is obliged to compensate for harm caused to a person who has provided assistance to the BIS or its officer with their knowledge (hereinafter referred to as 'the assisting person'). The state may be exempted from this obligation only if the assisting person has deliberately inflicted this harm upon himself or herself. The state is obliged to compensate for damage incurred to the assisting person in connection with the provision of assistance to the BIS or to its officer. The state is obliged to compensate for harm caused by the assisting person to a third person in connection with the provision of assistance to the BIS or its officer. The compensation is made on behalf of the state by the BIS, as provided for in specific legislation.

The BIS is authorised to record, store and make use of data on natural and legal persons where it is necessary for the fulfilment of the tasks within its purview. The BIS is obliged to secure the protection of the data contained in its records against disclosure, abuse, damage, loss and theft. The BIS does not inform the natural and legal persons of the fact that it keeps records on them, nor does it make the contents of these records known to them. The BIS may consolidate information and information systems and may acquire information under the cover of a different purpose or through different activities. Types of registers and the way that they are administered are determined by internal regulations issued by the Director of the BIS.

When compelled by the need to keep their activities secret, the intelligence services and their officers may use special ways of presenting data for the purposes of national social security and reporting data on their management of resources from the state budget, including the management of foreign currency funds, income tax returns, data on the payment of health and social insurance and contributions to the government employment policy, and use special procedures in the management of the state assets of the Czech Republic. These special ways of reporting such data and special procedures in the management of the assets are determined by the government.

2.4. Protection of Classified Information

There are proceedings in connection to which the law explicitly mentions the use of intelligence findings. These include security screenings, i.e. background checks for granting or withdrawing security clearance for manipulating classified information. As part of the security screenings, the intelligence services cooperate with the National Security Authority (NBU), i.e. they participate in security screenings in the area of protecting classified information. The purpose of a security screening is to decide whether to grant or withdraw security clearance, which allows for access to information that is classified as 'Confidential', 'Secret' or 'Top Secret' or for a security eligibility certificate (a document which entitles the holder to perform sensitive activities) to/from a natural or business person, and this is done by the NBU. Within the security screening, the intelligence services

either only reply to the NBU's requests for information on a natural or business person if they have the person in their system (administrative enquiry) or actively participate in the security screenings of natural and business persons by means of acquiring field information (field enquiry). Field enquiries involve standard intelligence activities, including the use of specific means of acquiring information and their combinations. In this domain and within their scope of authority, the intelligence services procure information indicating that the holder of security clearance or a security eligibility certificate no longer meets the requirements set for the holder thereof, doing so also without the request of the NBU. The intelligence services then provide the NBU with potential relevant information without delay if it does not jeopardise a major intelligence interest of a given service.

2.5. Internal and International Cooperation

When conducting the security screenings of individuals and companies, the intelligence services cooperate with other state authorities and institutions based on legal provisions as well as interdepartmental cooperation agreements. This cooperation concerns, for instance, applications for Czech citizenship, permits for employment facilitation services, residence permits, foreign investments and electronic identification as well as administrative procedures concerning permits to transport explosives across the Czech territory and permitted transfer routes, granting or withholding licences for manipulating with highly dangerous substances or exports of dual-use items or their transport within the EU.

Furthermore, following a request of one of the intelligence services, the police issues decisions to label a foreign national as a persona non grata and the intelligence services also have the authority to propose an investigation of a suspicious transaction, i.e. a transaction made under suspicious circumstances indicating a possible attempt at money laundering, a potential misuse of money from the transaction to finance terrorism, a possibility that the transaction might in other ways be related or linked to financing terrorism or other facts that might suggest that such suspicions are true.

The intelligence services can cooperate with the intelligence services of foreign powers only with the consent of the government. The BIS is currently authorised to cooperate with over a hundred intelligence services from all over the world; it exchanges information and actively stays in touch mainly with services from the EU and NATO member countries. Cooperation between Czech intelligence services is regulated by agreements made with the consent of the government. The BIS cooperates with the other two intelligence services by means of exchanging information as well as in other operational, analytical and technical activities.

CHAPTER VI

Estonia

Karel Virks, Harrys Puusepp

1. POSITION OF THE SERVICE IN THE DOMESTIC LEGAL SYSTEM

1.1. Position and Role of the Service in the Public Administration System

The Prime Minister and the ministers who head the ministries in whose area of government the security authorities are shall constantly cooperate with each other to organise and harmonise the work of the security authorities.

The Government of the Republic shall establish, by an order for each year, a plan regarding the obtaining and analysis of state security information. The plan concerning the obtaining and analysis of state security information shall provide for the functions set for the security authorities and the Defence Forces upon the conduct of military intelligence and the list of information to be collected, in the order of relevance.

The Security Committee of the Government of the Republic (hereinafter referred to as 'the Security Committee') shall:

- coordinate the activities of the security authorities
- analyse and assess the security situation in the state
- determine the state's need for security-related information
- perform the functions imposed on the Security Committee by the National Defence Act and other acts and the Government of the Republic.

The government authorities are required to give assessments of threats and other information related to the security of the state and national defence to the Security Committee, the Government of the Republic, relevant government authorities, the President of the Republic, the President of the Riigikogu (the Parliament) and relevant committees of the Riigikogu. Where necessary, the Security Committee shall organise the communication of information related to national defence to the persons and previously specified authorities.

1.2. Oversight and Supervision of the KAPO

The first supervisory control is performed at the level of the KAPO, above all in regard to the justification of initiating surveillance proceedings. The surveillance proceedings are very resource-demanding, in terms of both workforce and finances. Therefore, it is obviously not possible to cover all threat sources by surveillance activities and relevant choices need to be made already at the agency level.

In order to ensure compliance with the acts, supervisory control is also exercised over the personnel within the agency.

The activities of the KAPO are additionally supervised by a number of other agencies exercising executive, judicial and legislative power:

- **The Government of the Republic and the Public Prosecutor's Office.** The Ministry of Internal Affairs performs supervisory control over the activities related to the collection of information and surveillance of all agencies within its area of government, including the Estonian Internal Security Service, without intervening in criminal proceedings. The KAPO reports on its activities to the Government of the Republic twice a year. The Prosecutor's Office in its turn exercises supervision over surveillance activities in criminal proceedings. In criminal matters, it is possible to perform surveillance activities only with the knowledge and consent of the Prosecutor's Office.
- **Judicial supervision.** The surveillance activities infringing fundamental human rights most shall be performed only with the consent of the court and at the reasoned request of the prosecutor.
- **The Chancellor of Justice and the State Audit Office.** The Chancellor of Justice monitors the conformity of the activities of the Internal Security Service with the Constitution of the Republic of Estonia and other legal acts and any individual who perceives an infringement of his or her constitutional rights and freedoms has the right to turn to the Chancellor of Justice. The State Audit Office monitors the legality of the use of budgetary means of the Internal Security Service.
- **The Security Authorities Surveillance Select Committee of the Parliament**, also popularly known as 'the KAPO Committee'. It exercises parliamentary supervision, constituting the highest authority that exercises supervision over the Estonian Internal Security Service.

Consequently, the KAPO operates under the watchful eye of executive, legislative and judicial power. The supervision is continual, active and efficient, undoubtedly serving the best interests of both the Estonian Internal Security Service and the Republic of Estonia as a whole.

1.3. Legal Status of the Personnel

A citizen of the Republic of Estonia who has at least secondary education and full active legal capacity and who is proficient in Estonian to the extent provided by law or on the

basis of law may be employed in service or employed as an official and an employee of a security authority.

It is prohibited to employ in service and employ in a security authority a person:

- who receives a pension, remuneration or other regular compensation from a state which is not a state within the European Economic Area or Switzerland or which does not belong to the North Atlantic Treaty Organisation
- who lacks a personnel security clearance for access to a state secret of a required level or a personnel security clearance certificate for access to classified information of a foreign state of a required level if this is a prerequisite for working in a position of an official or of an employee.[1]

The Civil Service Act applies to an official of a security authority with the specifications arising from the Security Authorities Act. The Employment Contracts Act applies to an employee of a security authority with the specifications arising from the Security Authorities Act.[2]

An official of a security authority may be appointed to a position without competition.

Restrictions Imposed on Officials and Employees of a Security Authority

An official and an employee of a security authority may not:

- work for another employer, except with the written consent of the head of the authority
- participate in a strike
- be a member of a political party.[3]

The Police and Border Guard Act[4] applies to the activity of the Estonian Internal Security Service with the specifications arising from the Security Authorities Act. A police officer of the KAPO has, in the performance of his or her duties, the right to apply a state supervision measure and direct coercion on the basis of and pursuant to the procedure provided for in the Law Enforcement Act.[5]

The Identification of Officials of Security Authorities and the Badges of Office of Police Officers

The description and the format of the identification of officials of security authorities and the badges of office of police officers shall be established by a regulation of the minister responsible for the field governed by the Ministry of the Interior or the Ministry of Defence.

---

1 Security Authorities Act, Article 14.
2 Security Authorities Act, Article 12.
3 Security Authorities Act, Article 20.
4 Police and Border Guard Act. Website: https://www.riigiteataja.ee/en/eli/521012022003/consolide
5 Law Enforcement Act. Website: https://www.riigiteataja.ee/en/eli/503032021004/consolide

A list of positions in which police officers are issued a badge of office shall be established by a decree of the head of the relevant security authority.[6]

2. TASKS AND MANDATE

The prime objective of the KAPO within the limits of its competence is to reduce security threats aimed at the Republic of Estonia and by that to maintain national security. However, ensuring a qualitative security environment in today's world is not confined to the territory of one state. Sharing the common security area of NATO and the European Union obliges Estonia to contribute to the prevention of various global threats (i.e. terrorism, mass disorders, cybercrime, the proliferation of weapons of mass destruction). In this regard, the KAPO has an important role to fulfil by cooperating actively with the security and law enforcement authorities of other states and with international organisations. The aim of the joint activity is to protect core values such as democracy, human rights and freedoms and the state based on the rule of law.

The main tasks of the KAPO:

- the collection and processing of information for the prevention and combating of activities aimed at forcefully changing the constitutional order and territorial integrity of Estonia
- the collection and processing of information for the prevention and combating of intelligence activities directed against the state
- the protection of state secrets and classified information of foreign states, performance of security vetting
- the collection and processing of information for the prevention and combating of terrorism (including financing and supporting thereof)
- economic security and fight against corruption
- the non-proliferation of weapons of mass destruction, conduct of proceedings of offences related to explosive substances
- the conduct of criminal proceedings of offences within the investigative jurisdiction of the KAPO
- other administrative tasks and state supervision.

2.1. Investigative Powers and the Role in Criminal Procedure

The Code of Criminal Procedure[7] provides the rules for pre-court and court procedure concerning criminal offences and the rules concerning the enforcement of decisions made in criminal matters.

According to the Code of Criminal Procedure, investigative authorities are, within their respective jurisdictions, the Police and Border Guard Board, the Internal Security Service

6 Security Authorities Act, Article 15-2.

7 Code of Criminal Procedure. Website: https://www.riigiteataja.ee/en/eli/527122021006/consolide

(KAPO), the Tax and Customs Board, the Competition Board, the Military Police, the Environment Board as well as the Department of Prisons of the Ministry of Justice and the prisons, which perform the functions of an investigative authority directly or through an institution administered by them or through a local office.[8]

The KAPO is one of the investigative authorities that may conduct surveillance activities on the following bases:

- a need to collect information about the preparation of a criminal offence for the purpose of the detection and prevention thereof
- the execution of an order on declaring a person a fugitive
- a need to collect information in confiscation proceedings pursuant to the provisions of Chapter 161 of the Code of Criminal Procedure
- a need to collect information in criminal proceedings about a criminal offence.

The surveillance activities may only be conducted in the event of criminal offences specified in Article 1262(2) of the Code of Criminal Procedure and in respect of the persons specified in Article 1262(3) and (4). Where the bases for surveillance activities cease to exist, the surveillance activities shall be immediately terminated.

A surveillance agency may conduct surveillance activities on the basis specified in the Code of Criminal Procedure if this is related to a criminal offence which is in the investigative jurisdiction of such a surveillance agency. The Police and Border Guard Board and the KAPO may also conduct surveillance activities at the request of other investigative bodies.

Investigative Jurisdiction

Pre-court proceedings shall be conducted by the Police and Border Guard Board and the KAPO, unless otherwise provided in the Code of Criminal Procedure. The division of investigative jurisdiction between the Police and Border Guard Board and the KAPO is established by a regulation of the Government of the Republic.[9]

For reasons of expediency, the Prosecutor's Office may alter the investigative jurisdiction by an order in a particular criminal matter.

2.2. Intelligence Gathering

One of the main tasks of the KAPO is to ensure national security by the continuance of constitutional order through the application of non-military means of prevention and to collect and process information necessary for such a purpose.

---

8 Code of Criminal Procedure, Article 32.

9 Regulation of the Government of the Republic considering the division of investigative jurisdiction between the Police and Border Guard Board and the KAPO. Website: https://www.riigiteataja.ee/akt/107052019004

Counterintelligence

The counterintelligence activities of the KAPO are aimed at identifying, monitoring, influencing and impeding any intelligence activities conducted in Estonia. Additionally, preventive activities of alerting individuals, agencies and companies to possible espionage threats are of vital importance. An essential preventive measure for the state is organising the protection of state secrets and ensuring the efficiency thereof.

2.3. Analytical Tasks

Fight Against Terrorism and Extremism

In Estonia, the KAPO is the leading authority in the fight against terrorism and extremism. We mainly focus on prevention, creating defences and deterrents to make Estonia an inconvenient target for terrorists and to limit their potential freedom to act.

Economic Security and Fight Against Corruption

The aim of the activities of the KAPO in ensuring economic security is to prevent economic pressure that could damage the security of the Republic of Estonia. These forms of pressure may include dependence on foreign markets, suppliers, technologies, capital or labour, as well as the vulnerability of infrastructure to the activities of foreign investors. Naturally, we do not consider the source of the threat to be the European Union and NATO partner countries. The economic sectors exposed to the greatest security risks continue to be energy, transport (including transit) and IT, which are the focus of our work.

The functioning of democracy in a country is directly linked to the level of corruption. Since the beginning of the restoration of independence, Estonia has been successful in promoting democracy and one of its hallmarks and foundations is a comprehensive and systematic approach to anti-corruption, the functioning of the anti-corruption system and the necessary response to corruption offences. In Estonia, the fight against corruption is divided by the police and the KAPO. The KAPO has always paid attention to the fight against top-level corruption in larger municipalities (Tallinn, Tartu, Narva, Pärnu, Kohtla-Järve and Jõhvi) and high-level officials (i.e. members of the Parliament, members of the government, the Auditor General, the Chancellor of Justice, judges, prosecutors or a higher police officer etc.).

The Non-proliferation of Weapons of Mass Destruction

Located on the eastern border of the Western world, Estonia has experienced export controls since the Middle Ages, when the strategic goods of the day were, for instance, horses rather than nuclear components or tanks.

The modern concept of export control dates back to the immediate post-Cold War era, when the Western powers formed a united front against pariah states to prevent a technological arms race and future large-scale military conflicts. Counterproliferation, or the

fight against the spread of weapons of mass destruction, is one of the responsibilities of the KAPO. The Estonian authorities are responsible for ensuring the legality of transactions going through the country. It is important that military or dual-use items do not pass through Estonia to countries subject to sanctions or into the hands of terrorist groups.

Annual Reviews

The specific nature of the work of special services responsible both for national security and throughout the ages, foreign intelligence has required operating as covertly as possible, and a certain mystery has always surrounded it. In the information society, it is no longer possible to act completely undercover, and therefore more and more special services have understood the need of being more open and notify the public of their activities.

It is our position that without large-scale public support and public trust it is very difficult to be successful in performing the duties assigned to the Internal Security Service. However, it is impossible to gain support if nothing is known about one's activities or even one's existence. Therefore, we have tried to be as open as possible when speaking about our profession, goals and results of activities.

The second and not less important goal is informing the public of possible security risks and threats. In the form of an annual review, we have a simple but effective tool for achieving the aforesaid goals. An annual review is above all meant for the whole population of Estonia, but also for the international public – ranging from enthusiasts interested in special services to students and journalists. Colleagues from our partner services also constitute an important target group.

The first annual review of the Estonian Internal Security Service was published in 1998, being one of the first publications of its kind in the world. In compiling an annual review, we set ourselves the objective that in addition to being informative, it would also be interesting and easy to read.

The online editions of our annual reviews are available on our website: https://kapo.ee/en/content/annual-reviews/.

2.4. Administrative Tasks of the KAPO

The KAPO as a security authority may use the measures provided in the Security Authorities Act for restricting the fundamental rights of persons. According to the Security Authorities Act, the KAPO:

- may use shadow information and covert measures in order to hide from the data subject the performers of the act on the basis of a resolution of the head of the security authority[10]

[10] Security Authorities Act, Article 23.

- may use a legal person in private law for the performance or ensuring the performance of its functions on the basis of a resolution of the head of the security authority[11]
- may appoint on a post or recruit an undercover staff official or employee of the security authority on the basis of the resolution of the head of the security authority[12]
- has the right to recruit a person with active legal capacity to secret cooperation with his or her consent.[13]

The KAPO is permitted to restrict a person's right to the confidentiality of messages or the inviolability of home and family or private life.

A person's right to the confidentiality of messages is restricted by:[14]

- an examination of a postal item
- wire-tapping, observing or recording a message or other information transmitted over an electronic communications network
- wire-tapping, observing or recording information communicated by any other means.

A person's right to the inviolability of home and family or private life is restricted by:[15]

- the collection and processing of personal data
- covert surveillance
- the covert establishment of identity
- the collection of information on the fact, duration, manner and form of transmission of messages over an electronic communications network, and on the personal data and location of the sender or the receiver of such messages
- covert entry into the person's premises, building, enclosed area, vehicle or computer system for the purposes of the covert collection or recording of information or the installation and removal of technical aids necessary for such purposes
- the covert examination of an item and, if necessary, the covert alteration of the item, damage to the item or the replacement of the item.

In the case of a need to restrict a person's right to the confidentiality of messages or to the covert entry into the person's premises, building, enclosed area, vehicle or computer system for the purposes of the covert collection or recording of information or the installation and removal of technical aids necessary for such purposes, the head of the security authority must submit to the chairman of an administrative court or an administrative judge appointed by the chairman a reasoned written application for the corresponding permis-

11 Security Authorities Act, Article 23-1.
12 Security Authorities Act, Article 23-2.
13 Security Authorities Act, Article 24-1.
14 Security Authorities Act, Article 25
15 Security Authorities Act, Article 26.

sion. The application sets out the manner of the restriction of the corresponding right. The granting, extension and revocation of permission by the judge is decided without delay and without holding a court session. The permission may be granted for a period of up to 2 months or extended for the same period at a time.[16]

In emergency situations, i.e. if there is a threat to the national security or if there is sufficient information to indicate that a criminal offence is being prepared or committed and an act is necessary to combat that criminal offence and it is impossible to apply for the written permission of the administrative court, the act may be performed with the permission of the administrative court, which is issued in a manner which can be reproduced. The head of the security authority must submit a reasoned application which can be reproduced as a basis for the permission to the chairman of an administrative court or an administrative judge appointed by the chairman at the first opportunity, but no later than on the day following the day of commencing the act.

In other measures of the restriction of a person's right to the inviolability of home and family or private life (covert surveillance; the covert establishment of identity; the collection of information on the fact, duration, manner and form of transmission of messages over an electronic communications network, and on the personal data and location of the sender or the receiver of such messages; the covert examination of an item and, if necessary, the covert alteration of the item, damage to the item or the replacement of the item), the decision is made by the head of the security authority or an official authorised by him or her. The decision shall be valid for the term indicated therein, but for no longer than 2 months.

Other Administrative Tasks and State Supervision

- **Visa proceedings**

According to the Aliens Act, the KAPO is one of the agencies designated by the Minister of the Interior who coordinates the issue of a visa in Estonia. Also, the KAPO has the power to annul or revoke a visa.[17]

- **Entry bans**

According to the Obligation to Leave and Prohibition on Entry Act, the KAPO has the right to make a proposal to the Minister of the Interior to order the application of probation on entry into the territory of Estonia or the Schengen area.[18]

- **Background checks**

The KAPO has the legal right to conduct background checks and give assessments in order to verify the compliance of natural or legal persons with the requirements set in the

16 Security Authorities Act, Article 27(1) and (2).
17 Aliens Act, Articles 76, 77, 82. Website: https://www.riigiteataja.ee/en/eli/517082021004/consolide
18 Obligation to Leave and Prohibition on Entry Act, Article 31-1. Website: https://www.riigiteataja.ee/en/eli/517082021005/consolide

Weapons Act for natural persons who wish to hold a weapons permit or legal persons who wish to handle military weapons, ammunition and munition.

According to the Aviation Act, the KAPO is responsible for carrying out a background check on a person who applies for or holds or who will start performing or performs certain aviation security functions specified in the Aviation Act.[19]

- **E-resident's digital identity card**

The KAPO is one of the competent authorities to exercise state supervision over the use of the e-resident's digital identity card provided for in the Identity Documents Act.[20]

- **Approval of the activity licence of explosives**

The KAPO is one of the authorities who shall, within the limits of its competence, approve or not approve the application for the activity licence of a handler of an explosives pyrotechnic article.[21]

- **Strategic Goods Commission**

The KAPO is one of the authorities that participate in the Strategic Goods Commission.[22] The commission performs the following duties assigned to the commission by the Strategic Goods Act and other legislation:

- **Supervision of the requirements of nations defence objects and the protection thereof**

The KAPO exercises state and administrative supervision over compliance with the requirements of the organisation of the protection of national defence objects; the guarding and protection of national defence objects and the procedure of national defence object guarding.[23]

2.5. Protection of Classified Information

In Estonia, the KAPO is one of the main authorities who is responsible for the protection of state secrets and classified information of foreign states. According to the State Secrets and Classified Information of Foreign States Act, the KAPO is responsible for performing security vetting, except for some persons in respect of whom the security vetting is performed by the Estonian Foreign Intelligence Service.[24]

In addition to the KAPO, ensuring the protection of state secrets in Estonia is also within the sphere of the responsibility of the Estonian Foreign Intelligence Service and the General Staff of the Defence Forces.

---

19 Aviation Act, § 46-9. Website: https://www.riigiteataja.ee/en/eli/531122021004/consolide

20 Identity Documents Act, Article 20-8. Website: https://www.riigiteataja.ee/en/eli/501112021001/consolide

21 Explosives Act, Article 13. Website: https://www.riigiteataja.ee/en/eli/506042021003/consolide

22 Strategic Goods Act, Article 70. Website: https://www.riigiteataja.ee/en/eli/ee/512022020002/consolide

23 National Defence Act, Article 88. Website: https://www.riigiteataja.ee/en/eli/526042022005/consolide

24 State Secrets and Classified Information of Foreign States Act, Article 48. Website: https://www.riigiteataja.ee/en/eli/521052020005/consolide

The Estonian Foreign Intelligence Service organises INFOSEC in the field of state secrets and monitors compliance with the pertinent requirements. It organises and supervises the protection of state secrets in foreign representations and in structural units and subunits of the Defence Forces located outside the territory of the Republic of Estonia. In some cases, it also performs security vetting. The function of the Estonian National Security Authority is also performed by the Estonian Foreign Intelligence Service.

The General Staff of the Defence Forces organise and supervise compliance with the protection measures of state secrets in the Defence Forces and in the National Defence League.

2.6. Internal Cooperation

The security authorities cooperate with each other through mutual assistance and exchange of information. The exchange of information between the security authorities takes place on the basis of a plan regarding the obtaining and analysis of state security information.[25]

Information which is received in the performance of the functions of a security authority may be transferred to another person or authority if it is necessary for the performance of the functions of the security authority. For the performance of obligations arising from an international agreement, the legislation of the European Union or other laws, information which is received in the performance of the functions of the security authority may also be transferred to a foreign state or an international organisation.[26]

2.7. Personal Data Protection

For the performance of its functions or ensuring the performance thereof, a security authority may collect and process, among others, the following information:

- personal data
- special categories of personal data
- data rendered anonymous
- data addressed to the public and available from public sources.[27]

The KAPO may process the collected information for the performance of a function provided for in the Security Authorities Act or in another act or for the purpose of ensuring such performance. For the performance of obligations arising from an international agreement, the legislation of the European Union or other laws, personal data obtained from a foreign state or an international organisation may be processed.[28]

---

25 Security Authorities Act, Article 11.
26 Security Authorities Act, Article 32(3-1).
27 Security Authorities Act, § 21-1(1).
28 Security Authorities Act, § 21-1(5).

CHAPTER VII

France

Nicolas Lerner

1. POSITION OF THE DGSI IN DOMESTIC LEGAL SYSTEM

1.1. Legal Definition of Special Services (Intelligence and Security Services) and Their Position in the Public Administration System

The DGSI belongs to the French Intelligence Community, which includes several services placed under the authority of various ministries (of the Interior, Armed Forces, Economy and Finances, and Justice).

The Domestic Security Code (*Code de la sécurité intérieure*) sorts these services into two categories:

1) Specialised intelligence services, also known as 'first-circle services', are defined by the law. Article L. 811-2 of the Domestic Security Code provides that 'their mission, conducted in France and abroad, is to collect, process and provide the government with intelligence pertaining to geopolitical and strategic issues and to threats and risks likely to affect the life of the nation. They contribute to obtaining knowledge on those issues and anticipating them as well as to preventing and disrupting those risks and threats'. There are six such services, depending on three different ministries:

The Ministry of the Interior:

The General Directorate for Domestic Security (DGSI, *Direction générale de la sécurité intérieure*) is both an intelligence and a specialised criminal police service, which enables it to have a global approach to terrorist activities and interference from French and foreign organisations.

The DGSI is an intelligence service placed under the authority of the Ministry of the Interior. The DGSI was created by Decree No. 2014-445 of 30 April 2014 which defines its organisation and its missions. Its birth is the culmination of the rationalisation process of

domestic intelligence services launched in 2008 with the creation of the Central Directorate of Interior Intelligence (*Direction Centrale du Renseignement Intérieur* or the DCRI). The DCRI, then replaced by the DGSI, already resulted from the merge of the Central Directorate of General Intelligence (*Direction Centrale des Renseignements Généraux*, DCRG) and the Directorate of Territorial Surveillance (*Direction de la Surveillance du Territoire*, DST) in order to reinforce the complementarity and communication between the DCRG and the DST.

As it has the active-duty status of the national police, the DGSI has a general competence over the entire territory of the French Republic to search, centralise and exploit intelligence pertaining to national security or the fundamental interests of the nation. It also contributes to judicial police missions within its areas of competence on the whole territory (Article 1 of the Decree of 30 April 2014).

The Decree of 30 April 2014 establishing the DGSI defines its missions and organisation.

Pursuant to Article 4 of the above-mentioned decree and to carry out its mission of defending national security and the fundamental interests of the nation, the DGSI is comprised of central services located in the Paris region and a large network of territorial services located in the metropolitan area and in the French overseas territories.

- At the central level, the DGSI has a Directorate of Intelligence and Operations which oversees its thematic missions and several services ensuring its functioning and independent management, i.e. a Cabinet, a General Administration Office, a General Inspectorate and a Technical Directorate.
- The territorial services are directly under the supervision of the Director General and are present at different levels of the French territory. They have a zonal or an interdepartmental authority and are a central component of the DGSI's action. They fully participate in intelligence gathering and reporting and, more broadly, in the General Directorate's activity. They are placed under the control and coordination of the central services which provide the guidelines of the General Directorate for intelligence.

The Ministry of the Armed Forces:

- The General Directorate for External Security (DGSE, *Direction Générale de la Sécurité Extérieure*) aims to protect French interests and citizens around the world. It gathers intelligence outside of the French territory regarding the threats and risks likely to affect the life of the nation.
- The Defence Directorate for Intelligence and Security (DRSD, *Direction du Renseignement et de la Sécurité de la Défense*) is tasked with detecting and disrupting threats to the defence sector (armed forces and defence companies).
- The Directorate for Military Intelligence (DRM, *Direction du Renseignement Militaire*) provides the forces and operations in the field with intelligence relevant to the

military. Its insight facilitates the high political and military authorities' decision-making.

Ministry of Economy and Finances:

- The National Directorate for Intelligence and Customs Investigations (DNRED, *Direction Nationale du Renseignement et des Enquêtes Douanières*) is tasked with implementing the policy for intelligence, control and fight against fraud on customs.
- The nationally competent service called Processing Intelligence and Acting Against Illegal Financial Networks (TRACFIN, *Traitement du renseignement et action contre les circuits financiers clandestins*) is tasked with fighting against money laundering, illegal financial networks and terrorism financing.

2) So-called second-circle intelligence services currently depend on the Ministries of the Armed Forces, the Interior, and Justice. They can be tasked with intelligence missions and are authorised to implement specific technology-based tradecraft in compliance with Article L. 811-4 of the Domestic Security Code.

These services are divided into two categories:

- Services whose main mission is intelligence: this is especially the case for the Central Service for Local Intelligence (SCRT, *Service central du renseignement territorial*), the Intelligence Directorate of the Paris Police Prefecture (DRPP, *Direction du renseignement de la préfecture de police de Paris*), the National Gendarmerie's Sub-Directorate for Operational Anticipation (SDAO, *Sousdirection de l'anticipation opérationnelle*) and the apparatus combining the National Service for Prison Intelligence (SNRP, *Service national du renseignement pénitentiaire*) with the Interregional Prison Intelligence Cells (CIRP, *Cellules interrégionales du renseignement pénitentiaire*) of the Interregional Directorates of Prison Services (*directions interrégionales des services pénitentiaires*) and with the Overseas Territories Prison Services Mission (*mission des services pénitentiaires d'outre-mer*).
- Services that are authorised to implement technology-based tradecraft, but whose main missions are not intelligence-related. This is particularly the case for criminal police services.

1.2. Scope of Activities of the Services

The intelligence activities and the actions of intelligence services were legitimised and specified by Law No. 2015-912 of 24 July 2015 on intelligence (*loi n° 2015-912 du 24 juillet 2015 relative au renseignement*) via Articles L. 811-1 and L. 811-3 of the Domestic Security Code.

Pursuant to these articles, 'the public policy for intelligence contributes to the national security strategy and to defending and promoting the Nation's fundamental interests. It is an exclusive competence of the state' (Article L. 811-1 of the Domestic Security Code). Article L. 811-3 specifies the seven fundamental interests of the nation which serve as a basis for the intelligence services' activity, i.e.:

- France's national independence, territorial integrity and national defence
- the major interests of France's foreign policy, the execution of France's European and international commitments and the prevention of any type of foreign interference
- France's major economic, industrial and scientific interests
- terrorism prevention
- the prevention of: a) attacks against the republican form of institutions; b) actions aimed at maintaining or rebuilding groups dismantled pursuant to Article L. 2121; c) collective violence likely to severely jeopardise public peace
- the prevention of organised crime and delinquency
- the prevention of the proliferation of weapons of mass destruction.

These general missions defined in the law are further detailed in a National Intelligence Strategy (SNR, *Stratégie Nationale du Renseignement*). This document, which is approved by the President of the Republic win the framework of the National Intelligence Council, is the intelligence roadmap. It specifies the priority issues, the goals and the ensuing organisational scheme. This strategy concerns the whole intelligence community and it is destined to intelligence services as a priority, although it also targets the entities contributing to the public intelligence policy (police and gendarmerie services, armed forces, oversight and support bodies etc.) and all the persons who are to contribute to or benefit from it with regard to their responsibilities.

The latest version of the National Intelligence Strategy dates back to July 2019 and defines four priority challenges:

- fighting terrorism
- anticipating major crises and disruption risks
- protecting and promoting our economic and industrial interests
- fighting cross-cutting threats.

These challenges are not only identified in the National Intelligence Strategy, but they are also developed operationally in the National Intelligence Orientation Plan (PNOR, *Plan National d'Orientation du Renseignement*), which defines the action priorities for intelligence services, including the DGSI.

1.3. Oversight and Supervision of the Services

Apart from the monitoring performed by the CNCTR regarding the implementation of intelligence techniques, the activities of intelligence services are subject to the monitoring of several institutions.

Each of them steps in at different levels:

- **Internal administrative and hierarchical monitoring**

All the services have internal monitoring apparatus, although the nature and importance of this monitoring vary from one service to the next.

As far as it is concerned, the DGSI answers to its general inspection, but also to its line ministry – the Ministry of the Interior – which ensures that the service's activity is in compliance with its remit.

- **Intelligence Service Inspectorate** (*Inspection des services de renseignement* or the ISR) **monitoring**

Created by Decree No. 2014-833 of 24 July 2014, the Intelligence Service Inspectorate can request that inspection measures are conducted within intelligence services upon request by the Prime Minister, under whose orders it is placed.

Its agents have access to all locations, information and documents pertinent to accomplishing their mission.

- **National Data and Freedoms National Commission** (*Commission Nationale de l'Informatique et des Libertés* or the CNIL) **monitoring**

Under Article 118 of Law No. 78-17 of 6 January 1978 pertaining to data and freedoms, intelligence services are subject to regular document-based checks and on-site checks by the CNIL whose task is to protect personal data in the framework of intelligence activities.

- **Parliamentary monitoring**

Created in 2007, the Parliamentary Delegation for Intelligence (*Délégation parlementaire au renseignement*) – whose organisation and remit are defined in Article 6 *nonies* of Ordinance No. 58-1100 of 17 November 1958 pertaining to the operation of parliamentary assemblies – controls the government's action regarding intelligence and assesses public policy as well as monitors the current stakes and upcoming challenges on the matter.

In this regard, it can be given certain information, under the conditions provided by law, and proceed to the hearing of the Prime Minister, the members of the government, the National Defence and Security Secretary General, the Head of the National Centre of Intelligence and Counter-Terrorism (*Centre national du renseignement et de la lutte contre le terrorisme*) and the heads of the intelligence services.

Incidentally, the DGSI is also subjected to the monitoring of the Special Funding Audit Commission (*Commission de vérification des fonds spéciaux*). It is a parliamentary body tasked with monitoring the use of public funds for the intelligence services' sensitive operations.

Coordination of the Activities of the Services

In order to reinforce the strategic coordination in the whole intelligence community and ensure that the corresponding services make proper use of the intelligence instruments, a coordinating structure placed under the authority of the President of the Republic was created first informally in 2008, then officially as of 2010 (Decree No. 2009-1657 of 24 December 2009 regarding the Defence and National Security Council and the General Secretariat for Defence and National Security, *décret n° 2009-1657 du 24 décembre 2009 relatif au conseil de défense et de sécurité nationale et au secrétariat général de a défense et de la sécurité nationale*). Since 2017, this structure has been called the National Coordination of Intelligence and Counter-Terrorism (CNRLT, *Coordination nationale du renseignement et de la lutte contre le terrorisme*).

Its organisation and missions are specified in Articles R. 1122-8 to R. 1122-8-2 of the Domestic Security Code. The National Coordinator for Intelligence and Counter-Terrorism is appointed by way of a decree at the Council of Ministers and his or her task are as follows:

- to advise the President of the Republic on intelligence and counterterrorism
- to coordinate the actions of specialised intelligence services and, if need be, so-called second-circle services. Most particularly, the National Coordinator ensures to disseminate the President's instructions to the ministers in charge of these services and sees that they are effectively implemented
- to be in charge of the global threat assessment and to propose orientations for the intelligence and counterterrorism policy to the President of the Republic
- to coordinate and develop the initiatives taken by France in terms of European and international cooperation in the field of intelligence counterterrorism.

1.4. Legal Status of the Agents

In order to carry out its intelligence and judicial police missions, the DGSI recruits a wide range of people all over the country, whatever their status or profile may be.

Indeed, the DGSI employs agents of French nationality who are cleared at the *très secret* (Top Secret) level and with several different statutes: police officers, public service administrative personnel, contractual agents, individual contractors or reservists. It also recruits multiple profiles, whether they are generalists (analysts), specialists, technical (technicians and engineers) or linguists.

As the DGSI personnel, these agents benefit from certain protections in virtue of their intelligence service agent status.

Firstly, they benefit from a specific legal protection that guarantees their anonymity: according to Article 413-12(1) of the Penal Code, 'revealing any information which may lead, either directly or indirectly, to the discovery of the use of […] an assumed identity, of

false pretences, of the real identity of a [1st or 2nd circle] service agent or of their belonging to one of these services is punishable with five years' imprisonment and a €75,000 fine.'

Subsidiarily, it is important to emphasise the fact that this legal protection of their identity is also 'applicable to the revealing of any information which may lead, whether directly or indirectly, to the effective or assumed identification of a person as a source or collaborator of a [1st or 2nd circle] service' (the last para. of Article 413-12 of the Penal Code).

Secondly, Article L. 861-2 of the Internal Security Code provides for the possibility for security service agents to 'use a false identity or false pretences' in the call of duty for a mission regarding national defence and security. Therefore, and according to para. 2 of the aforementioned Article, the intelligence agents using these means as well as the people necessary for the sole purpose of establishing or allowing this use are exempted from all legal responsibility.

Thirdly and lastly, the intelligence agents benefit from protection to their anonymity whenever they are called to testify as part of legal proceedings. Article 656-1 of the Penal Procedure Code indeed creates a deposition modality specific to the intelligence service personnel who may witness offences in the line of duty.

2. TASKS AND MANDATE

Article 2 of the above-mentioned Decree of 30 April 2014 defines the DGSI's missions. It has six main tasks:

- **Preventing and contributing to the repression of any foreign interference**

  Counter-espionage is the historical mission of the DGSI. It is aimed at countering the interference attempts conducted by foreign organisations and powers on French territory through disruptive or retaliation measures which are adjusted according to the originator or the seriousness of the hostile acts detected.

- **Contributing to the prevention and repression of terror acts or actions undermining the security of the state, the integrity of its territory or the institutional continuity of the Republic**

  The DGSI plays a key role in this apparatus due to its specific missions, its operational means and its CT expertise recognised at the national and international level. In 2018, it was also assigned the leadership on CT matters by the French President. Due to this task, the DGSI has a key role and a specific responsibility in organising and leading the fight against terrorism at the national level.

The DGSI is in charge of the operational coordination of intelligence, carries out judicial investigations under the supervision of dedicated magistrates and establishes the national and international cooperation strategies of the Ministry of the Interior in the field of counterterrorism. It conducts this mission in close cooperation with the whole community of French intelligence services.

- **Participating to the monitoring of radical-inspired individuals and groups likely to use violence and undermine the national security**

While the DGSI is not in charge of right-wing and left-wing extremism – intelligence services do not have the competence to monitor their activities, as they represent political currents – it can monitor individuals who, on behalf of extreme ideologies, are likely to use physical violence and even, in some cases, want to threat the republican form of the institutions or the state's representatives.

- **Contributing to the prevention and repression of acts violating national defence secret or those undermining the economic, industrial or scientific capabilities of the country**

In order to address the growing and multiple crises or threats likely to impact French interests, the DGSI is tasked with economic protection aimed at detecting and preventing vulnerabilities, threats and foreign interference attempts against key French economic actors. These actors are, but are not limited to, large groups, start-up or academic and research institutions, which are regularly threatened by aggressive foreign actors operating destabilisation and espionage attempts through data collection.

In this field, the DGSI carries out intelligence operations aimed at raising the awareness of political authorities who will engage means to counter these interferences. The General Directorate also conducts awareness-raising operations with economic actors in order to alert them to the risks and it can provide them with support if necessary.

Regarding the protection of secrecy, the DGSI has two missions: firstly, to issue clearance for the state personnel who are granted security clearance relating to national defence secrets; secondly, to support companies, administrations and institutions by conducting awareness-raising missions regarding a compromise.

- **Contributing to the prevention and the repression of activities related to the procurement or the manufacturing of weapons of mass destruction**

To better address the proliferation of weapons of mass destruction, the DGSI is tasked with detecting, preventing and disrupting: on the one hand, the DGSI detects and disrupts procurement pipelines of materials that could contribute to the development of weapons and, on the other hand, it prevents know-how theft, i.e. techniques and innovations of French companies. The DGSI also has awareness-raising and consulting missions regarding the risk of weapons proliferation with French economic and scientific actors and, more specifically, civilian research industries and institutions.

- **Contributing to the prevention and repression of ICT crimes**

The DGSI is tasked to protect France's sovereignty in the cyber field by monitoring cyber *modus operandi* likely to violate the fundamental interests of the nation and operating proactively or reactively to counter these threats. More specifically, the DGSI is responsible for cyber threats related to espionage and interference, proliferation, terrorism, violent subversions and economic protection.

Among all these missions, the DGSI is in charge of identifying and preventing the risks and threats that France is facing in order to provide the policy makers with an independent assessment of the situation.

Beyond its mission to anticipate and provide authorities with information, the DGSI is also in charge of disrupting any threat that it detects. To achieve this mission and as a specific service, the DGSI has both a judicial competence and an intelligence one: on the one hand, it is an intelligence service which mission is to collect information pertaining to national security and the fundamental interest of the nation, and on the other hand, it is a judicial police service responsible for 'detecting offences under criminal law, collecting evidence and searching for the perpetrators' in accordance with Article 14 of the Criminal Procedure Code. This specific feature is valuable, as it enables greater fluidity between intelligence and judicial procedures.

2.1. Intelligence Gathering

Specialised intelligence services operate within a specific legal framework resulting from a double requirement: firstly, to prevent crimes against national security in accordance with the rights and freedoms of citizens, and secondly, to secure the action of the service and its agents as part of their missions.

In the field of intelligence, dedicated laws were enacted, such as Law No. 2015-912 of 24 July 2015 pertaining to intelligence, Law No. 2015-1556 of 30 November 2015 pertaining to the surveillance measures of international electronic communications, Law No. 2017-1510 of 30 October 2017 regarding domestic security and fight against terrorism or Law No. 2021-998 of 30 July 2021 pertaining to the prevention of terrorist acts and to intelligence.

Since the adoption of the above-mentioned Law of 24 July 2015 pertaining to intelligence, the intelligence-gathering techniques that can be implemented on the whole national territory by specific intelligence services are strictly defined and regulated. The main techniques authorised by law are the following:

- the administrative access to connection data, in real time or not (Articles L. 851-1, L. 851-2, L. 851-3 of the Internal Security Code)
- real-time geolocation (Article L. 851-4 of the Internal Security Code)
- the use of technical devise (Article L. 851-5 of the Internal Security Code)
- security interception of correspondence (Article L. 852-1 of the Internal Security Code)
- the records of words spoken in private or images from a private location (Article L. 853-1 of the Internal Security Code)
- the collection of computer data (Article L. 853-2 of the Internal Security Code)
- the surveillance of communications emitted or received abroad (Articles L. 854-1 ff of the Internal Security Code).

As stated in Article L. 801-1 of the Internal Security Code, 'respect for privacy, in all its components, including privacy of correspondence, protection of personal data and inviolability of the home, is guaranteed by law. Authorities may override it solely in case of public necessities provided by law, within the limits fixed by it and in compliance with the principle of proportionality.'

Intelligence services are allowed to use intelligence techniques only with the authorisation of the Prime Minister after consultation with an independent administrative authority, i.e. the National Commission for Control of Intelligence Techniques (CNCTR). This authorisation is granted pursuant to the fundamental principles of proportionality and subsidiarity and can only be issued under the purposes of protecting and promoting the fundamental interests of the nation. These objectives are listed exhaustively by the legislators under Article L. 811-3 of the Internal Security Code:

- national independence, territorial integrity and national defence
- major interests in foreign policy, implementation of European and international obligations of France and prevention of all forms of foreign interference
- the major economic, industrial and scientific interests of France
- the prevention of terrorism
- the prevention of attacks on the republican nature of institutions, actions towards the continuation or constitution of groups disbanded, and collective violence likely to cause serious harm to public peace
- the prevention of organised crime and delinquency
- the prevention of the proliferation of weapons of mass destruction.

Upon authorising the use of these techniques, specific safeguards are necessary for their implementation: the periods of authorisation to use these techniques, such as the duration of data retention, are limited in time and vary, depending on how much individual freedoms are infringed.

The implementation of these techniques is subject to an *a posteriori* oversight by the CNCTR which is responsible for ensuring their compliance with the legal framework. To this end, the Commission has a permanent, comprehensive and direct access to collected intelligence as well as transcripts and extractions operated by intelligence services (Article L. 833-2 of the Internal Security Code) which enables it to perform document-based and on-site controls. During these controls, members of the Commission visit services and discuss with the agents who provide them with the information on all the results related to a specific technique.

The specialised intelligence services act within a precisely defined framework. This framework is the result of two goals: firstly, to prevent attacks to national security while respecting the rights and freedoms of citizens; and secondly, to secure the service's actions and its agents in the line of duty.

In the field of intelligence, specific texts have been drafted, such as Law No. 2015-912 of 24 July 2015 pertaining to intelligence, Law No. 2015-1556 of 30 November 2015 pertaining to the monitoring of international electronic communications monitoring, Law No. 20171510 of 30 October 2017 pertaining to domestic security and counterterrorism or Law No. 2021-998 of 30 July 2021 pertaining to terrorism prevention and intelligence.

The Legal Framework Dealing with Technical Intelligence Collection

Since the Law of 24 July 2015 pertaining to intelligence, the intelligence collection techniques which can be implemented on the national territory are strictly framed and defined. To date, the main authorised techniques are the following:

- administrative access to log-in data, either time-deferred or real-time (Articles L. 851-1, L. 851-2, L. 851-3 of the Domestic Security Code)
- real-time geolocation Article L. 851-4 of the Domestic Security Code)
- beacon installation (Article L. 851-5 of the Domestic Security Code)
- security interceptions (Article L. 852-1 of the Domestic Security Code)
- the recording of words and images in a private location (Article L. 853-1 of the Domestic Security Code)
- the collection of computer data (Article L. 853-2 of the Domestic Security Code)
- the monitoring of communications either sent or received abroad (Articles L. 854-1 ff of the Domestic Security Code).

As recalled in Article L. 801-1 of the Domestic Security Code, 'the respect of private life, in all aspects, notably the confidentiality of correspondence, protection of personal data, and inviolability of the home are guaranteed by the law. The public authority can infringe upon these rights only in cases of compulsory public interest defined by the law, within the limits set by the said authority and in compliance with the proportionality principle.'

Therefore, the intelligence services can use these techniques only with the authorisation of the Prime Minister, delivered after assessment by an independent administrative authority, the Intelligence Technique Monitoring National Commission (*Commission nationale de contrôle des techniques de renseignement* or the CNCTR). This authorisation is granted in the application of the fundamental principles of proportionality and subsidiarity and can be delivered only for specific ends pertaining to the defence and promotion of the fundamental interests of the nation, which are incurred and enumerated by the legislator in Article L. 811-3 of the Domestic Security Code:

- national independence, territorial integrity and national defence
- the major foreign policy interests, the execution of France's European and international engagements, and the prevention of foreign interference of any kind
- France's major economic, industrial and scientific interests

- terrorism prevention
- the prevention of attacks to the republican form of the institutions, of actions aiming to maintain or reform disbanded groups as well as of collective violence likely to gravely violate the public order
- the prevention of petty and organised crime
- the prevention of the proliferation of weapons of mass destruction.

Once these techniques are authorised, specific guarantees dictate their implementation: the duration of the implementation of the said techniques as well as the duration of the retention of collected data are limited and vary, depending on the degree of the offence perpetrated against individual freedoms.

The implementation of these techniques by the services are also subjected to *ex post facto* checks by the CNCTR, which is tasked with ensuring their compliance to the legal framework. In that respect, the Commission has permanent access to the collected intelligence as well as to the transcripts and extractions conducted by the intelligence services (Article L. 833-2 of the Domestic Security Code). This enables the Commission to carry out inspections on and offsite. During these inspections, the Commission members go on the services' premises and meet the agents, who share all the results linked to a technique with them.

Other Intelligence Sources and Activities Defined by French Law

In parallel to the technical intelligence collection techniques, French law also provides for the possibility for the intelligence services to collect intelligence:

- with other administrative authorities: Article L. 863-2 of the Internal Security Code enables the intelligence services to share 'any information, even if it is covered by a secret protected under the law, which is strictly necessary for the performance of the service's duties and for the promotion of the fundamental interests of the nation as mentioned in Article L. 811-3'
- with the judicial authority: Articles 706-25-2 and 706-105-1 of the Criminal Procedure Code enables the judicial authority to share elements from judicial proceedings with certain intelligence services, including the DGSI. These elements have to be necessary to the performance of the duties of the said services pertaining to counterterrorism, cyber threats as well as some offences qualified as organised crime.

2.2. Personal Data Protection

In France, the processing of personal data is regulated by Law No. 78-17 of 6 January 1978 pertaining to data protection and freedom (*informatique et libertés*). This text transposes into the French law the European regulation pertaining to personal data

stemming from Regulation (EU) 2016/679 of 27 April 2016 and from Directive (EU) 2016/680 of 27 April 2020.

It also provides specific provisions applicable to the processing of personal data relative to state security and defence which do not fall under the European legislator's purview. Most of the processing conducted by the intelligence services falls under this specific national legislation when they aim to pursue the fundamental interests of the nation.

In compliance with Title IV of Law No. 78-17 of 6 January 1978, the processing falling under state security and defence must be granted by a decree issued by the State Council, after the National Data and Freedoms National Commission (*Commission Nationale de l'Informatique et des Libertés* or the CNIL) has been consulted. It is an independent administrative authority acting as a regulator for personal data. Due to their specific subject and because of the often-classified nature of the data that they contain, these processing procedures follow rules which derogate from the rules set by the European framework:

- They are exempted from presenting the CNIL with an impact assessment regarding data protection as part of the declaration procedure.
- They can be exempted from being published in the Official Journal.
- They are subjected to indirect right of access, of rectification and of deletion. This implies that access, rectification or deletion requests cannot be filed by private persons directly with the person responsible with processing. These requests go through the CNIL.
- Regarding the disputes made by private persons, they fall under the purview of the State Council's special group which examines these disputes and rules on them following an asymmetrical procedure.

CHAPTER VIII

Germany

Thomas Haldenwang

1. POSITION OF THE SERVICE IN THE DOMESTIC LEGAL SYSTEM

1.1. Legal Definition of Special Services

There is no legal definition of the term 'intelligence service' (or 'special service') in German law.

1.2. Position and Role of the Services in the Public Administration System

The BfV (*Bundesamt für Verfassungsschutz*) is Germany's federal domestic intelligence service. In addition, each of the 16 German states (or *Länder*) has its own domestic intelligence agency (*LfV/Landesbehörde für Verfassungsschutz*). Thus, there are 17 civil domestic intelligence services (referred to as offices for the protection of the constitution) in total.

The BfV is subordinate to the Federal Ministry of the Interior; the 16 domestic intelligence services of the *Länder* report to the ministry of the interior of their respective Land. Based on this hierarchical system, the ministries of the interior exercise administrative and operational supervision over the domestic intelligence services. The BfV has no authority to issue directives to the LfVs, but it performs a coordinating role.

1.3. Scope of Activities of the Services

The 17 offices for the protection of the constitution are, as civil internal intelligence services, responsible for collecting and analysing information on anti-constitutional activities as well as on espionage by foreign countries. Their aim is to protect the free democratic basic order as well as the continued existence and security of the Federation and of the *Länder*.

The investigative activity of the domestic intelligence services mainly takes place prior to a possible concrete threat situation and/or prior to criminal laws being violated. As laid

down in Section 3(1) of the Federal Act on the Protection of the Constitution (BVerfSchG – *Bundesverfassungsschutzgesetz*), the BfV's and the LfVs' main task is to collect and analyse information

a) on activities
   - against the free democratic basic order
   - against the existence or security of the Federation or of a Land
   - that are intended to unlawfully hamper constitutional bodies of the Federation or of a Land or their members in the performance of their duties
b) on activities posing a threat to security or intelligence activities carried out in Germany on behalf of a foreign power
c) on activities carried out within the area of application of the BVerfSchG which, by the use of force or acts preparing the use of force, endanger the external interests of the Federal Republic of Germany
d) on activities carried out in Germany that are directed against the concept of international understanding, against peaceful relations between nations in particular.

In order to effectively perform their role as an 'early warning system', the BfV and the LfVs produce situation reports and analyses which enable the Federal Government or the governments of the *Länder* to initiate measures aimed at countering threats to the free democratic basic order or to internal security at an early stage. Furthermore, the domestic intelligence services, which on their part do not have any law enforcement powers, transfer intelligence to police authorities and public prosecutors to support the initiation of law enforcement measures.

Another field of work of the domestic intelligence services is protection against sabotage and the security of information: they conduct, for instance, security vetting checks of staff working in sensitive areas.

The Federal Intelligence Service (BND) is the external intelligence service of the Federal Republic of Germany. It reports to the Federal Chancellery and collects both military and civil information abroad which is of significance to Germany's foreign and security policies. Moreover, it prepares situation analyses for overseas deployments of the *Bundeswehr*, Germany's armed forces, and gathers intelligence on hostile intelligence services abroad.

The mandate of the Federal Office of Military Counterintelligence (BAMAD) includes the task of acting as an authority for the protection the constitution within the remit of the Federal Ministry of Defence. As the '*Bundeswehr*'s security service', the BAMAD protects the German armed forces themselves against extremist activities or activities jeopardising security within their own ranks while also protecting the German constitution against such endeavours. The other German intelligence services are explicitly not in charge of gathering intelligence on the German military. In the exercise of its duties, the BAMAD

may also – in connection with the *Bundeswehr*'s overseas deployments – become active abroad, which regularly entails overlaps of duties and requirements of dissociation from those of the BND.

1.4. Oversight and Supervision of the Services

Article 20(3) of the German Basic Law defines the principle of democracy. It states that the executive shall be bound by law and justice. Thus, also Germany's domestic intelligence services – as part of the executive – are also bound by the law in force.

Nevertheless, until the 1970s, there was the thesis that intelligence services, in their fight against the supposed 'adversary', were not able to absolutely adhere to law and justice. There was rather the view that those who clandestinely operate against adversaries operating clandestinely were generally acting in the interests of the order enshrined in the Basic Law.

Almost as late as in the 1980s, this view or interpretation changed. Since then, the supervision of the German intelligence services has been extended and has taken more and more definite and concrete forms, including legal regulations on the one hand and oversight bodies on the other hand, which were newly created or equipped with more far-reaching powers.

The work of the domestic intelligence services is governed by strict rules based on the principles of the rule of law. Infringements of the citizens' civil rights and liberties that the domestic intelligence services are allowed to commit are subject to conditions defined by special statutory provisions. In order to ensure that the domestic intelligence services strictly adhere to their statutory mission and to the legal provisions governing their work, there is a complex system of oversight in operation comprising several levels.

As an agency subordinate to the Federal Ministry of the Interior and Community (BMI), the BfV is subject to the BMI's supervision. The BMI exercises administrative and operational supervision.

In the exercise of their supervising responsibilities, the ministries of the interior examine the lawfulness and expediency of operation of the domestic intelligence service that they are responsible for (e.g. faultless and consistent application of law, transparency, communication of information). In addition, the ministries of the interior control the domestic intelligence services, for instance, by issuing directives and decrees on specific issues related to the protection of the constitution, by making agreements on targets or by giving guidelines. Controlling always takes place within the legal boundaries and on the basis of the statutory duties and powers of the domestic intelligence services. What is absolutely forbidden, however, is to exert any form of political influence on the domestic intelligence services and/or to instrumentalise them in the course of administrative or operational supervision.

The senior management of a domestic intelligence agency also performs a controlling function by determining priority tasks, by defining the focus of attention based on the

statutory mission and taking the existing subjects of monitoring into account or by deciding that activities presumed to be of intelligence concern must be investigated.

Apart from supervision by such executive bodies (i.e. the ministries of the interior), parliamentary, judicial and public oversight are to guarantee that the domestic intelligence services operate exclusively within the boundaries marked by the powers and competences assigned to them. What applies to all these supervisory systems is the fact that they are not commensurable, i.e. a certain supervisory process cannot be replaced with another or be made superfluous. Still, different forms of supervision can be interconnected and successive.

As for parliamentary oversight, one of the means of the German parliament, the Deutscher Bundestag, to exercise supervision over the BfV are parliamentary interpellations. A designated body of the parliamentary oversight is the Parliamentary Control Panel (PKGr), which is comprehensively informed by the Federal Government on a regular basis about the general work of the intelligence services and about matters of special significance. Once a year, the PKGr holds a public hearing of the heads of the three German federal intelligence services. During this hearing, the respective heads of service will answer questions about the implementation of organisational reforms and amendments with regard to statutory competences as well as about the investigation of extremism and terrorism.

As for restrictions on the privacy of correspondence, posts and telecommunications, which is protected by Article 10 of the German Basic Law, the independent G10 Commission, appointed by the PKGr, examines the permissibility and necessity of interception measures. In addition, the PKGr regularly submits a report on the kind and extent of such restrictions, which is open to the public as a printed paper of the German Bundestag.

The Federal Commissioner for Data Protection and Freedom of Information (BfDI) is responsible for supervising the BfV's compliance with and the implementation of data protection regulations, also having the right to inspect files.

Measures taken by the BfV that, as stated by the persons concerned, impair the rights of individuals are subject to judicial review.

However, the general public also exercises some kind of supervision, for instance, by way of media coverage of topics concerning the domestic intelligence services.

Oversight of the domestic intelligence agencies of the *Länder* (LfVs) takes place on the *Land* level based on an analogous system in accordance with the legal provisions in effect.

1.5. Legal Status of the Officers/Employees

In the Federal Republic of Germany, there is, for members of the civil service, a difference between civil servants and public employees. Germany's federal system also involves differentiation of federal, *Land* and municipal civil servants. The BfV employs both civil servants and public employees.

Article 33 of the German Basic Law contains a stipulation on the professional civil service. According to that, civil servants are especially employed where sovereign powers are exercised. ('The exercise of sovereign authority on a regular basis shall, as a rule, be entrusted to members of the public service who stand in a relationship of service and loyalty defined by public law.') The legal basis for the employment of civil servants is the Federal Civil Service Act (BBG – *Bundesbeamtengesetz*), which is complemented by additional laws and statutory instruments. Civil servants are not employed on the basis of a private-law employment contract, but their employment is based on a unilateral act of appointment on the part of the state. The positions are assigned to individuals depending on their aptitude, qualifications and professional achievements.

In the system of the professional civil service, there are four different career levels (*Laufbahnen* in German): lower, middle, higher and senior grades. They require, as conditions for entry, different levels of education (school-leaving qualifications in particular), they involve different kinds of tasks and vary according to (managerial) responsibility and pay.

Civil servants are in a special relationship of service and loyalty vis-à-vis their employer, which involves specific rights and duties. Sections 60 et seqq. of the BBG specify the duties of civil servants. They include the duty of neutrality, the obligation of impartial and just performance of duties and the obligation of loyalty to the constitution. Violations of these duties may be subject to criminal prosecution and may also be punishable under disciplinary law, i.e. the Federal Disciplinary Act (BDG).

On the other hand, this obligation of service and loyalty also implies special duties of care on the part of the employer vis-à-vis the civil servant. One of them is the duty of adequate financial support derived from Article 33 of the Basic Law, which includes an adequate salary, a pension and an allowance in case of illness. Such an allowance granted by the employer does not cover all the costs, however, but it is just a supplement to the civil servant's own health insurance that they can be expected to maintain. Furthermore, civil servants law generally provides for life tenure so that a termination of employment is only possible under certain strictly defined legal conditions.

Public employees, however, are employees who work in the civil service on the basis of a private-law employment contract. They are subject to the pertinent labour laws as well as to the labour contracts agreed between employers and public sector unions. As for the BfV's public employees, the Labour Contract for the Civil Service (TVöD) for the federal public sector applies. The TVöD lays down the essential conditions of employment.

A violation of the duties resulting from employment may have consequences under labour law, such as a written reprimand or the termination of employment.

Unlike civil servants, public employees are members of the statutory health, nursing care, annuity and unemployment insurances. In addition, there is an additional employee pension for the civil service.

There is no career level system in public labour law. Payment depends on the kind of job and professional experience. The job of public employees is assessed on the basis of agreements laid down in the TVöD as well as in supplementary labour contracts (Labour Contract on the Federal Payment System); the payment for their job is based on this assessment.

2. TASKS AND MANDATE

2.1. Investigative Powers and the Role in Criminal Procedure

When the Federal Republic of Germany was founded, the work of the intelligence services was reformed. The 'Police Letter' of 1949 stipulated that there had to be a separation between the law enforcement agencies and the domestic intelligence services. This principle of separation says that the community of the domestic intelligence services is not allowed to exercise any law enforcement – i.e. police – powers. The intelligence services merely collect and analyse information. Consequently, it is the sole competence of the police authorities to take, if required, law enforcement measures on the basis of intelligence thus produced. Vice versa, the police's powers are to exclude those specific ones of the intelligence services. The reason for this rule was the experience taught by the so-called Secret State Police (Gestapo), which had an almost limitless arsenal of power during the time of National Socialism.

The principle of separation involves three levels:

- First, there is a functional principle of separation. This refers to the above-mentioned division between law enforcement tasks (police competence) and those of preventive intelligence collection (competence of the domestic intelligence services).
- Secondly, there is an organisational principle of separation. This means that the tasks of the police and those of the domestic intelligence services must be carried out by two separate organisations.
- Finally, there is an informational principle of separation. The domestic intelligence services are not allowed to ask the police authorities for administrative assistance, for instance, to thus gain information collected by means of coercive methods that they would not have been allowed to use. The exchange of information between the police and the domestic intelligence services is, accordingly, subject to clear statutory provisions for transfer.

In consequence, the domestic intelligence services have, unlike the police, no law enforcement powers. Their activity is limited to the monitoring of and/or preventive intelligence collection on anti-democratic or anti-constitutional activities or activities posing a threat to security. There is no prosecution of criminal offences by the domestic intelligence services.

Unlike the police, the domestic intelligence services are not bound by the principle of compulsory prosecution (*Legalitätsprinzip* in German) either, but they are governed by the principle of opportuneness (*Opportunitätsprinzip* in German), which gives them some discretion over prosecution within certain limits. They have no compulsory obligation to initiate criminal prosecution. A possible interest in criminal prosecution may, for instance, be outweighed by the need of protection of an intelligence source. A source generally indicates the source of a piece of information, but in connection with source protection the term frequently refers to human sources.

The domestic intelligence services are – unlike the police – allowed to use covert techniques even before there is a concrete threat or offence.

As a general rule, there is an obligation to submit information in criminal proceedings. Pursuant to Section 96 of the German Code of Criminal Procedure (StPO), the highest service authorities may refuse to submit secret documents for reasons of public welfare, though. In such cases, there is the possibility of presenting intelligence information in court proceedings without any reference to the origin of the information by way of a written 'official testimony'. Such a testimony only contains unclassified information.

2.2. Intelligence Gathering

The investigative activity or intelligence gathering by the domestic intelligence services mainly takes place prior to a possible concrete threat situation and/or prior to criminal laws being violated. As laid down in Section 3(1) of the Federal Act on the Protection of the Constitution (BVerfSchG), the BfV's and the LfVs' main task is to collect and analyse information on anti-constitutional activities:

> *Section 3 of the BVerfSchG*
> *Tasks of the Authorities for the Protection of the Constitution*
> *(1) The task of the federal and Länder authorities for the protection of the constitution shall be to collect and analyse information, in particular factual and personal information, intelligence and documents, on*
> 1. *activities which are directed against the free democratic basic order, the existence or the security of the Federation or of a Land or are intended to unlawfully hamper constitutional bodies of the Federation or of a Land or their members in the performance of their duties*
> 2. *activities posing a threat to security or intelligence activities for a foreign power within the area of application of this Act*
> 3. *activities within the area of application of this Act which, by the use of force or preparations for the use of force, endanger the external interests of the Federal Republic of Germany*

4. activities within the area of application of this Act which are directed against the concept of international understanding (Article 9(2) of the Basic Law (Grundgesetz)), in particular against the peaceful relations between nations (Article 26(1) of the Basic Law).

The domestic intelligence services obtain the largest part of their information from open sources (OSINT), i.e. overt and publicly available sources. This is done by means of overt internet investigations, media monitoring and the analysis of public statements and actions.

In addition, the BfV is entitled to request information from other authorities and registries, e.g. the population register, National Firearms Register, Central Register of Vehicles, commercial register, land registries etc.

However, the collection of open material does not always produce a complete picture because foreign intelligence services, extremists and terrorists operate clandestinely, without overtly displaying their aims.

Therefore, the domestic intelligence services are also entitled to use covert intrusive techniques for gathering intelligence within the statutory boundaries and in accordance with the principle of proportionality. However, the use of such covert techniques will only be possible if all the other means of intelligence collection at hand are exhausted. In no event must the domestic intelligence services violate the core area of personal rights, which includes a person's most intimate spheres of private life in particular.

The covert techniques the intelligence services are entitled to use include, pursuant to Section 8(2) of the BVerfSchG, the use of confidential agents and informants, surveillance, image and sound recordings, cover identity documents and cover number plates.

Section 8 of the BVerfSchG
Powers of the Bundesamt für Verfassungsschutz (BfV)
(2) The Bundesamt für Verfassungsschutz (BfV) may use methods, objects and instruments for covert information gathering such as the use of confidential agents and informants, surveillance, image and sound recordings, cover identity documents and cover number plates. Interference with individual rights is permissible only on the basis of special powers. In any event, the use of a technique referred to in the first sentence must not create a disadvantage that is perceptibly disproportionate to the importance of the matter under investigation.

Under the Act on Restricting the Privacy of Correspondence, Posts and Telecommunications (Act adopted by virtue of Article 10 of the Basic Law – the Article 10 Act), the BfV and the LfVs are entitled to infringe on the privacy of correspondence, posts and telecommunications. An imperative prerequisite for such an infringement is the fact that such

monitoring is required to counter threats to the free democratic basic order of the Federation or of a *Land*. Another prerequisite is the existence of tangible evidence of certain serious crimes, e.g. treason against the internal security of the state, activity as an agent on behalf of a foreign intelligence service or forming a terrorist organisation. The last prerequisite is the fact that alternative methods of investigating the matter in question would be futile or would at least render its investigation considerably more difficult.

In addition to classic telecommunications interception, Section 11(1a) of the Article 10 Act, amended accordingly in 2021, provides for the interception of telecommunications at terminal devices (called *Quellen-TKÜ* in German) by the BfV.

> *Section 11 of the Act to Restrict the Privacy of Correspondence, Posts and Telecommunications – Implementation*
>
> *(1a) Telecommunications transmitted after the date on which the order was made may also be intercepted and recorded in a manner that interferes with an information technology system used by the person concerned if this is necessary to enable interception and recording in unencrypted form in particular. The content and the circumstances of the communication stored in the person concerned's information technology system after the date on which the order was made may be intercepted and recorded if they could also have been intercepted and recorded in encrypted form during ongoing transmission processes in the public telecommunications network.*

Furthermore, our national and international partners contribute to collating a valid basis of information by sharing intelligence of relevance.

2.3. Analytical Tasks

In order to effectively perform their role as an 'early warning system', the BfV and the LfVs produce situation reports and analyses, which enable the Federal Government or the governments of the *Länder* to initiate measures aimed at countering threats to the free democratic basic order or to internal security at an early stage. Furthermore, the domestic intelligence services, which on their part do not have any law enforcement powers, transfer intelligence to police authorities and public prosecutors to support the initiation of law enforcement measures.

The collection and analysis of information is designed to produce analytically processed intelligence that can be shared for further use in protecting the free democratic basic order.

It is a central task of the BfV's and the LfVs' analysts to produce assessed intelligence from the information gathered by overt and covert means. They structure, record and analyse the data obtained. They make a decision on whether to involve the police, to inform the ministry of the interior on a development or to procure further information in a systematic effort.

The intelligence will be contained in a variety of different reports, which are prepared to inform other (security) agencies, the ministries of the interior or the interested public.

The conditions for processing and sharing intelligence are laid down in the BVerfSchG. Each instance of transfer must be examined in advance and be registered. The examination deals with the question of whether the purpose of that transfer is proportionate to the infringement of the personal rights of the person concerned resulting from the transfer. The transfer of intelligence to the police authorities and public prosecutors, for instance, is subject to stricter conditions than that within the community of the domestic intelligence services.

2.4. Administrative Tasks

The BfV participates in security vetting checks pursuant to the Security Vetting Act (SÜG – *Sicherheitsüberprüfungsgesetz*).

According to the SÜG, the BfV takes the necessary measures on behalf of the bodies responsible for the security vetting checks. In general, the body responsible for the checks is the public authority, other federal public agency or political party under Article 21 of the Basic Law (GG – *Grundgesetz*) that wants to employ the person to be vetted, i.e. that wants to entrust a person with sensitive tasks.

Checks of persons who are to be entrusted with sensitive tasks within private bodies such as business enterprises generally fall within the competence of the Federal Ministry for Economic Affairs and Climate Action. The BfV participates in these checks, too.

A person's trustworthiness may be called into doubt when the security vetting checks raise concerns about his or her personal reliability (e.g. because of past criminal offences), when the person is not committed to the free democratic basic order or when there are concrete indications of a risk that foreign intelligence services or a terrorist or criminal organisation may attempt to approach and recruit the person.

Security risks can lead to the 'security vote', i.e. the recommendation as to whether a person can be entrusted with sensitive tasks, being negative.

The measures that the BfV takes range from the verification of the person's identity, queries in databases (e.g. concerning criminal convictions in the Federal Central Criminal Register) and the inclusion of the respective spouse/partner to investigations into the living environment of the person to be vetted, such as interviews with persons who can provide information and with reference persons.

As in any other administrative authority, the BfV's department of central services also carries out classic administrative tasks in the narrow sense, for instance, HR services, management of budgetary resources and facility management. The BfV's other tasks, its so-called core business, concern – as outlined above – the performance of its statutory monitoring duties according to Section 3 of the BVerfSchG.

2.5. ICT Security

The BfV's cyberdefence continuously carries out preventive monitoring and analysis of the activities directed against Germany by foreign states or by APT (Advanced Persistent Threat) groups controlled by such states. Moreover, the BfV's cyberdefence supports entities at risk and victims of cyber-attacks. In addition, it takes action when, for instance, IT infrastructure hosted in Germany is used by foreign actors to commit cyber-attacks against targets abroad. The BfV's competence in that regard derives from Section 3(1) No. 2 of the BVerfSchG.

In concrete terms, the cyberdefence department has three major tasks in connection with investigating cyber-attacks that have an intelligence background:

- **Detection of cyber-attacks**. In the first step, it is important to detect cyber-attacks at an early stage.
- **Attribution of these attacks to a state or an APT (Advanced Persistent Threat) group or naming of individuals involved in a specific cyber-attack**. To avert cyber-attacks before they occur, intelligence about the respective actors is of major importance. With a view to gaining such intelligence, the BfV's cyberdefence analyses the attacks and attributes them to profiles that take both the technical capabilities and the socio-political interests of state attackers into account. The attribution of a cyber-attack is an essential element of investigation proceedings and serves the Federal Government as the basis for making political decisions.
- **Prevention of cyber-attacks**. Only based on the intelligence collected can preventive measures then be effectively carried out in the final step. These can, for instance, include compiling technical indicators of an attack or enhancing malware detection systems. The BfV's cyberdefence provides information about possible attacks and publishes indicators of a compromise, which entities at risk can use to determine whether they have been affected and to take appropriate protective measures.

Fighting cybercrime (cyber-attacks committed by criminals who have no links to a state) falls within the area of competence of the police authorities.

2.6. Protection of Classified Information

Handling classified material is part of the daily work at the BfV; it is governed by the directive on handling classified material developed by the Federal Ministry of the Interior and Community (BMI).

The directive on handling classified material is for federal authorities that work with classified material as well as for individuals who are employed there and have access to classified material or carry out activities in the context of which they can access classified material.

In the directive, classified material is defined as sensitive facts, objects or intelligence, regardless of the forms that these take (e.g. documents, photographs, electronic data carriers, technical equipment or spoken words), which must be kept secret in the public interest, in particular to protect the welfare of the Federation or of a *Land*.

The organisational unit responsible for material security at the BfV creates the organisational, constructional, mechanical, electronic and IT conditions to ensure the protection of classified material. This includes regulations on the handling of classified material, e.g. on its preparation, specific labelling, transport, release or storing (safes, electronic protection).

Only persons who have passed security vetting checks for the purpose of establishing their reliability may be authorised to handle classified material. In the area of personnel security, the BfV carries out almost 60,000 security vetting checks of persons annually.

2.7. International Cooperation

According to Section 1(1) of the BVerfSchG, the purpose of protection of the constitution is to safeguard the free democratic basic order as well as the existence and the security of the Federation and of the *Länder*. Thus, the BfV is an intelligence service responsible for the internal security of the Federal Republic of Germany.

> *Section 1 of the BVerfSchG*
> *Duty of Cooperation*
> *(1) The purpose of protection of the constitution is to safeguard the free democratic basic order as well as the existence and the security of the Federation and of the Länder.*

In order to fulfil this statutory mandate, however, the BfV's investigations cannot be limited to German territory alone. Almost all of the BfV's fields of work include international aspects. This is also reflected in the first sentence of Section 5(5) of the BVerfSchG. Accordingly, the BfV is responsible for official contacts with the competent public bodies of other states where such contacts are required for the performance of the BfV's tasks pursuant to Section 3 of the BVerfSchG.

> *Section 5 of the BVerfSchG*
> *Competences of the Bundesamt für Verfassungsschutz (BfV)*
> *(5) The Bundesamt für Verfassungsschutz shall be responsible for official contacts with the competent public bodies of other states where such contacts are necessary for the performance of tasks pursuant to Section 3.*

The cooperation with foreign partner services in matters relating to the protection of the constitution is primarily the responsibility of the BfV, and thus it also acts as the body that centrally coordinates the contact of the 16 domestic intelligence agencies of the *Länder* (LfVs) with foreign partner services.

International cooperation in practical matters is furthermore governed by Section 19(3) of the BVerfSchG; it provides the legal basis for the transfer of personal data by the BfV to foreign public bodies and supranational and intergovernmental bodies. What is more, Section 22b of the BVerfSchG allows for the creation of joint data files and Section 22c of the BVerfSchG allows for taking part in joint data files with foreign intelligence services.

The BfV's cooperation with foreign intelligence services is carried out in various ways, for istance, in multilateral bodies and it is an essential pillar in the performance of the BfV's tasks.

The mutual exchange of relevant intelligence with foreign intelligence services is subject to strict data protection regulations at all times and must always be examined on a case-by-case basis.

2.8. Personal Data Protection

According to Article 2(2)(a) of the European General Data Protection Regulation (GDPR) in conjunction with the third sentence of Article 4(2) of the Treaty on European Union (TEU), the processing of personal data in the field of intelligence work falls outside the scope of the GDPR as a Union legal act.

At the BfV, the protection of the personal data of data subjects is guaranteed by the corresponding special legal provisions of the BVerfSchG. Hence, the BVerfSchG constitutes a specific complete legal framework for data protection that does not leave room for the GDPR or the implementing provisions of the Federal Data Protection Act (BDSG – *Bundesdatenschutzgesetz*) referring to the GDPR to be applied in the context of the performance of the BfV's tasks.

This means that the BVerfSchG fully governs all aspects of the processing of personal data (such as collection, storage, adaption, consultation, disclosure by transmission, erasure or destruction as well as 'restriction of processing') for the purpose of the performance of the BfV's tasks pursuant to Section 3 of the BVerfSchG. The BVerfSchG also establishes the right of the data subject to have incorrect personal data rectified and to have personal data erased when they are not or no longer required for the performance of the BfV's tasks. The right of the data subject to be provided with information on the processing of his or her data by the BfV is also laid down in the special legal provisions of the BVerfSchG.

According to Section 15(1) of the BVerfSchG, all individuals generally have the right to request information on the data stored on them by the BfV. To justify his or her right to request information, it is necessary that the individual concerned is able to show

a particular interest in receiving this information and that he or she refers to a specific matter (e.g. participation in a particular demonstration).

The right to request information is limited under the following conditions set out in Section 15(2) of the BVerfSchG: information will not be provided if there is:

- a risk that the provision of information would threaten the performance of the BfV's tasks
- a threat to sources
- a risk of discovery of the intelligence held by and/or the working methods of the BfV
- a threat to public security
- the necessity of keeping the data secret.

There is no right to inspect files.

According to Section 15(3) of the BVerfSchG, the obligation to provide information does not extend to the origin of the data or the recipients of data transfers.

In case the provision of information is refused, the data subject may request the Federal Commissioner for Data Protection and Freedom of Information (BfDI) to review the lawfulness of the possible storage of his or her personal data as well as the refusal to provide information. The data subject may also take legal action. Irrespective of this, it is generally possible to directly contact the BfDI requesting information on one's personal data that may be stored by the BfV.

General oversight of the BfV by the national data protection supervisory authority (BfDI) is governed by the BVerfSchG as a special regulation. For this reason, the BfDI's rights to control the BfV have remained unchanged since the point in time that the GDPR has to be applied by the EU member states; particularly, the more extensive powers stipulated in the GDPR have not been conferred to the BfDI when it comes to oversight over the BfV.

CHAPTER IX

Greece

Panagiotis Kontoleon

1. POSITION OF THE SERVICES IN THE DOMESTIC LEGAL SYSTEM

1.1. Position and Role of the Services in the Public Administration System

The National Intelligence Service (EYP) shall be an autonomous public civilian service and come under the authority of the Prime Minister who is competent to determine the activity of the EYP, in the context of national priorities of the government policy.[1]

The EYP shall consist of the Central Service and the Regional Units.[2]

The mission of the EYP, in the context of the Constitution and the laws, shall be to seek, collect, process and notify to competent authorities information about:

- protecting and promoting the country's political, economic, military and overall national strategic interests
- preventing and dealing with activities constituting threats against democracy, the fundamental human rights, the territorial integrity and the national security of the Greek state as well as the country's national wealth
- preventing and dealing with activities of terrorist organisations and other organised crime groups.[3]

---

1 Law 3649/2008, Official Gazette A' 39, *National Intelligence Service and Other Provisions*, Article 1, *Character-Subordination*, as amended by Law 4704/2020, Official Gazette A' 133, *Acceleration and Simplification of the Audio-Visual Works Support, Strengthening of Digital Governance*, Article 30(1).

2 Law 3649/2008, Article 3(1), *Composition – Structure.*

3 Law 3649/2008, Article 2(1), *Mission.*

The following Hellenic Police services operate on the territory of Greece:

- The State Security Division (DIKA)[4]
- The Information Management and Analysis Division (DIDAP),[5] subject to the Head of Police[6]
- The Special Violent Crime Division (DAEEB) of the Hellenic Police,[7] subject to the Head of Police.[8]

The Hellenic Police is a special armed Security Corps. The services of the Hellenic Police and its staff are on constant alert for the prevention and suppression of crime, the protection of the democracy and the rule of law and the response to emergencies. The uniformed personnel are considered to be in an ordered service, in any case where their intervention becomes necessary.[9] Preventive action is the primary duty of the Hellenic Police. It aims to prevent crime and ensuring public peace, order and seamless social life of citizens. The suppressive action is manifested in cases of execution or an attempt to commit a criminal offence, either as a judicial pre-trial investigation or as a pursuit action. It aims to thwart the criminal actions or reduce their adverse consequences, to investigate the committed crimes, to detect and arrest the perpetrators and to find and confiscate the evidence and the product of crime.[10]

- The Military Intelligence Directorate (DDSP) and the intelligence branches of the National Defence Headquarters come under the Minister of National Defence and their competence is the defence of the country.
- The Government Council for National Security (KYSEA) has a permanent character and exercises its responsibilities, in the context of the general directions of the government policy, as it is determined by the Council of Ministers.

  The President of the KYSEA is the Prime Minister.

The Government Council of National Security is responsible for formulating interministerial policies and making decisions on issues related to the security of the country. In particular, the Council formulates the national security strategy by taking into account foreign and defence policy, public order and civil protection policy, cybersecurity strategy, energy security and the security of critical national infrastructure. At the same time,

---

4 Presidential Decree 178/2014, Official Gazette A' 281, *Organisation of Services of Hellenic Police*, Article 2(3)(b) and Article 7(1, 3).

5 Law 4249/2014, Official Gazette A' 73 on the reorganisation of the Hellenic Police, Fire Brigade, Upgrade of Services of the Ministry of Citizen Protection, Article 22(1).

6 Presidential Decree 178/2014 Article 1(3)(a), as amended, with Presidential Decree 88/2019, Official Gazette A' 135, *Amendment of Provisions Concerning Organisational Issues of Police Services*, Article 1(2).

7 Presidential Decree 178/2014, Article 29 and Law 4689/2020, Official Gazette A' 103, *Transposition at the National Law of Directive… 2017/541*, Article 37.

8 Presidential Decree 178/2014, Article 1(3)(a), as amended, with Presidential Decree 88/2019, Article 1(2).

9 Law 4249/2014, Article 13(1, 2).

10 Presidential Decree 141/1991, Official Gazette A' 58 on the Responsibilities of Bodies of the Ministry of Citizen Protection, Issues of Organisation of Services, Article 93(1, 2).

it coordinates the relevant bodies and necessary resources in order to implement the national security strategy.[11]

- The General Secretariat of the Prime Minister includes, *inter alia*, the Office of National Security Advisor who is responsible for supporting the Prime Minister and the Government Council for National Security (KYSEA) for any issue related to internal and external security of the country and the management of the risks and crises related to it.[12]

1.2. Oversight and Supervision of the EYP

- **Prime Minister**

The National Intelligence Service (EYP) shall come under the authority of the Prime Minister.[13]

- **EYP Director General**

The EYP Director General shall manage, guide, coordinate, and supervise the service and shall be liable to the Prime Minister for the performance of his or her duties.[14]

- **Parliamentary Control**

The Government is subject to parliamentary control.

The parliamentary control means include petitions, questions, current questions, applications for documents submission, interpellations, current interpellations etc. Specifically, Members of the Parliament have the right to address a written question to the Prime Minister or the Ministers regarding any matter of public importance aiming at keeping the Parliament updated on specific issues.

In case that the question pertains the activity of the EYP, the Prime Minister should give a response.[15] Hence, the EYP is under its political head's scrutiny.

- **Special Permanent Committee on Institutions and Transparency**

The President of the Hellenic Parliament constitutes special permanent committees. The special standing committees are set up in proportion to the representation of the parliamentary groups with the participation of at least one member from each parliamentary group.[16]

The parliamentary control for issues concerning EYP activity is a competency of the Special Permanent Committee on Institutions and Transparency.

The Government must, either on its own or at the request of the Committee, inform the Committee about the activity of the EYP, unless there are reasons of overriding a public

---

11 Law 4622/2019, Official Gazette A' 133, *Executive State: Organisation, Operation Transparency of Government Bodies*, Article 7(1, 2, 5).
12 Law 4622/2019, Article 23(2)(b, d).
13 Law 3649/2008, Article 1.
14 Law 3649/2008, Article 9. *Director General-Deputy Directors*, par. 6.
15 *Code of Governing the Hellenic Parliament*, Official Gazette A' 106/1987, Article 124, as amended with Official Gazette A' 284/2001, Article 10(1)(a) and with Official Gazette A' 92/2017, Article 18.
16 Official Gazette A' 126/2008, Article 11(10).

interest or protection of personal data, which are reported by the EYP Political Head to the Committee.

The Special Permanent Committee on Institutions and Transparency can summon, in hearing, EYP Director General, for issues that pertain to the activities of the EYP.[17] The discussions about the activity of the EYP are confidential and the members of the committee ought to maintain this confidentiality after the end of their term.

The Committee may publish the findings of its audit, always taking into account the above-mentioned obligation of confidentiality.

- **Authority for Communication Security (ADAE)**

The Authority for Communication Security protects the secrecy of communication in any possible way, as well as the networks and information security.

The ADAE proceeds in monitoring the compliance to the terms and the procedures of lifting of communication privacy, without placing under scrutiny the judgment of the competent judicial authorities.

The Authority for Communication Security puts into effect scheduled and emergency auditing procedures, *ex officio* or upon complaint, of installations, equipment, archives, databases and documents of the EYP.

The personal attendance of the President of the ADAE is required for the monitoring of archives kept for reasons of national security.[18]

- **Public Prosecutor**

A public prosecutor shall be posted to the EYP by decision of the Supreme Judicial Council for a period of up to three years. Such an official shall check the legality of special operational actions of the EYP relating to human rights and shall have any other powers assigned to him or her.[19]

1.3. Legal Status of the Officers/Employees

The EYP personnel shall consist of:

- permanent civilian personnel
- special scientific and technical or auxiliary personnel under a fixed or open-ended private law employment contract
- other officers of the public sector.[20]

---

17 Official Gazette A' 106/1987, Article 43A. *Special Permanent Committees.*
* Article 43 A was added with Official Gazette A' 151/1996.
** Article 43 A was amended with Official Gazette A' 126/2008.

18 Law 3115/2003, Article 1 and Article 6(1)(a).

19 Law 3649/2008, Article 5(3).

20 Law 3649/2008, Article 10(1). *Categories of Personnel.*

The organic positions of the EYP personnel shall be determined in total in its Regulation.[21] The composition of EYP personnel by branch and specialty shall be determined in the bylaws and the Composition and Distribution Table of personnel,[22] which are confidential and shall not be published in the Official Gazette.[23]

The EYP bylaws shall regulate the details of the organisational structure of EYP services, their staff, their specific powers, the specific duties of the Director General, the Deputy Directors General and the head of units as well as the specific obligations of EYP personnel.[24]

The EYP Director General and Deputy Directors General, its personnel of any category as well as its employees of its autonomous units with any kind of employment relationship or project contract or members of working groups, collective bodies or committees, shall have a duty of confidentiality in relation to documents, information or other particulars of which they are made aware in the context of performance of their duties. The violation of the confidentiality duty shall constitute a disciplinary offence, which shall be punished pursuant to the Civil Servants Code.

The above persons shall also have a confidentiality duty relating to classified documents, information or other particulars even after their withdrawal from the service, for the duration of the classification.

Any person who publicises in any way classified documents or information concerning the official status of the EYP personnel and equipment and any person who breaches the duty of secrecy or confidentiality, shall be punished by imprisonment of at least one (1) year and a financial penalty, provided that the act is not punished more severely pursuant to any other provision, particularly Articles 146 and 147 (about espionage) of the Penal Code.

The EYP personnel shall not testify as witness before courts or any other authority in relation to matters, information, facts or persons concerning the service without the prior approval of the Prime Minister.

Notwithstanding any general or special provision as currently in force, the EYP shall be exempted from the obligation to forward to other public services and legal entities in public or private law any information or particulars, if the Director General considers that the publication thereof would prejudice public interests. Access to EYP files shall be allowed only to its personnel that are authorised to keep and process that information.[25]

The opportunity to defend themselves before the criminal courts is provided to the EYP staff, against whom criminal proceedings are conducted for offences attributed to them in the performance of their duties, by officials of the Legal Council of the State (NSK), by

---

21 The EYP Regulation is included to the Presidential Decree 1/2017, Official Gazette A' 2, as amended by Presidential Decree 96/2020, Official Gazette A' 232. *Amendment of the EYP Regulation*.

22 Law 3649/2008, Article 10(2).

23 Law 3649/2008, Article 12. *Bylaws*.

24 Law 3649/2008, Article 12. *Bylaws*.

25 Law 3649/2008, Article 14, *Duty of Confidentiality*, par. 1–5, as amended with Law 4704/2020, Article 27(7).

decision of the President of the NSK, after prior approval of the EYP Political Head, if: a) the act, for which they are prosecuted does not constitute the commission of a disciplinary offence and b) the staff will not be represented by a lawyer. The employee is deprived of legal coverage, in the case that the criminal prosecution against him or her is a consequence of a complaint by the service.[26]

A presidential decree (the EYP Regulation) determines the formal and substantive qualifications (general, special and additional) of candidates of all categories and specialisation of staff, the terms, the conditions, their scoring and the procedure for their selection, appointment, distribution and training.[27]

The vacancies of civilian staff are filled, by selection after announcement among those who have the qualifications provided in the EYP Regulation.

The appointed civilian staff is subject to a two-year probation during which it attends the introductory training programs provided for the newly appointed employees by the provisions of the Civil Servants Code and attends EYP seminars.[28]

The Service Board[29] of the EYP civilian personnel, competent for the judgment of staff during their professional career, shall consist of the following five members:

- The Deputy Director General, appointed by EYP Bylaws as Chairman, substituted by the other EYP Deputy Director General, by decision of Director General[30]
- Two permanent EYP civil servants of the highest rank and holders of a university degree appointed, along with their substitutes, by the Director General
- Two elected representatives of EYP civil servants, who will be elected by direct and secret ballot of EYP civilian staff.[31]

The Service Board shall perform the duties of the Disciplinary Board. The decisions of the Board shall only be challenged before competent courts.[32]

The Director General has disciplinary authority. The disciplinary penalties are imposed to the EYP civilian personnel as provided by the applicable provisions for the EYP.[33]

---

26 Law 3649/2008, Article 14A(1)(a). *Legal Defence of the EYP Staff*.
* Article 14a was added with Law 4456/2017, Official Gazette A' 24. *Additional Measures for the Implementation of Regulation 1141/2014… Issues of Ministry of Interiors*, Article 13(1).

27 Law 3649/2008, Article 11A(1).
* Article 11A was added with Law 4033/2011, Official Gazette A' 264 *Adaptation of Directive 2009/18*, Article 28(11)

28 Presidential Decree 1/2017, Article 43. *Appointment of Civilian Staff*.

29 Law 3649/2008, Article 15. *Service Board*.

30 Law 3649/2008, Article 15(1)(a) was amended with Law 4623/2019, Official Gazette A' 134. *Provisions of the Ministry of Interiors*, Article 113(2).

31 Law 3649/2008, Article 15(1)(c) was replaced with Law 3938/2011, Official Gazette A' 61. *Establishment of an Office for Arbitrariness in the Ministry of Civil Protection*, Article 20(4).

32 Law 3649/2008, Article 15(4).

33 Presidential Decree 1/2017, Article 54(1, 2). *Disciplinary Provisions*.

The principles and security standards that the EYP should apply for the protection of the classified material and specifically for the handling, safeguard and distribution of classified material are stipulated in classified legal acts.

The EYP personnel, handling classified material, are trained accordingly in order to achieve the highest degree of familiarisation with the safety measures and perform their duties effectively.

2. TASKS AND MANDATE

To carry out its mission, the EYP shall have the following powers:

- To collect and provide information and data, make evaluations and submit recommendations to the Prime Minister and other competent ministers about the prevention or aversion of threats against national security or the democracy as well as the protection of the country's national interests.
- To seek, collect, process and provide intelligence, in the context of the preceding paragraph, mainly about matters relating to the activities of terrorist organisations or other organised crime groups in the fields of trafficking of human beings, human organs, weapons, drugs or other prohibited substances, mainly nuclear, radiobiological and chemical substances (NRBC), as well as about matters relating to money laundering.
- To coordinate, in the context of Government Council for National Security decisions, the activities of the country's intelligence and security services in the field of collection and dissemination of information relating to the EYP mission. Also, to cooperate with and inform the Military Intelligence Directorate (DDSP) and the intelligence services of the army, the navy and the air force, supervised thereby on matters of their competence.
- To prevent and handle espionage activities against the country.
- To provide the state's competent crisis management bodies with intelligence, to assist them in their mission.
- To provide competent bodies of the Ministry of National Defence with intelligence for the operational planning of the National Defence General Staff.
- To serve as the Information Security Technical Authority (INFOSEC) and procure the security of national communications and information technology systems, as well as the classified material certification of national communications.
- To be designated as National Authority against Electronic Attacks. It is competent for preventing and dealing – statically and actively – with electronic attacks against communication networks, information storage facilities and computer systems.[34]

[34] Law 3649/2008, Article 4. *Competences*.

- To prepare, on the basis of available intelligence, information bulletins, studies and reports which shall be forwarded to the competent authorities.
- To cooperate with relevant services of other countries and international organisations, as well as state services and legal entities in public and in private law of the broader public sector for the more effective performance of its duties.

For the promotion of the work of the EYP, the modernisation of its function and the facilitation of its cooperation with the aforementioned bodies (last point):

- The EYP may sign memorandum of cooperation with the bodies, in particular the Ministry of Foreign Affairs, the Ministry of Citizen Protection, the Ministry of National Defence, the Ministry of Digital Governance. The memorandums of cooperation specify the object and the terms of each cooperation.
- Working Groups may be set up consisting of members of EYP staff and by members proposed by the respective collaborating body, by decision of the Director General.
- The memorandums of cooperation and decisions shall not be published in the Official Gazette.[35]

It is obvious that the EYP manages all intelligence for the profit of the state and it is ready to respond to any lawful demand in the framework of its competences.

The EYP is authorised to operate inside and outside the country but does not have executive competences, unlike prosecuting authorities (i.e. the police).

The EYP includes a Historical Archive and a Historical Museum Service. They come directly under the EYP Director General, with the main task of filing and developing documents and audio-visual material, as well as the assortment and maintenance of museum materials.[36]

2.1. Investigative Powers and the Role in Criminal Procedure

When exercising the powers of the EYP, its personnel:

- shall lift, by order of the public prosecutor, who is posted to the EYP, the secrecy of letters and telephone or other communication and record the activities of persons out of their residences, using special technical media, especially audio-visual devices
- may collect information, on matters of national security by infiltration, following an order of the EYP Director General and with the approval of the supervising public prosecutor

35 Law 3649/2008, Article 4(9), as replaced with Law 4625/2019, Official Gazette A' 139, *Provisions About Infrastructure Ministry*, Article 21(1).

36 Law 3649/2008, Article 3(4)(b), as amended by Article 27(1) of Law 4704/2020.

- may act under cover of identity, capacity or activity, individually or collectively, as specified in its bylaws
- are obliged to carry out their duties in compliance with the provisions of Law 3115/2003.[37]

Authorised EYP personnel may, if deemed necessary and at the request of the competent authority, take part in control and shall express an opinion about whether a foreign citizen is dangerous to national security and whether he or she meets the requirements to be characterised as persona non grata.

The EYP personnel shall be trained in the use of weapons and special devices and machines. Specific EYP personnel carry weapons for their own protection and the protection of EYP facilities.[38]

State services and legal entities in public and in private law of the broader public sector, as well as the first and second instance local authorities, shall be obliged to provide authorised EYP officers with any information or assistance required to perform their duties. The aforementioned bodies and EYP personnel shall be obliged to observe the secrecy of communication and of the content of the request, as well as of the identity of the personnel that undertook the case.

Any refusal, delay or neglect, any incomplete and untimely response to the request for official assistance, as well as any violation of the obligation to observe the secrecy shall constitute special disciplinary offence, punishable pursuant to the Civil Servants Code.[39]

For the purpose of performing their duties more effectively, the EYP personnel shall be educated, trained, specialised in the service's educational courses and participate in programmes conducted by domestic or foreign bodies.[40]

2.2. Personal Data Protection

The EYP has designated a Data Protection Officer who reports to the Head of the Service.[41]

Competence of the Hellenic Data Protection Authority (HDPA)

The EYP personnel are obliged to carry out their duties in compliance with the provisions of laws concerning personal data protection (4624/2019 and 2472/1997).[42]

---

37 Law 3115/2003, Official Gazette A' 47 on the Hellenic Authority for Communication Security and Privacy.

38 Law 3649/2008, Article 5. *Supervision – Method of Exercise of Powers*, par. 1b, 2, 4.

39 Law 3649/2008, Article 6. *Obligations of Authorities – Services*, par. 1, 2.

40 Law 3649/2008, Article 13. *Training of EYP Personnel*, par. 1, 2.

41 Law 4624/2019, Official Gazette A' 137 on the Hellenic Data Protection Authority (HDPA) and Measures for Implementing Regulation (EU) 2016/679 (GDPR), Articles 6, 7, 8 on the Appointment, Position and Duties of the Data Protection Officer.

42 Law 3649/2008, Article 5(1).

* Law 4624/2019, Article 83 has replaced Law 2472/1997, Official Gazette A' 50 on Personal Data Protection.

** According to Article 84 of Law 4624/2019, certain provisions of Law 2472/1997 are still in force.

Every data subject shall have the right to lodge a complaint with a supervisory authority if the data subject considers that the processing of personal data relating to him or her, infringes his or her rights.[43]

The Hellenic Data Protection Authority shall handle complaints lodged by the data subject and inform the complainant of the progress and the outcome of the investigation or inspection within a reasonable time period.[44]

The Authority shall not be competent to supervise processing operations of classified personal data carried out for activities concerning national security.[45]

[43] Article 77 of Regulation (EU) 2016/679 (GDPR) on the right to lodge a complaint with a supervisory authority. Law 4624/2019, Article 1.
[44] Law 4624/2019, Article 13(1)(g).
[45] Law 4624/2019, Article 10(5).

CHAPTER X

Hungary

Péter Béla Kalász

1. POSITION OF THE SERVICES IN THE DOMESTIC LEGAL SYSTEM

1.1. The Concept of the National Security Services

The organisation, legal statuses and tasks of the national security services of Hungary are stipulated in the Act CXXV of 1995 on the National Security Services.

Pursuant to the Act, the national security services of Hungary constitute the following organisations:

- the Information Office (IH)
- the Constitution Protection Office (AH)
- the Military National Security Service (KNBSZ)
- the Special Service for National Security (NBSZ)
- the National Information Centre (NIK).

In general, the national security services promote the national security interests by open and clandestine information gathering, performing tasks enabled by special tools (powers) of the national security services. Their tasks include the detection of threats and information gathering in relation to the protection of the national security interests in order to counter and hinder the hostile activities and intentions endangering the security of the nation.

The collection, analysis and assessment of information and data on threats are essential in preventing circumstances posing external threats to the nation and the country. Similarly, the assessment of the external security environment and its impact is important to enforce the interests of the country as well as to prevent, detect and counter domestic threats in Hungary.

1.2. The Position and Role of National Security Services in the Public Administration System

The military and civilian national security services are governmental institutions with individual budgetary provisions and independent financial management. The services are directed by the Government and have nationwide territorial competence.

The Government shall manage the Military National Security Service through the minister responsible for national defence; the Information Office (IH), the Constitution Protection Office (AH), the Special Service for National Security (KNBSZ) and the National Information Centre (NIK) through the minister in charge of direction of civilian national security services, currently the Minister for the Cabinet Office of the Prime Minister.

The recommendation for the appointment regarding the Director General of the Special Service for National Security shall be taken by the minister in charge of direction of civilian national security services in agreement with the minister responsible for national defence and the minister responsible for law enforcement.

The national security services have many similarities to law enforcement agencies and the military forces, such as the chain of command and ranks of their personnel. There is a relevant distinction regarding the use of force, as it is a sanction possibly applied by the law enforcement and national security agencies only as the last resort, whereas the use of force obviously is not only a marginal option in the case of the military.

1.3. Scope of Activities of the National Security Services

The Military National Security Service is a national security service specialised in foreign and domestic military intelligence and counterintelligence.

The Information Office is a civilian national security service performing foreign intelligence tasks.

The National Information Centre is also a civilian national security service. Its main task is to analyse the security and criminal situation in Hungary and report to the government, and to facilitate cooperation between law enforcement organisations and national security services.

The Special Service for National Security, *inter alia*, provides services for the implementation of secret information gathering, ensures specific telecommunications connections to the users specified by the government and provides administrative supervision in relation with the protection of security documents.

The Constitution Protection Office

The Constitution Protection Office has a wide range of competences, including counter intelligence (CI). In this respect, the Constitution Protection Office shall detect and counter the

foreign secret service endeavours and activities interfering with or threatening the sovereignty or the political, economic, security or other important interests of Hungary.

The detection activity is fundamentally preventive, the essence of which is to identify the covert efforts preferably before the adverse economic and political damage. The CI activity aims to deactivate, hinder and prevent the risks and dangers having been identified.

The Constitution Protection Office shall also detect and counter surreptitious endeavours to alter or disturb the law and order of Hungary by unlawful means. Influencing activities typically affect the functioning of the institutions of public and state administration and the perpetrators try to make the operation of those organisations more difficult and destabilise them in order to achieve their goals.

Within this framework, when the national security service becomes aware of information that falls within their competence, it may transfer that information to the law enforcement organisations responsible for the physical security of an event.

The Constitution Protection Office is also responsible for combating violent religious extremism. Within this framework, *inter alia*, the Constitution Protection Office may provide its official standpoint as a special authority in the proceedings where churches and religious denominations apply to the competent authority for the acquisition of registered ecclesiastical status. It should be noted that the resolution of by the Constitution Protection Office in this procedure is not binding.

The Constitution Protection Office shall detect and counter the covert efforts endangering the economic, scientific-technical and financial security of Hungary as well as the illegal drug and arms trafficking. The economy security can be divided into two major group of tasks. On the one hand, it means the protection of national assets and budgetary interests. On the other hand, it means the protection of the financial system. It should also be noted that only covert endeavours are included in this scope, but these efforts do not necessarily have to constitute a criminal case. The act/event therefore falls within the competence of the Constitution Protection Office in case it interferes with the operation of the national economy, i.e. it involves a potential risk to national security.

The Constitution Protection Office shall provide for the security of organisations (institutions) and facilities relevant for central state power and governmental activities. Within this framework, the Constitution Protection Office shall support the operation of protected institutions free from external influences and the detection, prevention and eradication of illegal attempts to establish relationships that would jeopardise it. In addition, the tasks of the Constitution Protection Office in the field of institutional protection include countering possible data and information leaks, attempts to unlawfully influence official procedures as well as systematic detection and prevention of risk factors and increasing security awareness, also by presenting case studies. The Constitution Protection Office is also responsible for identifying deficiencies related to the safety of the protected organisations.

It should be noted that the aforementioned protection does not correspond to the provision of physical protection (for which the police departments and the Parliamentary Guard are responsible). The Constitution Protection Office does security vetting, it checks databases for traces and collects information.

Government Decision No. 2009/2015 determines the organisations (institutions), which need to be protected. These organisations are relevant for the central state administration and government activities and include, for instance, ministries, the Constitutional Court, the Office of the Prosecutor General, and the National Tax and Customs Administration.

The Government Decision also lists a number of enterprises and facilities important for the central state administration and government activities. For these organisations, it is not mandatory, but optional to conclude a cooperation agreement. If an enterprise refrains from taking advantage of the offered option, it shall not be obliged in any other way to cooperate.

The tasks of the Constitution Protection Office include not only the protection of organisations and institutions important for government activities, but also the provision of national security protection of persons in certain positions. This includes, among others, the President of the Republic, the Prime Minister, the Prosecutor General and his deputies, and the Governor and Deputy Governors of the Hungarian National Bank.

The purpose of the national security protection ensured by the Constitution Protection Office is to detect and counter efforts interfering or jeopardising the national security interests of Hungary, including covert efforts targeting the activity of protected persons and the illegal access to protected information related to the activity of these persons.

It should be emphasised that national security protection and physical protection are not the same. They are interrelated, interdependent activities, but the two types of protection cover two different areas of protection of the protected person. The law enforcement agencies and the national security services perform the protective duties in close cooperation.

In the case of many occupations, the employment is bound to having a national security clearance that is based on the conduct of national security vetting.

The purpose of the national security vetting is to examine whether there is any national security threat to the legitimate operation of the state and national economy in the context of the security conditions of those individuals falling under national security vetting.

National security threat is being established if the persons subjected to national security vetting are unsuitable for the lawful performance of the position bound to national security vetting without undue influence or if there are circumstances that interfere with or endanger the interests of the protection of classified information. The difference between the two groups is that in the former case, the person under vetting wittingly carries out unlawful influence or pursuit of it, while in the latter case, there are risk factors in which the person unwittingly falls victim to unlawful information acquisition.

The Act CXXV of 1995 on the National Security Services, its executive orders and the internal regulations of the individual institutions list and define the positions for which a national security vetting procedure is required and describe the positions for which the conduct of national security vetting is excluded. The latter includes, for instance, the Prime Minister, the President of the Republic and members of the Parliament (with the exception of members of committees responsible for parliamentary control of the national security services). If a national security risk factor arises during the vetting procedure, as a general rule, the legal relationship on which the vetting is based cannot be established or maintained. There is an exception when it is approved by the organisation or person supervising the individual or organisation which has established a legal relationship subject to national security vetting. The risk-free security experts' statement is valid for 5 years from the date of issue. The entitled entity shall initiate a new national security vetting procedure maximum 180 days and minimum 90 days before the expiry of the valid risk-free personal security certificate.

If the subject to the national security vetting does not accept the risk assessment, he or she may appeal to the minister in charge, and in the second instance he or she may appeal to the National Security Committee and to the Budapest-Capital Regional Court in the third instance.

The Constitution Protection Office also has the responsibility to control legal and illegal migration. Within this framework, the Constitution Protection Office carries out the national security screening of the persons applying for the document certifying settled status, seeking refugee status, applying for Hungarian citizenship and having submitted an application for a visa.

In the course of the control of illegal migration, the Constitution Protection Office shall detect and counter the covert activities of the persons and groups related to the mentioned applications, entering or staying in Hungary unlawfully and those who facilitate it, thus, those who endanger the national security of the country.

The Constitution Protection Office participates as an advisory authority in proceedings related to citizenship, residence permits and visa procedures. In the course of these official proceedings, the expert statement provided by the Constitution Protection Office shall not be binding; the competent authority may take a decision to the contrary.

The Constitution Protection Office, on the other hand, acts as a special authority in the procedure for establishing settlement, asylum and stateless status. Within the framework of these proceedings, the resolution of the Constitution Protection Office has a binding effect, thus, no contrary decision can be made by the authority.

The Constitution Protection Office may detect a range of crimes until the investigation is ordered, including crimes against humanity, war crimes, crimes against the state as well as some military crimes of great importance in its field of operation. In general, these crimes are most effectively detected by the special tools of the empowered national security services.

The Constitution Protection Office is responsible for obtaining information on various criminal acts, such as the misuse of classified information, violation of international economic restrictions, incitement against a community, scaremongering and threatening with public danger.

The Constitution Protection Office shall participate in the detection, prevention and prohibition of the proliferation of internationally controlled products and technologies and military equipment and services, and in the control of their legal trade.

The Constitution Protection Office controls not only natural persons, but also legal entities and associations not having legal personality within the framework of an economic organisation audit. The purpose of the industrial security clearance is to establish whether handling classified information by the economic organisations constitutes a national security threat. In order to establish the existence or absence of the risk, the Constitution Protection Office shall carry out national security vetting on the owners and employees of the economic organisation.

If the check does not establish a risk factor, a facility security clearance is issued for the company concerned, authorising the economic organisation to handle classified information.

The Constitution Protection Office, within the scope of its industrial security screening, shall make the pre-selection and rating related to procurement procedures under the Act on the defence and sensitive security procurements. Furthermore, it may carry out the necessary additional checks regarding its own classified procurements and screen persons seeking permission under the Act on the uniform electronic card issuing framework and it shall perform the related tasks.

In the scope of its duties related to internal security, crime prevention, national security vetting and national security protection of organisations and institutions, the Constitution Protection Office obtains information on and detects corruption, including bribery, active and passive bribery of a public official, abuse of function and corrupt influence.

The Constitution Protection Office performs the internal security and crime prevention checking of organisations – except the national security services – operating under the management and supervision of the Government or members of the Government, in the course of which it may complete integrity tests. The aim of the integrity test is to determine whether the person concerned complies with the obligations deriving from laws, official regulations and collateral in-plant and working agreements. The integrity test is performed by creating an artificial situation that occurs, or is likely to occur, during the conduct of working duties in real life.

The Director General of the Constitution Protection Office can order the integrity test by a resolution that is to be approved or denied by the public prosecutor. The public prosecutor shall be informed without delay about the resolution as well as the accomplishment thereof.

The duration of the test is 15 days that can be prolonged by the Director General for another 15 days. The person concerned should be notified about the end of the test in 15 working days. A disciplinary or misdemeanour procedure shall not be launched based on the result of the test.

Fight against violent right-wing extremism and terrorism falls within the competence of the Counter Terrorism Centre (TEK), a law enforcement organisation authorised to use covert means of intelligence gathering.

It should be emphasised that the territorial competence of the national security services is always related to their basic scope and to their specific tasks defined by law. Consequently, as a general rule, the Information Office performs its tasks abroad, while the Constitution Protection Office performs its duties on the territory of Hungary.

1.4. Oversight and Supervision of National Security Services

The external and independent oversight of the national security services is exercised by two committees of the National Assembly, the National Security Committee and the Committee on National Defence. The latter has legitimacy to supervise the Military National Security Service, whereas the National Security Committee has legitimacy to supervise the civilian and partially the military national security services. The national security services are directed by ministers, respectively, while the directors general of the services are responsible for the operation of the national security services.

The competent ministers regulate the activity and operation of the national security services through decrees and normative instructions. They allocate tasks and give instructions to the national security services to perform their tasks regulated by law. The minister makes proposals for the budget of the national security services and carries out expediency and efficiency control in respect of the budget management thereof.

Among other tasks, the minister investigates complaints about the activities of the national security services and in certain cases acts as a forum for decision-making of second instance regarding the decisions made by national security services (e.g. when the national security service acts as a special authority with advisory power, e.g. in cases of alien administration or in cases of complaints against the security vetting expertise).

The leadership has its boundaries, namely the competent minister may not instruct the national security services regarding the content of their decision when they act as an authority.

The competent minister informs the Committee on National Defence at least once a year regarding the general activity of the Military National Security Service, on government decrees related to the service. The committee interviews the candidate for the position of the Director General of the Military National Security Service prior to his or her appointment and it takes a position on his or her eligibility.

The Committee on National Security has the entire above-described jurisdiction regarding all national security services.

During exercise of the parliamentary control, the Committee may request information about the national security situation of the country and about the operation and activities of national security services from the minister and from the director general of the national security service.

The committee may request information about the procedure of secret information gathering authorisation from the Minister of Justice, from the directors general of national security services and from the minister in charge of direction of civilian national security services.

The Committee may investigate complaints against the unlawful activities of national security services if the complainant does not accept the result of the investigation conducted by the competent minister. If the Committee assumes that an activity of a national security service is illegal or improper, it may call upon the competent minister to conduct an investigation.

If the Committee holds that an operation of a national security service is against the law, and finds it reasonable, it may carry out a fact-finding investigation, as part of which it may inspect documents relevant to the case and may hear the staff members of national security services.

If the Committee identifies, in any way, an illegal or improper activity of a national security service, may invite the minister to take the necessary measures and may initiate the examination of responsibility: the minister shall inform the Committee of the result of this examination.

The Committee gives its opinion on the detailed draft of the budget of the national security services and makes proposals to the National Assembly regarding the adoption of legislative proposals in the course of their discussion.

The Committee is also entitled to have an insight into the information reports by national security services, with the exception of those related to individual cases.

1.5. The Legal Status of the Personnel of National Security Services

The legal status of the personnel of national security services is divided into two categories. The personnel consist of persons in professional service relation, law enforcement administration employees (at the Military National Security, they are called employees of national defence) and workers. The professional personnel and the employees may be seconded or transferred to another organisation of law enforcement or state administration. However, solely the professional personnel of national security services are entitled to accomplish their task covertly by taking up external employment.

The professional personnel of national security services, in accordance with the Act C of 2012 on the Criminal Code, are considered as members of an armed organisation of

the state: therefore, they undergo stricter rules of proceedings and may be prosecuted for military crimes.

This makes a significant difference between the professional personnel of national security services and the other personnel members with a different legal status.

The distinction between the different types of personnel is made first of all by the extent of restrictions of fundamental rights concerning the personnel. No regulation prescribes which personnel of a certain employment status should occupy a position, but it is the interest of the service to make a distinction between positions and the applicable employment status taking the restrictions on fundamental rights into consideration.

Restrictions on fundamental rights concerning the professional personnel and the law enforcement and administration employees are obligations, such as the one to notify the superior about the whereabouts when not in service; there is the restriction of freedom of expression, the professional personnel may not become members of the National Assembly, European Parliament members, locally elected representatives and they may not be elected as Mayor. Besides, the members of the professional personnel are obliged to notify their superiors about their travel abroad (the travel might be prohibited or restricted for security interests), they may not establish labour unions or join them, may not join organisations whose activity is against the tasks of the service. Contrary to the above-mentioned, the fundamental rights of workers should not be restricted at all.

In order to prevent crimes falling within the functions of national security services and in order to capture the perpetrator, the members of the professional personnel may apprehend the perpetrator, and for that they may use physical coercion and handcuffs.

The members of the professional personnel of national security services have the right to carry service firearms and are entitled to use firearms.

Apart from the cases of justifiable defence and necessity, the members of the professional personnel may use firearms to prevent attacks on life or attacks seriously endangering physical integrity or the direct threat thereof; to prevent or interrupt crimes against the state, against humanity and against public order.

Firearms can be used also in the case of unauthorised acquisition of data classified as 'Szigorúan titkos!' ('Top Secret'), or an attempt thereof, by violence against a person, as well as to counter attacks against, or directly threatening, the facilities of a national security service.

Because of possible use of firearms by a member of the professional personnel of national security services, the person concerned may submit a complaint to the director general of the national security service. In case of its denial, the complainant may submit an appeal against the decision to the minister. The complainant may take action in an administrative court against the minister's decision.

2. TASKS AND MANDATE

2.1. Investigative Power and Role of National Security Services in Criminal Proceedings

The national security services and as such the Constitution Protection Office are not investigative authorities, thus have no authorisation to conduct investigation.

In case the Constitution Protection Office obtains information during the fulfilment of its task that indicates commission of a criminal offence, which is out of the scope of its main functions, it may not proceed with information collection.

In case the Constitution Protection Office obtains or receives information that serves as the basis for initiating criminal proceedings, it may consider whether or not to report it to the investigating authority having relevant competence and jurisdiction. This is because, provided that the initiation of criminal proceedings or handing over data would jeopardise the performance of its stipulated tasks, the Constitution Protection Office is not obliged to initiate criminal proceedings. The possible data provision may not result in the disclosure of a person cooperating with national security services (data source).

If the Constitution Protection Office has information indicating commission of a criminal offence, with the exception of above-mentioned cases, may hand over the data to the competent investigative authority.

The Constitution Protection Office has the opportunity to hand over the results of secret information gathering requiring external authorisation to the investigative authority. In this respect, it is necessary to examine the date when the Constitution Protection Office received the results of secret information gathering.

If the Constitution Protection Office intends to hand over information, the result of secret information gathering requiring external authorisation that are not related to crimes stipulated by the Act CXXV of 1995 on the National Security Services to the investigative authority, the Constitution Protection Office has 30 days from the receipt of the result to initiate criminal proceedings.

The national security services have a year (1 year) to initiate criminal proceedings if the result of secret information gathering requiring external authorisation are related to crimes stipulated by the Act CXXV of 1995 on the National Security Services and if the earlier initiation of criminal proceedings would endanger the successful performance of their task prescribed by law.

The Constitution Protection Office has no foreign intelligence responsibilities.

2.2. Analytical Tasks

The Constitution Protection Office has no task of analysing the entire sphere of national security. Obviously, its own ongoing procedures are monitored by the field of analysis and assessment within the Office.

2.3. Administrative Tasks

The Constitution Protection Office also acts as a body providing formal opinion, as well as an administrative authority with advisory power in the procedures of naturalisation and of visas. The Constitution Protection Office acts as an administrative authority in performing the task of civil aviation security. The Office takes part in procedures for approving the appointment and revocation of in-flight Security Officers and Chief Security Officers, also in procedures for approving the appointment and revocation of security instructors, in procedures for the allowance of prohibited articles and in the procedure for designating the civil aviation authority as a small airport in perspective of civil aviation security.

2.4. Tasks of Cybersecurity

The Constitution Protection Office performs IT and facility protection in the field of cybersecurity. In this respect, it strives to cooperate with the relevant representatives of the sector, collects information and conducts risk assessment regarding new technologies. In addition, it screens persons and organisations of risk concern that would pose a national security threat to the operation of IT systems and of priority investments in perspective of the government info-communication and it continuously monitors cyberevents.

2.5. Protection of Classified Information

The Constitution Protection Office has no tasks of an administrative authority regarding the protection of classified information. However, in the case of misuse of classified information, it is the Office's task to obtain the possibly emerged information. The Constitution Protection Office, as an organisation processing data, observes the regulations regarding the protection of classified information in performing its tasks.

2.6. International Cooperation

The minister in charge of direction of civilian national security services has the power to maintain contacts in order to facilitate international cooperation between national security services. In parallel, the competent minister is the one who approves the proposals on the international relations of the national security services on the motion of the Directors General. The Constitution Protection Office may conduct cooperation exclusively with its international partner services, not with individuals or companies, or international organisations.

2.7. Protection of Personal Data

The procession and protection of personal data is regulated by the provisions of the General Data Protection Regulation. In compliance with the Act CXII of 2011 on the right to informational self-determination and on freedom of information, personal data may be processed for law enforcement and for national security purposes. Data processing for

national security purposes means processing data by the national security services, within their functions and powers laid down by law. Consequently, the regulations on the processing of personal data are laid down in the Act CXII of 2011 on the right to informational self-determination and on freedom of information and in the Act CXXV of 1995 on National Security Services. In case the national security service obtains and processes data that are not necessary for completing its tasks, the provisions of the General Data Protection Regulation are normative. National security services may process all types of data related to their scope of activity.

As set forth in the Act CXII of 2011, the national security services are entitled to handle all types of data provided that the data fall within their scope. The national security service can handle the personal data until it is necessary for the performance of its tasks. The timeframe might be from 10 up to 70 years.

The Act on the National Security Services defines that the national security services can use the data that they become aware of strictly for the purpose that has served as legal grounds for collecting of those data, unless the data indicate that the statutory elements of a criminal offence have been fulfilled and their transmission is permitted by the Act or establishes an obligation to provide the information to another national security service if the recipient himself or herself is also entitled to receive the data.

Upon international commitment, the national security services are entitled to transmit personal data to a foreign entity empowered with data procession, under the framework of the pertinent legal regulations on the protection of personal data.

CHAPTER XI

Italy

Claudio Gentili

1. POSITION OF THE SERVICE IN THE DOMESTIC LEGAL SYSTEM

The *Agenzia Informazioni e Sicurezza Interna* (Internal Intelligence and Security Agency – the AISI) is a state administrative entity under the direction and general responsibility of the President of the Council of Ministers.

The juridical system specifically provides for and regulates the AISI's structure, functioning and organisation as part of the *Sistema di Informazione per la Sicurezza della Repubblica* (Intelligence System for the Security of the Republic – the SISR), both through primary and secondary law.

In accordance with the provisions of the reform Law No. 124/2007, the SISR consists of the President of the Council of Ministers (PCM), the *Comitato Interministeriale per la Sicurezza della Repubblica* (Interministerial Committee for the Security of the Republic – the CISR), the *Dipartimento delle Informazioni per la Sicurezza* (Security Intelligence Department – the DIS), the *Agenzia Informazioni e Sicurezza Esterna* (External Intelligence and Security Agency – the AISE) and the *Agenzia Informazioni e Sicurezza Interna* (Internal Intelligence and Security Agency – the AISI).

Law No. 124/2007 specifically regulates the functions and powers conferred upon each of the Internal (AISI) and External (AISE) Agencies.

1.1. Legal Definition of Special Services

Article 7 of Law No. 124/2007 establishes the *Agenzia Informazioni e Sicurezza Interna* (Internal Intelligence and Security Agency – the AISI) and defines its tasks. The Agency is responsible for gathering and processing all information falling within the areas of its competence that serves to defend the internal security of the Italian Republic and its underlying democratic institutions as established by the Constitution (including in implementation of international agreements) from every threat, subversive activity and form

of criminal or terrorist attack. The AISI's organisation and functioning are governed by a specific regulation.

The AISI is responsible for the security intelligence activities that are carried out within the national territory in order to protect Italy's political, military, economic, scientific and industrial interests. The AISI is also responsible for identifying and countering within the national territory those espionage activities that are directed against Italy and those activities that are aimed at damaging national interests.

The AISI may carry out operations abroad only in collaboration with the AISE, where such operations are closely linked to activities that the AISI is itself conducting within the national territory. To this end, the DIS' Director General makes provision for ensuring the necessary forms of coordination and informational linkage, including for the purposes of avoiding functional and territorial overlapping.

The AISI is directly answerable to the President of the Council of Ministers and keeps the Minister of Defence, the Minister of Foreign Affairs and the Minister of the Interior promptly and constantly informed about the profiles of their respective competence.

After prior consultation with the CISR and by way of a decree, the President of the Council of Ministers appoints and dismisses the AISI's Director, who is chosen among the state's administrative entities' top-echelon officials or equivalent, for a maximum term of eight (8) years.

The AISI's Director constantly reports on his or her agency's activities to the President of the Council of Ministers (or to the Delegated Authority, where appointed) through the DIS' Director General. He or she reports directly to the President of the Council of Ministers in cases of urgency or when other particular circumstances so require, informing the DIS' Director General of such fact without delay. He or she submits an annual report on the agency's organisation and operation to the CISR, through the DIS' Director General.

The President of the Council of Ministers appoints and dismisses one or more Deputy Directors, after consulting the AISI's Director, who makes the other appointments within the agency.

The *Agenzia Informazioni e Sicurezza Esterna* (External Intelligence and Security Agency – the AISE), whose organisation and functioning are also governed by a specific regulation, is instead responsible for gathering and processing all intelligence falling within its areas of competence that serves to defend the independence, integrity and security of the Republic (including in the implementation of international agreements) against threats originating abroad (pursuant to Article 6 of Law No. 124/2007).

In particular, the AISE is responsible for intelligence activities that are performed outside the national territory in order to protect Italy's political, military, economic, scientific and industrial interests; identifying and countering outside national territory those espionage activities that are directed against Italy and those activities that are aimed at damaging na-

tional interests; counter-proliferation activities concerning strategic materials (e.g. nuclear material), protection of high technology and *dual use* material.

The AISE is directly answerable to the President of the Council of Ministers and keeps the Minister of Defence, the Minister of Foreign Affairs and the Minister of the Interior promptly and constantly informed about the profiles of their respective competences.

Article 4 of Law No. 124/2007 establishes the *Dipartimento delle informazioni per la sicurezza* (Security Intelligence Department – the DIS) within the Presidency of the Council of Ministers. In particular, the President of the Council of Ministers (PCM) and the Delegated Authority (AD – the Undersecretary to the Presidency of the Council), where appointed, exercise their powers through the DIS, for the purposes of ensuring a fully unified approach[1] in the planning of intelligence collection as well as in the AISE's and the AISI's analyses and operational activities.

According to the same law, the DIS is also responsible for coordinating intelligence activities for the protection of the country's critical and cyber space infrastructure, in which the government is actively engaged both on the prevention side and on the side of the response to potential hostile acts.

In short, as for its tasks and functions, the DIS coordinates all security intelligence activities, including those related to cybersecurity, and reviews the results of the activities carried out; it keeps itself constantly informed about the operations of the AISE and the AISI and passes the reports and analyses produced by the Security Intelligence System on to the President of the Council of Ministers; it gathers the information, analyses and reports drafted by the AISE and the AISI, from other state administrative entities and from research organisations, including private ones; without prejudice to the exclusive competence of the AISE and the AISI to draw up their own respective operational intelligence collection plans, it draws up strategic or other specific analyses to be submitted to the CISR or the individual ministers it consists of. The DIS also makes assessments and forecasts based on the sectoral analytical contributions made by the AISE and the AISI; it promotes and ensures the exchange of information between the intelligence services and police forces; it oversees the activities of the AISE and the AISI through the Central Inspection Office; it ensures the correct application of the provisions issued by the President of the Council of Ministers governing the administrative protection of state secrets and classified documents; it issues guidelines for the unified management of the DIS', the AISE's and the AISI's staff; it manages the common procurement and logistics services of the DIS, the AISE and the AISI; in agreement with the AISE and the AISI, it draws up a

[1] With the adoption of Law No. 133/2012 by the Houses of Parliament, initiated by COPASIR and unanimously approved, the DIS' coordination role has been further strengthened, especially with regard to intelligence strategic analysis and unified management of human and material resources available to the security intelligence services. The DIS has been especially entrusted with the responsibility for these functions.

plan for the acquisition of human and material resources and every other kind of resource instrumental to the security intelligence services' activities, to be submitted for approval by the President of the Council of Ministers; it sees to institutional communications and the activities promoting security awareness.

Moreover, the DIS consists of several offices, including: the *Ufficio centrale per la segretezza* (UCSe – the Central Secrecy Office), responsible for the administrative protection of State secrets, including the issue or suspension of the security clearance; the *Ufficio Centrale degli Archivi* (UCA – the Central Archives Office), responsible for coordinating, regulating and overseeing the management of the data owned by the intelligence services; the *Ufficio Centrale Ispettivo* (UCI – the Central Inspection Office), responsible for overseeing the AISE and the AISI, checking that their activities comply with acts and regulations, as well as with the directives and provisions issued by the President of the Council of Ministers; the *Scuola di Formazione* (Instruction School), responsible for providing training, refresher courses, specialised and technical-operational continuing education to staff working in the DIS and in the agencies. The School is also engaged in promoting and disseminating security awareness and it cooperates with similar entities from Public Administration, Universities and study centres both in Italy and abroad.

As for the exclusive nature of the functions attributed to intelligence bodies, it should be pointed out that Article 8 of Law No. 124/2007 states that 'The functions attributed under this Act to the DIS, the AISE and the AISI may not be carried out by any other agency, body or office'.

1.2. Position and Role of the Services in the Public Administration System

As mentioned above, the Republic's security intelligence services are state administrative bodies within the Intelligence System for the Security of the Republic set out in Article 2 of Law No. 124/2007 and consisting of the President of the Council of Ministers (PCM), the *Comitato Interministeriale per la Sicurezza della Repubblica* (Interministerial Committee for the Security of the Republic – the CISR), the *Autorità Delegata* (Delegated Authority, Undersecretary to the Presidency of the Council), where appointed, the DIS and the two agencies, the AISE and the AISI. It therefore consists of all bodies and authorities responsible for ensuring 'intelligence activities' aimed at defending the Republic against dangers and threats originating both inside and outside the country.

1.3. Scope of Activities of the Services

Following reform Law No. 124/2007, a decision was made to divide the competences of the two Agencies – the External Intelligence and Security Agency (AISE) and the Internal Intelligence and Security Agency (AISI) – on a territorial basis depending on the origin

of the threat: an external threat for the AISE, pursuant to Article 6, and an internal threat for the AISI, pursuant to Article 7.

Based on the division of competences, specifically the AISE is responsible for gathering and processing all intelligence falling within its areas of competence that serves to defend the independence, integrity and security of the Republic against threats solely originating abroad; conducting counter-proliferation activities concerning strategic materials as well as the security intelligence activities that are performed outside the national territory in order to protect Italy's political, military, economic, scientific and industrial interests; identifying and countering, outside national territory, those espionage activities that are directed against Italy and those activities that are aimed at damaging national interests; the AISE may carry out operations within the national territory only in collaboration with the AISI, where such operations are closely linked to activities that the AISE itself carries out abroad.

The AISI, on the other hand, is responsible for gathering and processing all information falling within the areas of its competence that serves to defend the internal security of the Republic and its underlying democratic institutions as established by the Constitution from every threat, subversive activity and form of criminal or terrorist attack; conducting security intelligence activities that are carried out solely within the national territory in order to protect Italy's political, military, economic, scientific and industrial interests; the AISI may carry out operations abroad only in collaboration with the AISE, where such operations are closely linked to activities that the AISI is itself conducting within the national territory; it is responsible for identifying and countering, within the national territory, those espionage activities that are directed against Italy and those activities that are aimed at damaging national interests.

1.4. Control and Supervision over the Services

The activities of the Intelligence Security System are subject to several checks by 'control bodies' for ensuring that its actions comply with the Constitution and laws in the sole interest of and for protecting the Italian Republic and its institutions.

In particular, one type of control is the parliamentary oversight by the Parliamentary Committee for the Security of the Republic (COPASIR).

Chapter IV of Law No. 124/2007, Articles 30–38, as well as the COPASIR's internal Regulation approved at the sitting of 22 November 2007, specifically cover this parliamentary oversight function.

The committee is bicameral. It consists of five deputies and five senators who are to be appointed by the Presidents of the two Houses of Parliament within 20 days of the opening of every parliamentary term. The said Committee's composition shall reflect the number of members in the parliamentary groups, whilst ensuring the equal representation of both

the majority and the opposition groups and taking the specific nature of the Committee's tasks into account.

The Committee's Bureau consists of a chairperson, a deputy chairperson and a secretary. The Bureau is elected by the Committee members by way of a secret ballot. The chairperson is elected from amongst the members belonging to the opposition groups.

For the exercise of its functions the Committee has access to extensive information. Firstly, the Committee can hear several entities possessing information and competences of interest. In addition to the hearing of the President of the Council of Ministers, the Minister or Undersecretary for Coordination of intelligence security services, the Ministers forming the Interministerial Committee for the Security of the Republic (CISR), the DIS', AISE's and AISI's directors, the Committee also has the right, in exceptional cases, to provide for the hearing of persons employed by the Security Intelligence System, without prejudice to the President of the Council of Ministers' right to oppose the holding of the hearing, stating the reasons for it. The Committee also has the power to hear any other person, not belonging to the Security Intelligence System that is able to provide information or assessments.

Another way of acquiring information needed for performing parliamentary oversight is Committee's power (including in derogation from the prohibition under Article 329 of the Code of Criminal Procedure) to obtain copies of records or documents relating to proceedings or inquiries being conducted by a judicial authority or some other investigative body, as well as copies of records or documents relating to parliamentary investigations or inquiries, and information of interest to it from the Security Intelligence System or public administrative bodies.

A special procedure also involving the President of the Council of Ministers is provided for, should the communication of a piece of information or the transmission of a requested document risk prejudicing specific security needs. When the Committee, by unanimous vote, has called for investigations as to whether the behaviour of the security intelligence services' members corresponds to the institutional duties provided for in the establishing law, neither state secret status nor the need for confidentiality can be invoked.

The Committee also has the power to access and carry out on-the-spot checks in the offices falling within the Security Intelligence System's competence upon communication of such actions to the President of the Council of Ministers. The Committee is also responsible for auditing directly the expenses documentation for completed operations.

Significant advisory powers are also conferred on the Committee. In particular, the Committee is due to give its mandatory non-binding opinion on all draft decrees and regulations referred to in the reform law, as well as any other draft decree or regulation concerning the organisation and status of the intelligence security bodies' personnel.

The Committee and its President receive several mandatory periodic reports from the Government and intelligence bodies. In this context, the President of the Council of Min-

isters is officially obliged to inform the President of the Committee about the appointments of the directors and deputy directors of the DIS, the AISE and the AISI in advance.

In addition to an annual report, the Committee can submit urgent reports and information to the Houses of Parliament.

Finally, the Committee also enjoys significant powers related to confirmation of the invocation of state secret status by the President of the Council of Ministers. Article 40(5) and Article 41(9) establish that the President of the Council of Ministers is bound to communicate to the Parliamentary committee for the security of the Republic every case where an invocation of state secret status is confirmed and to give the essential reasons for such confirmation. If the Committee considers the invocation of state secret status to be groundless, it reports the matter to both Houses of Parliament for their subsequent assessment.

In addition to parliamentary oversight, a specific office within the DIS is responsible for internal control. Through its *Ufficio Centrale Ispettivo* (Central Inspection Office – the UCI), the DIS oversees the activity of the AISE and the AISI, checking that their activities comply with acts and regulations, as well as with the directives and provisions issued by the President of the Council of Ministers.

1.5. Legal Status of the Officers/Employees

The status of security intelligence services staff is accurately regulated both by primary and secondary law.

Article 21 of Law No. 124/2007 is specially dedicated to the specific personnel group employed by the DIS and the security intelligence services, established within the Presidency of the Council of Ministers and to be provided for by way of a specific regulation.

The same regulation, in derogation from the legal provisions in force but in observance of the criteria established by the a.m. law, also governs the personnel's organisation and recruitment (guaranteeing its unified management), the related pay and pensions, as well as conditions of disclosure of the regulation itself.

The regulation also defines the all-inclusive remuneration for personnel employed by the DIS, the AISE and the AISI within the limitations of the financial resources provided for under the legislation in force. Such remuneration comprises basic salary, special supplementary allowance, family allowance and a functional allowance, to be attributed according to rank, qualification and profile held as well as to the functions performed.

Any form of additional pay other than those provided for by the regulation is forbidden. Should a member of the personnel return to his or her administrative entity of origin or be transferred to another public administrative entity, he or she will not maintain the main and additional pay due during employment with the security intelligence services.

The regulation governs the cases where either permanent or temporary employment is terminated and it establishes the conditions of ineligibility precluding an employment

relationship with the DIS or with the security intelligence services based on certain personal conditions, posts held or activities performed, providing for specific disclosure duties and, where these are breached, the consequential sanctions.

Persons whose scrupulous loyalty to the Constitution cannot be fully relied upon on account of subversive behaviour or actions towards democratic institutions, cannot carry out any form of activity under the Security Intelligence System's employment.

In no case shall the DIS or the security intelligence services have the power (even occasionally) to employ the following persons directly or recruit them in a freelance or consultancy capacity: members of the European Parliament, the national Parliament or government; regional, provincial or municipal councillors or members of their respective executives; employees working within constitutional bodies, members of the judiciary, religious ministers and employed or freelance journalists.

All staff who work for DIS or the security intelligence services in any capacity are bound to preserve the secrecy of everything that has come to their knowledge in the exercise of or on account of their duties, even after the termination of such activity.

The security intelligence services consist of both staff with a military and a civilian background. Finally, Security Intelligence Services employees can perform either operational or administrative-logistical activities and are integrated into three macro-areas: managers, officials and assistants.

2. TASKS AND MANDATE

2.1. Investigative Powers and the Role in Criminal Procedure

Law No. 124 of 3 August 2007 has kept the separation between intelligence and law enforcement functions. Under Section 23, the personnel employed by DIS and the Security Intelligence Services within the specific personnel group shall not have the status of judicial police officers or agents, nor of public security officers or agents, except for some cases in which this status is temporarily granted. As a matter of fact, subsections 23(2), (3), (4) and (5) of Law No. 124/2007 stipulate that the President of the Council of Ministers may accord the status of public security officer or agent to a member of the DIS or the Intelligence Services following a specific preliminary procedure and based on a request made by the Director General of the Security Intelligence Department (DIS), after assessing operational requirements and carefully analysing the prerequisites. The status is accorded in two cases: for a specific operation or for activities aimed at protecting the premises and the personnel of the Security Intelligence Services and the DIS. In addition, there must be a necessary functional connection between the duties associated with the status of public security officer or agent and the operations or activities to be conducted. The parameter to assess this connection is defined in Section 23(2) as 'preventive policing duties'.

The people having such status in their administrative entity of origin shall have it suspended during the period of their employment within the a.m. specific personnel group.

As mentioned above, the strict separation of functions *ratione personae* is aimed at setting the boundaries between security-related intelligence activities and criminal investigations in those fields, where the overlapping of scope may easily occur. It is worth noting that Law No. 124/2007 has not directly addressed the issue of using the information obtained by the Intelligence Services during their activities as evidence in criminal proceedings. The matter is deferred to the dichotomous interpretation of the legal doctrine.

As a consequence, one might wonder which law applies if an intelligence officer becomes aware of alleged crimes. One of the main corollaries of the security intelligence officers being precluded from the status of judicial police officer or agent is that they are not subject to the judiciary's oversight and are not obliged to report crimes to it. In this regard, Subsections 23(6), (7) and (8) of Law No. 124/2007 apply, which – in derogation from the provisions provided for under Article 331 of the Code of Criminal Procedure[2] – lay out specific rules that the personnel of the intelligence services and the DIS must respect, should they become aware of a crime while performing their functions.

Therefore, Italian intelligence personnel have the duty to report facts constituting a criminal offence to their respective directors. Therefore, the peculiar aspect of this provision is not the content of their reporting but rather the relevant recipient: intelligence officers have to report the offences to the director of their service who, in turn, will inform the President of the Council of Ministers without delay. The Directors of the intelligence services and the Director General of the DIS also have the duty to transmit to the relevant judicial police bodies the information and evidence related to those facts which may constitute a criminal offence and that have come to their knowledge within the structures they are responsible for.

However, the fulfilment of this duty may be delayed, with prior authorisation of the President of the Council of Ministers (or the Delegated Authority, if appointed) pursuant to Subsection 23(8).

Separately, it is worth noting that the information exchange with the law enforcement authorities is promoted and ensured by the DIS that also promotes, among other things, periodic meetings.

The DIS, besides being the collector of the information gathered nationally, is also the privileged counterpart of the Anti-Terrorism Strategic Analysis Committee which has to provide every kind of cooperation to the Intelligence System for the Security of the Republic in the performance of the tasks it is entrusted with.

Furthermore, Armed and Police Forces have many obligations towards intelligence officers. Section 12(1) establishes that the Armed Forces, the Police Forces and the officers

[2] Duty of public officials and public servants to report crimes.

and agents working in the Judicial Police and law enforcement shall, within their respective fields of competence, offer the staff working in the security intelligence services every possible form of cooperation – including technical and operational cooperation – in the performance of their duties. As to this aspect, the provision refers to 'every possible form of cooperation', hence any kind of support or assistance envisaged by the law, including 'technical and operational one'.

An additional cooperation tool is provided for by Law No. 155/2005 (concerning urgent measures to counter international terrorism). Article 2 establishes that a residence permit may be issued to a non-EU national for investigative purposes, at the request, among others, of the 'Directors of the Security and Intelligence Services'. It is worth noting that this is a rewarding measure, because it is not conditional on the existence of a danger for the beneficiary, and therefore it is not related to the measures envisaged for collaborators of justice nor to the legislation concerning residence permits for humanitarian reasons. The requirement that must be met to be granted the a.m. residence permit is the need to guarantee the stay in Italy of the foreigner who cooperated in police operations, investigations (including those conducted by the intelligence services) or proceedings connected with terrorism-related offences, also international terrorism, or subversive actions against the democratic order. Obviously, the type of permit which will be issued strictly depends on the importance of the foreigner's cooperation. The residence permit is issued to a foreigner whose cooperation is inherently trustworthy, substantially new or complete and is considerably important for the investigations or the judgement.

2.2. Intelligence Gathering

In Italy, Law No. 124/2007 establishes that the Security Intelligence Department (DIS) and the two intelligence services – the AISI and the AISE – are tasked with gathering, retaining and transmitting to the relevant entities, be they public or private, the information pertaining to the protection of the security of institutions, citizens and businesses.

As to its function, intelligence gathering can be defined as a three-phase cycle aimed at fulfilling the general objectives set by government authorities. The first phase consists in acquiring information, through the search, collection and evaluation of data from a wide array of sources, ranging from a single individual to the use of sophisticated electronic equipment. At this stage, open sources – such as mass media and the internet – are particularly important.

The second phase of information processing is the distinctive trademark of the pure intelligence activity, through which raw data are analysed and transformed into finished intelligence.

Finally, the third phase is the dissemination of relevant information, reports, analyses and situational overviews to government authorities, as a support for the decisions or ac-

tions to be taken. Since the concept of national security has become broader, intelligence products are now disseminated also to public administrations and bodies.

2.3. Analytical Tasks

The AISI has the remit to carry out security intelligence activities on the national territory in order to protect Italy's political, military, economic, scientific and industrial interests. The AISI is also responsible for identifying and countering within the national territory those espionage activities that are directed against Italy and those activities that are aimed at damaging national interests. In this context, the AISI is in charge of gathering and processing all information falling within the areas of its competence that serves to defend the internal security of the Republic and its underlying democratic institutions as established by the Constitution (including in implementation of international agreements) from every threat, subversive activity and form of a criminal or terrorist attack. To this end, the various departments within the AISI have ad hoc analysis divisions.

2.4. Administrative Tasks

In order to carry out its administrative and logistic functions, the AISI relies on a dedicated office. To fulfil specific needs, the agency is allowed to interact with all public administrative entities and bodies providing public utilities, which operate under an authorisation, concession or agreement, and request their logistical and administrative cooperation. To this end, the Agency can draw up agreements with the said parties, as well as with universities and research organisations (pursuant to Section 13 of Law No. 124/2007. *Cooperation Requested of Public Administrative Entities and Public Utility Providers*).

2.5. ICT Security

The AISI is not tasked with the protection of Italy's ICT. Decree Law No. 82 of 14 June 2021 redefined Italian cyber architecture and set up the National Cybersecurity Agency (ACN) to protect Italian cybersecurity interests.

The ACN is today the national authority responsible for cybersecurity and is entrusted with the following tasks: ensuring the coordination between public entities involved in the cyber domain; promoting common actions to guarantee the necessary cybersecurity and resilience for Italy's digital development; pursuing national and European digital strategic autonomy, in synergy with the national production system and through the involvement of academia and research centres; fostering specific training courses to enhance workforce's skills employed in this sector and supporting awareness-raising campaigns and a widespread cybersecurity culture; ensuring the implementation of the national cybersecurity strategy adopted by the President of the Council of Ministers, by also encouraging the implementation of a consistent regulatory framework; conducting inspections and imposing sanctions;

developing cooperation relations with similar agencies abroad, besides ensuring the coordination between public entities and developing public-private synergies aimed at ensuring cybersecurity and resilience for the digital development of the country.

2.6. Protection of Classified Information

The oft-mentioned Law No. 124/2007 sets the rules on state secrets and regulates its application, invocation and confirmation as well as the circumstances under which it is forbidden to resort to this instrument. The same law provides for the use of a specific four-level secrecy classification system to protect information and restrict access on a strict need-to-know basis. The four levels are: top secret, secret, confidential and restricted.

For the administrative protection of State secrets and secrecy classifications the *Ufficio centrale per la segretezza* (UCSe – the Central Secrecy Office) is established within the DIS (not the AISI). The President of the Council acts as the National security authority through the UCSe. In this context, UCSe is responsible for issuing security clearances.

In Italy, the national security authority is responsible for the administrative protection of national classified information and information classified as State secrets. The national security authority is the President of the Council of Ministers, who performs his or her duties as such through the Central Secrecy Office (UCSe) established within the DIS.

The Central Secrecy Office (UCSe) performs executive, advisory, coordination and oversight tasks relating to the administrative protection of State secrets and secrecy classifications.

Secrecy classifications indicate the secrecy level assigned to a specific piece of information at the national level. Classified documents are all types of records – be it tangible or intangible, analogue or digital – containing classified information and, therefore, subject to physical, logical and technical protection from the time of their origin until they are destroyed or declassified.

During such lifetime, the handling and management of such records are specifically regulated. Single parts of a document may require different classifications.

There are four classifications provided for in Article 42 of Law No. 124/2007 – *segretissimo* (SS – top secret), *segreto* (S – secret), *riservatissimo* (RR – confidential) and *riservato* (R – restricted) – and they are assigned by the originator of the information depending on the severity of the damage its non-authorised disclosure would cause to the state's security.

With regards to their impact, classifications limit access to a certain piece of information solely to those individuals who need to know about it to perform their tasks, are aware of the rules to handle and store it correctly and hold suitable clearance, except for the classification 'restricted'; classifications also imply a system of measures – set by the DIS' Central Secrecy Office (UCSe) – to make sure that the access restriction is actually in place.

Each classification level entails, indeed, a set of provisions to ensure its protection (storage and reproduction systems etc.).

These provisions are proportionate to the relevance of the protected interest, therefore, the more incisive, the higher the level, from restricted to top secret. They do not prevent the judicial authority from obtaining knowledge of the information.

However, if, in performing their institutional functions, judicial authorities acquire classified documents, they are obliged to see that they are kept in a manner that protects their confidentiality whilst guaranteeing the right of the parties to the proceedings to view them. In specific cases, documents can be subject to declassification, meaning a downgrade of the classification to a lower level or the complete lifting of secrecy classification.

Finally, it is important to point out that Law No. 124/2007 introduced a mechanism according to which the secrecy classification is automatically downgraded to the lower level – e.g. from *riservatissimo* (confidential) to *riservato* (restricted) – upon the expiry of five (5) years from the date of its original application. Once a further five-year period has expired, all classification restrictions shall be lifted. These automatic mechanisms do not apply when, by way of a measure stating reasons, the restriction's duration is extended by the entity who effected the original classification or, in cases of extension beyond a term of 15 years, by the President of the Council of Ministers.

2.7. Personal Data Protection

With regards to the processing of personal data by our services, the national legislature provided for the AISI's processing of personal data in a special regulation, with the intention to balance the personal right to confidentiality and the essential need to protect the security of the Republic and its underlying democratic institutions.

In this spirit, the Privacy Code referred to in Legislative Decree No. 196/2003 (laying down provisions for the transposition of EU Regulation No. 2016/679 into domestic law) provides that processing of personal data by our Services shall be regulated by the provisions included in Article 160(4) of the a.m. Code, as well as, *mutatis mutandis*, by Articles 2, 3, 8, 15, 16, 18, 25, 37, 41, 42 and 43 of Legislative Decree No. 51 of 18 May (regulating data processing for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, implementing EU Directive 2016/680, the so-called law enforcement directive).

In accordance with the key role conferred by Law No. 124/2007 on the President of the Council of Ministers – who is responsible for the political orientation and organisation of the Intelligence System for the Security of the Republic – Article 58(4) of the Privacy Code deferred to a regulation (the Prime Minister's decree) the definition of the rules for the implementation of provisions applicable to *intelligence*, considering the different types

of data, individuals, possible processing operations and people in charge, also in relation to their update and retention.

Finally, with regard to data retention, please be informed that Italy did not have to make any changes or normative adjustments following the successive rulings of the Court of Justice of the European Union in cases on data protection. According to Article 132 of Legislative Decree No. 196/2003 (the Privacy Code) the time limits for storage and availability of data remain 24 months for telephone traffic, 12 months for telematic traffic (and 30 days for missed calls).

Furthermore, Article 24 of Law No. 167 of 20 November 2017 for the transposition into domestic law of Directive 2017/541 on combating terrorism provides that 'for the purposes of detection and repression of offences referred to in Article 51, para. 3-quarter, and Article 407, para. 2, point a), of the code of criminal procedure, the time limit for storage of data on telephone and telematic traffic, as well as data concerning missed calls, is set at seventy-two months (6 years).'

Regulations on data storage requires telecommunications operators to store telephone and telematic traffic metadata (not conversations) for 6 months.

CHAPTER XII

Latvia

Egils Zviedris

1. POSITION OF THE SERVICE IN THE DOMESTIC LEGAL SYSTEM

1.1. The Position and Role of Services in the Public Administration System

The Constitution Protection Bureau (*Satversmes aizsardzības birojs*, SAB) is a state security institution supervised by the Cabinet of Ministers. The SAB, the State Security Service (*Valsts drošības dienests*, VDD) and the Defence Intelligence and Security Service (*Militārās izIūkošanas un drošības dienests*, MIDD) are the three state security institutions of Latvia, all of them are equal but have different competences and capacities. The SAB was formed in 1995 according to the Law on the Constitution Protection Bureau.

The head of the Constitution Protection Bureau is the director. Candidates for the director's post are promoted by the National Security Council, but the director is appointed by the Saeima (Parliament). Initially, the term in the office was four (4) years. Now it is extended to five (5) years. The number of such terms in the office for one person is not limited.

The SAB acts in line with the National Security Law, Law on State Security Institutions, the Law on the Constitution Protection Bureau, the Law on Official Secrets, the Operational Activities Law and the associated regulations of the Cabinet of Ministers.

The Centre for the Documentation of the Consequences of Totalitarianism (CDCT)

The CDCT is a unit of the Constitution Protection Bureau since 6 November 1995. The primary functions of the CDCT are stipulated in the Law on the Preservation and Use of Documents of the State Security Committee (KGB) and on Establishment of the Fact of Collaboration with the KGB and include preservation of the received documents of the

KGB of the Latvian SSR, preparation of documents concerning establishment of the fact of collaboration by certain individuals with the KGB of the Latvian SSR for submission of these documents to the specialised multi-branch public prosecutor's office, provision of reference information to public authorities, natural entities and the Latvian security institutions concerning the facts of collaboration with the KGB and collection of documents which ensure the political, legal and moral rehabilitation of individuals who suffered repression, persecution or spying by the KGB.

The State Security Service (VDD)

The State Security Service is the main counterterrorism coordinating body in Latvia that ensures:

- continuous counterterrorism threat monitoring and the coordination of the cooperation of state and local government institutions as well as the cooperation of legal entities in the area of counterterrorism
- counterintelligence and operational activities in order to fight crimes posing threats to state security or to state power
- fight against unauthorised proliferation of nuclear materials, drugs, weapons as well as explosives
- protection of official secrets in line with the Law on Official Secrets
- coordination of activities of state and local government institutions as well as legal entities in the area of counterterrorism and analysis of the national policies implemented in this area
- provision of protection (guarding) of the state officials and representatives of international organisations and institutions indicated by the Cabinet of Ministers.

The Defence Intelligence and Security Service (MIDD)

The primary tasks of the Defence Intelligence and Security Service include:

- protection of official secrets at the Ministry of Defence, its subordinate institutions and National Armed Forces
- military intelligence and counterintelligence in the military area
- security vetting for granting personnel security clearances for access to official secrets for employees of the Ministry of Defence.

1.2. Scope of Activities of the Services

The main tasks of the SAB include intelligence, counterintelligence and protection of official (state) secrets. As the National Security Authority, the SAB also ensures the protection of NATO and EU classified information in public institutions engaged in work with such information.

The SAB is also responsible for:

- obtaining, receipt, compilation, accumulation, storage, analysis and use of the information related to the national security, protection, economic sovereignty and ecological threats in accordance with the procedures laid down in law
- prevision of threats to national security, prevention or neutralisation thereof in conformity with its competence
- development of proposals and programmes in the issues of national security in conformity with its competence
- timely and complete informing the authorities implementing state authority and administration and their responsible officials of threats to national security
- provision of information and materials to the prosecutor's office or the relevant investigating institution on criminal offences and individuals who may be accused of having committed them
- performance or organisation of the performance of certain tasks given by the Cabinet of Ministers in writing within the scope of its competence
- preparation of the Analysis of the National Threat in cooperation with the State Security Service and the Defence Intelligence and Security Service
- cooperation with foreign partner services
- ensuring the operation of the Centre for the Documentation of the Consequences of Totalitarianism (CDCT).

1.3. Legal Status of the Personnel

The personnel of the SAB are officials and employees. An official of the SAB is employed in the service of the SAB. Upon commencement of the performance of the official duties at the SAB, the officials thereof confirm their loyalty to the Republic of Latvia by taking an oath.

A person who meets the following mandatory requirements may be an official or employee of the SAB:

- is a citizen of Latvia
- is at least 18 years of age
- is fluent in Latvian and at least one foreign language
- has obtained higher education
- conforms to the requirements laid down in the Law on Official Secrets in order to receive a special permit to access official secrets
- the state of health and psychological qualities and also physical preparedness are appropriate for the performance of service (work) duties
- has not been sentenced for an intentional criminal offence or for the disclosure of official secrets out of negligence, regardless of the clearing or extinguishing of the criminal record

- has not been convicted of an intentional criminal offence or of disclosure of official secrets out of negligence, released from the sentence or the criminal proceedings initiated against the person have been terminated on the basis of exoneration
- has not been sentenced with the deprivation of the right to hold a specific office in official service by a court judgment or a prosecutor's penal order in a criminal case
- has not been retired (dismissed) from the service of the state security institutions, military or other official service in the last five years upon the application of a disciplinary sanction – retirement from service or dismissal from office
- is not or has not been a permanent or freelance employee of the security service (intelligence or counterintelligence service) of the USSR, Latvian SSR or other foreign state or an agent, resident or keeper of a safe house (any covert organisation of any form thereof)
- has not worked in the CPSU (LCP), the Working People's International Front of the Latvian SSR, the United Council of Labour Collectives, the Organisation of War and Labour Veterans or the All-Latvia Salvation of Society Committee after 13 January 1991
- is not and has not been a member of an organisation prohibited by law or a court ruling.

A person who has not acquired higher education or is not fluent in any foreign language may be recruited into service (work) in a state security institution and employed if such education or the knowledge of a foreign language is not necessary for the performance of the relevant office (work) and the person has acquired at least secondary education. If a person has the specific skills or experience necessary for the service, the head of the SAB may also recruit into service a person who has reached the service pension age specified in the Law on Service Pensions of Officials of State Security Institutions or who will reach this age earlier than within five years, but this does not interfere with the performance of service duties.

A person who applies for service (work) in the SAB has an obligation:

- to present a personal identification document, documents certifying education, an official language proficiency certificate if education has not been obtained in the official language, and a document certifying the skills of a foreign language
- in conformity with the requirements stipulated by the head of the SAB, to submit an opinion on the state of health and also a statement of a narcologist that excessive use of alcohol, use of toxic substances, use of narcotic or psychotropic substances without medical indications has not been determined in relation to the person and a statement of a psychiatrist that the person has not been diagnosed with psychiatric diseases or behavioural disorders have not been determined
- in conformity with the requirements stipulated by the head of the SAB, to undergo professional, physical, and psychological health tests
- not to disclose information which has become known thereto or is available at the SAB due to the application to the service (work).

Upon recruitment into service (work) and appointment to office, a probationary period of up to six months is determined for an official and employee in order to ascertain whether the official or employee is suitable for the performance of duties entrusted thereto. If necessary, the head of the SAB may extend the probationary period for the official. The total probationary period for an official can not exceed nine months. During the probationary period, the head of the SAB may dismiss an official or employee from office (work) and retire him or her from service without indicating the reason and notifying thereof in writing at least three working days in advance.

An official of the SAB is a representative of the state authority and the lawful requirements and orders made or issued by him or her when performing service duties are mandatory for all individuals. Resisting an official of the SAB, endangering the life or health thereof as well as action interfering with the performance of his or her service duties are punishable in accordance with the law. An official of the SAB is issued with a service certificate for the certification of the authority thereof.

Without the consent of the Prosecutor General, an official of the SAB is not to be held criminally liable on the territory of Latvia, is not to be subject to detention (including administrative detention), search, conveyance by force, and also their residential or service premises, personal or service vehicles are not to be subject to search or inspection. The criminal procedural restrictions are not applied to an official of the SAB in cases where he or she is caught committing a criminal offence of which the Prosecutor General and the head of the respective SAB (?) are informed within 24 hours.

An official and employee of the SAB is prohibited from:

- carrying out political activities, organising strikes, demonstrations, pickets and participating therein, establishing trade unions and participating in their operation
- using the service status to decide matters related to the personal interests of the official or employee himself or herself, his or her fiancée or fiancé, spouse, parents, grandparents, children, grandchildren, adopters, adoptees, brothers, sisters, half-brothers and half-sisters of the official or employee as well as the individuals with whom the relevant official or employee lives and with whom the official or employee has a joint (undivided) household.

Taking into account the necessity of the service and safety considerations, the head of the SAB may impose a prohibition on an official or employee to travel to a specific foreign country or to impose other restrictions. Restrictions on commercial activity, obtaining income, combination of offices and performance of work as well as other restrictions and duties in relation to an official of the SAB are determined by the Law on the Prevention of Conflict of Interest in Activities of Public Officials.

An official and employee of the SAB is not allowed to discredit himself or herself, the institution and the state with his or her actions during and outside the performance of service (work) duties.

The general duties of an official and employee of the SAB are:

- to comply with the Constitution of the Republic of Latvia, the norms of international laws binding on the Republic of Latvia and laws and other regulatory enactments
- to fulfil the oath taken in good faith
- conscientiously, in good faith, acting in the interests of the state and the public, to perform the service (work) duties and the lawful orders (writs) of officials of higher institutions
- to comply with the specified principles of the ethics
- to regularly expand his or her knowledge and to improve the professional skills and abilities necessary for the performance of the service (work) duties.

An official and employee of the SAB is held disciplinarily, administratively or criminally liable for illegal or unethical conduct as well as for the violation of the requirements of the service (work) specified in an order (writ) of the head of the SAB and, in conformity with the restrictions and procedures provided in laws and regulations, he or she is materially responsible for the losses (damages) caused.

2. TASKS AND MANDATE

2.1. Investigative powers and the role in criminal procedure

According to Section 19 of Law on State Security Institutions, the officials of a state security institution have the right to:

- within the scope of their competence, request and receive information, documents and other materials from state and local government authorities, economic operators, organisations, officials and other individuals irrespective of the ban of the use thereof. Information, documents and materials are issued in the requested form and free of charge.
- within the scope of their competence, become freely acquainted with all types of state and local government information carriers, including electronically accumulated data, directories, archive materials and other documents, as well as access these, irrespective of the ban of the use thereof. Becoming acquainted with the information carriers and access thereto are ensured in the requested mode and free of charge.
- within the scope of their competence, upon request of the head of a state security institution, become freely acquainted with existing information in the registered data bases, the registration of which has been specified in laws and regulations, irrespective of the belonging thereof, as well as to access such information and to receive it. Becoming

acquainted with such information, access thereto and receipt thereof are ensured in the requested scope, mode and free of charge.

- while performing their service duties and presenting their certificates of an official of the state security institution, freely and without delay access (enter) the non-residential premises and land plot territories belonging to authorities, economic operators, organisations and private individuals, the subdivisions of the National Armed Forces, except for the premises and land plot territory which have exterritorial status.
- if necessary, be exceptionally provided with transport tickets in any type of public transport, but if there are no tickets, to be provided with the possibility to enter and travel by such means of transport.
- in the interests of the service, use the communications and mass information means belonging to the state and local governments, and in exceptional cases – also belonging to private individuals, free of charge. Expenditures for the use of communications and mass information means belonging to private individuals are reimbursed if requested by the owner.
- keep and carry service or personal weapons and special means, use weapons, use physical force and special means in accordance with the Law on the Police.
- within the scope of their competence, receive free of charge the necessary information, documents and other materials on services provided to individuals, including information from the holder of information and technical resources regarding contacts of the individuals, using post, telegraph, telecommunications and other data transmission networks.
- while performing the service duties, verify the personal identification documents.
- acquire, register, process, collect, analyse and store the information necessary for the performance of the functions of the relevant state security institution.
- within the scope of their competence, summon any person to the state security institution in connection with the inspection of information and also with cases and materials, the examination of which is within the competence of the state security institution.
- if signs attesting to the possibility of illegal activity have been detected in actions of a person, give a warning to the person that a violation of the law, which is directed against state security or may harm it, is unacceptable.

In addition to the rights referred to above, an official of the State Security Service has the right to:

- convey individuals by force in accordance with the procedures laid down in law if they do not arrive, without justifiable reason, after being summoned to the state security institution in connection with the examination of cases and materials.

- within the scope of the competence, request individuals to cease violations of the law and other actions that interfere with the execution of the powers of officials of a state security institution and also to use the provided compulsory means of constraint against the offenders.
- in accordance with the procedures laid down in law, detain and hold under guard individuals who are suspected or accused of having committed criminal or administrative offences.
- within the scope of the competence, temporarily restrict or suspend transport or pedestrian traffic on streets and roads as well as the entry or exit of individuals in specific places or facilities if such is required by the interests of state security, public safety, protecting the lives, health and property of individuals, and also the interests of an investigation.

The information obtained in accordance with the procedures laid down above is used only within the framework of intelligence, counterintelligence (including by conducting a personal check for access to official secrets), operational and criminal proceedings.

2.2. Intelligence Gathering

Intelligence activities of the SAB are aimed at acquiring proactive information concerning intentions or actions of foreign governments, institutions, organisations or individuals targeted against the Republic of Latvia or against its vital national interests.

SAB also observes the political, economic and security situation in non-NATO and non-EU countries in order to identify potential risks in a timely manner and the foreign interests in Latvia. After the collection and analysis of such information, the SAB presents it to senior officials of Latvia in order to adopt decisions most acceptable in view of the national interests.

Intelligence activities of the SAB are performed in strict compliance with the effective laws of Latvia, international standards and inter-governmental agreements. Intelligence is only aimed at protecting the interests of Latvia; it is not targeted against the security of other countries.

Counterintelligence

Special services of non-NATO and non-EU countries acting in Latvia are interested in gaining publicly unavailable information regarding the political and economic situation, agendas of senior officials, military activities and technical equipment of Latvia, its scientific potential as well as mass media and their editorial policies. Foreign intelligence officers collect information both from open sources and 'trusted contacts' by taking the respective secrecy measures.

The tasks of the SAB's counterintelligence are the timely identification and control of foreign intelligence activities targeted against Latvia and respective counter-actions.

2.3. Protection of Classified Information

According to Section 2 of Law on Official Secrets, an official secret is military, political, economic, scientific, technical or other information, the loss or illegal disclosure of which may cause harm to the security and economic or political interests of the state.

In Latvia, pursuant to Section 10 of the Law on Official Secrets, the SAB is the only service granting national top secret personal security clearances as well as EU and NATO personal security clearances. In addition, the SAB is also vetting members and personnel of Parliament (Saeima), the Chancellery of the President, the State Chancellery, the Cross-Sectional Coordination Centre, the State Audit Office, the Bank of Latvia, the Ministry of Foreign Affairs, the Office of the Prosecutor General, the Corruption Prevention and Combating Bureau for national cofidential and secret clearances. The MIDD, in turn, is vetting the personnel of the Ministry of Defence and the National Armed Forces for national cofidential and secret clearances, and the VDD is vetting the personnel of all other state institutions for national cofidential and secret clearances.

2.4. Oversight and Supervision of the Services

According to the legislation effective in Latvia, a comprehensive five-level control and supervision mechanism is established for the supervision and control of the SAB's work.

Parliamentary Supervision

The SAB is subject to parliamentary control by the national Security Committee of the Saeima. The SAB has continuously cooperated with this Committee and has provided information regarding any aspect of the SAB's work.

Supervision by the Cabinet of Ministers

The SAB, being an institution of the executive power, is subordinated to the Cabinet of Ministers which ensures supervision via the Ministry of Justice. Every year, the SAB submits a comprehensive annual report to the Cabinet of Ministers and coordinates its primary tasks for the upcoming year. The Cabinet of Ministers is entitled to assign special tasks to the SAB.

Legal Supervision

All the three state security institutions, including the SAB, are subject to a uniform court control mechanism over special-method operational activities. The necessity of such

special-method operational activities is examined by the Chief Justice of the Supreme Court or judges of the Supreme Court accordingly authorised by him or her. Special-method operational activities are only conducted if their necessity is declared justified by a Supreme Court judge who is also required to issue a respective authorisation.

Supervision by the Public Prosecutor's Office

The legitimacy of the activities of the SAB, particularly special-method operational activities, is examined by the Prosecutor General and prosecutors authorised by him or her; they are authorised to examine documents, materials and information possessed or acquired by the SAB. At least once a month, prosecutors from the Prosecutors with the special powers unit of the Public Prosecutor's Office visit the SAB in order to check the correspondence of the phone numbers used in the phone conversation control system with authorisations issued by judges of the Supreme Court.

Financial Supervision

In accordance with the State Audit Office Law, the legitimacy of the implementation of the SAB's financial resources is examined by the State Audit Office, but the legitimacy of the use of the SAB's operational resources is examined by the Auditor General in person.

CHAPTER XIII

Lithuania

Inga Šilinytė, Kristina Vaičiūnė

1. POSITION OF THE VSD IN THE DOMESTIC LEGAL SYSTEM

1.1. Legal Definition of Special Services

There is no definition of 'special services' in the Lithuanian laws, however, it is customary to use the term 'statutory services'.

According to the Law on Civil Service of the Republic of Lithuania, there are three main types of civil servants: career civil servants, state politicians and statutory civil servants. A 'statutory civil servant' means a civil servant whose service is regulated by a special law, which specifies conditions of recruitment to the civil service, fulfilment of the service, remuneration, social guarantees, release/dismissal, liability and other conditions related to specific features of the service. It is stated in the Law on Civil Service of the Republic of Lithuania that it shall not apply to statutory civil servants or to servicemen in the professional military service. There are special laws on different statutory services, such as the Law on Special Investigation Service of the Republic of Lithuania, the Law on Financial Crime Investigation Service of the Republic of Lithuania, the Law on Approval of the Statute of the Internal Service, the Law on Prosecution Service of the Republic of Lithuania etc.

The activities of intelligence services, including the State Security Department of the Republic of Lithuania (hereinafter referred to as 'the VSD'), are regulated under the Intelligence Law of the Republic of Lithuania (hereinafter referred to as 'the Intelligence Law').

1.2. Position and Role of the Services in the Public Administration System

Statutory services in the Lithuanian public administration system can be divided into three groups according to the nature of their functions:

- **Pre-trial investigation institutions**

The pre-trial investigation body is the police. The State Border Guard Service, the Special Investigation Service, the Military Police, the Financial Crimes Investigation Service, the Customs of the Republic of Lithuania, the Fire Protection and Rescue Department are also pre-trial investigation bodies when investigating criminal offences that have come out during the performance of the direct functions of these institutions.

- **Institutions conducting criminal intelligence**

The main institutions of criminal intelligence are as follows: the Financial Crimes Investigation Service under the Ministry of the Interior of the Republic of Lithuania, the Prison Department under the Ministry of Justice of the Republic of Lithuania, the Dignitary Protection Service of the Republic of Lithuania, the Customs Department under the Ministry of Finance of the Republic of Lithuania, the Police Department under the Ministry of the Interior of the Republic of Lithuania, the Special Investigation Service and State Border Guard Service under the Ministry of the Interior of the Republic of Lithuania. The Second Investigation Department under the Ministry of National Defence (hereinafter referred to as 'the AOTD') and the VSD also have the rights and duties of the main institutions of criminal intelligence when their subdivisions conduct criminal intelligence investigations on the grounds and in accordance with the Law on Criminal Intelligence.

- **Intelligence services**

The activities of the intelligence institutions are carried out by the VSD and the AOTD.

1.3. Scope of Activities of the Services

As it is mentioned above, the activities of intelligence institutions in the Republic of Lithuania shall be carried out by the following institutions:

- the VSD – a state institution accountable to the Seimas of the Republic of Lithuania (hereinafter referred to as 'the Seimas') and the President of the Republic of Lithuania
- the AOTD – an institution of the system of national defence subordinate to the Minister of National Defence.

Article 8(2) of the Intelligence Law provides that the VSD shall engage in intelligence and counterintelligence:

- in public political, economic, scientific, technological and information activity areas, with the exception of the areas indicated in Article 8(3)(1)
- in the area of the security of the state diplomatic service of the Republic of Lithuania and other institutions of the Republic of Lithuania operating abroad, with the exception of the institutions indicated in Article 8(3)(2)
- in the areas of the protection of information comprising a state secret and an official secret, with the exception of the institutions indicated in Article 8(3)(3)

- in the area of the installation and operation of electronic communications networks intended for state governance and the cryptographic and other protection thereof.

The AOTD shall engage in intelligence and counterintelligence:

- in defence, military/political, military/economic, military/technological and military/information areas
- in the area of activities of institutions of the national defence system of the Republic of Lithuania abroad
- in the area of protection of information comprising a state secret and an official secret of institutions of the national defence system of the Republic of Lithuania.

Therefore, the VSD is the only civilian intelligence service in Lithuania. As it is mentioned above, military intelligence and counterintelligence are carried out by the AOTD.

The main mission of the VSD is to provide decision-makers in Lithuania with the information that would enable them to make proper decisions concerning future actions in the political and social spheres of the country's life.

The aforementioned role of the VSD is defined by the Intelligence Law which assigns the mission to neutralise threats to national security to our institution, too. It is authorised to take action against threats individually or in cooperation with the law enforcement authorities.

1.4. Control and Supervision of the Services

Most of the above-mentioned statutory services in Lithuania have the status of a body attached to a ministry, which means that the body is subordinate and accountable to the ministry that established it. There are only several exceptions: the Military Police is a subdivision of the Lithuanian Armed Forces, the Dignitary Protection Service of the Republic of Lithuania is accountable to the Government of the Republic of Lithuania, both the Special Investigation Service of the Republic of Lithuania and the VSD are accountable to the President of the Republic of Lithuania and the Seimas.

The Director of the VSD shall be appointed and dismissed by the President of the Republic of Lithuania. The Seimas performs parliamentary control of the activities of the VSD.

The State Defence Council is responsible for coordination of the activities of the intelligence offices and the formulation of intelligence tasks. The Council shall:

- approve intelligence needs and priorities
- approve strategies of the activities of intelligence institutions
- assess the conformity of intelligence information to intelligence needs and priorities
- resolve the issues of the coordination of activities of intelligence institutions

- establish guidelines for international cooperation of intelligence institutions with intelligence and security institutions of foreign states, international organisations and institutions.

The Director of the VSD shall report to the State Defence Council on an annual basis for the activities of the intelligence institution directed by him or her and submit draft strategies of activities of the intelligence institution according to the areas of the activities of the intelligence institution.

The parliamentary scrutiny of intelligence institutions shall be exercised by the Seimas' committee specified by the Statute of the Seimas in accordance with the procedure laid down by the Statute of the Seimas. The Seimas committee shall:

- control the compliance with laws and other legal acts of the Republic of Lithuania by intelligence institutions and intelligence officers in implementing the tasks assigned to them
- consider complaints of persons pertaining to actions of intelligence institutions and intelligence officers
- submit proposals concerning improvement of the legal acts related to activities of intelligence institutions and protection of human rights in the area of intelligence and counterintelligence
- establish shortcomings in activities of intelligence institutions and provide recommendations on elimination thereof.

The Seimas committee shall have the right to obtain and consider:

- intelligence information needs
- reports on the activities of intelligence institutions
- data on intelligence institutions' needs for funds of the budget and use thereof
- oral and written explanations of the heads and officers of intelligence institutions and reports on the implementation of laws and other legal acts of the Republic of Lithuania
- other information on the issues of the activities of intelligence institutions.

The Director of the VSD shall annually submit a report on activities of the VSD in accordance with the procedure laid down by the Statute of the Seimas.

Intelligence officers shall have the right to directly address the Seimas committee regarding the activities carried out by the intelligence institution.

The government shall exercise control over intelligence institutions within the remit established by the Constitution and laws of the Republic of Lithuania. The government shall:

- provide to intelligence institutions, according to the intelligence needs and priorities approved by the State Defence Council, the intelligence information needs required to ensure national security
- obtain from intelligence institutions, in accordance with the procedure laid down by this Law, information on risks, dangers and threats to national security.

On 1 January 2022, the new Law on Intelligence Ombudsmen and amendments to the Intelligence Law entered into force, legalising the position of the Intelligence Ombudsmen and the establishment of the Office of the Intelligence Ombudsmen. Independent external control of intelligence institutions shall be performed by the Intelligence Ombudsmen in accordance with the procedure established by the Law on Intelligence Ombudsmen.

Intelligence Ombudsman – a state official appointed by the Seimas to supervise the legality of the activities of intelligence institutions and to assess compliance with the requirements for the protection of human rights and freedoms. The Seimas appoints two Intelligence Ombudsmen for a 5-year term. The Intelligence Ombudsmen shall carry out investigations:

- on their own initiative, identifying indications that intelligence authorities and/or intelligence officers may be abusing their powers or potentially violating human rights and freedoms or legitimate interests, or potentially violating the processing of personal data processed for national security or defence purposes requirements, or who otherwise potentially violate human rights and freedoms in the field of public administration
- upon receipt of a notification from an intelligence officer
- upon receipt of the applicant's complaint.

Complaints about actions of intelligence officers resulting, when engaged in intelligence and counterintelligence, in violations of human rights or freedoms shall be examined and considered by the Intelligence Ombudsmen in accordance with the procedure laid down by the Law of the Republic of Lithuania on the Intelligence Ombudsmen.

The decisions of the Intelligence Ombudsmen are indicative.

1.5. Legal Status of the Officers/Employees

All statutory services are staffed by officials whose status is regulated by special laws and by employees working under employment contracts covered by the Labour Code.

The personnel of the VSD shall consist of:

- intelligence officers
- employees working under employment contracts. The conditions of work of the VSD's employees shall be established by the Labour Code of the Republic of Lithuania and other legal acts regulating labour relations, unless the Intelligence Law establishes otherwise.

The law obliges the VSD to ensure the protection of intelligence officers and their family members. In fulfilling this obligation, the VSD has the right to acquire and use technical and other means and materials necessary for this purpose as well as to classify and encrypt the identity of intelligence officers.

Prior to assuming office, an intelligence officer shall swear an oath of allegiance to the State of Lithuania.

Prohibitions and restrictions applicable to the intelligence officers:

a) An intelligence officer shall be prohibited from:
   - being a member or sponsor of political parties and political organisations
   - being a member of an organisation which is prohibited in accordance with the procedure prescribed by law
   - participating in the meetings or other public actions of political parties and political organisations expressing political convictions or political demands or directly supporting a political party or a political organisation
   - making political statements, giving speeches, publishing articles expressing disagreement with the policy declared and implemented by a democratically elected state government, publicly raising political demands to the state government
   - being the owner of a private or public legal person, a member of a general partnership or a limited partnership, an appointed (elected) member of management bodies, the founder and stakeholder of a legal person
   - working with private or public legal persons under employment or civil contracts, irrespective of whether this work is remunerated, also receiving other remuneration, excluding cases where the intelligence officer is employed or is remunerated in the interests of the intelligence institution
   - engaging in economic, commercial or self-employment activities
   - receiving income from immovable and movable property, funds, securities, member shares and related transactions, where this is of commercial nature
   - engaging in agricultural activities and forestry
   - representing the interests of other Lithuanian and foreign legal persons
   - going on strike
   - picketing
   - establishing trade unions, being a member thereof and participating in their activities
   - using service hours, property and opportunities provided by service for purposes other than those related to the service
   - accepting gifts or services or offering them, where this can result in a conflict of public and private interests.
b) An intelligence officer may not visit foreign states or territories, which are facing an armed conflict, or other foreign states or territories for purposes other than those related to the

service, where the presence of the intelligence officer therein may threaten the national security or interests of the Republic of Lithuania. The procedure for visiting foreign states by intelligence officers and lists of foreign states or territories, which intelligence officers may not visit, shall be approved by the head of an intelligence institution.

c) An intelligence officer with the approval of the head of an intelligence institution, shall have the right:
   - to engage in creative activities, the results of which are subject to the Law of the Republic of Lithuania on Copyright and Related Rights, also in pedagogical practice
   - to participate in the activities of associations and other non-political alliances.

Guarantees of the activities of intelligence officers:

- Without the consent of the head of an intelligence institution, intelligence officers may not be detained or a subject to a body search or inspection of their personal or official vehicles and premises, with the exception of cases where an intelligence officer is detained in the course of committing a criminal act. In such a case, the institution which detained the intelligence officer must give a notice thereof to the head of the intelligence institution and the Prosecutor General no later than within 12 hours.
- A decision on the institution of criminal proceedings in respect of a criminal act committed by an intelligence officer shall be taken by the Prosecutor General.
- In order to ensure the protection of intelligence officers and their family members, measures may be applied as provided for in the Law of the Republic of Lithuania on the Protection of Participants in Criminal Proceedings and Criminal Intelligence and Officials of Justice and Law Enforcement Institutions Against Criminal Influence.
- The state shall show concern for an intelligence officer and his or her family members who became victims for the reasons related to serving at the intelligence institution and shall provide assistance thereto. The state shall compensate for the damage incurred to the intelligence officer or his or her family member for the reasons related to serving at the intelligence institution. The procedure for compensating for damage shall be laid down by the government.
- An intelligence officer may participate in judicial proceedings only in the capacity of a witness who shall be subject to anonymity or partial anonymity in accordance with the procedure laid down by laws.
- A person who, as an intelligence officer and in the performance of his or her official duties, may have committed an offence due to exceeding the limits of official risk – for which he or she is suspected or accused of having committed a criminal offence, an action has been brought against him or a complaint has been filed against him or her (request, statement) – shall be reimbursed from the funds of the intelligence institution for the costs of legal services or a part thereof. This

compensation shall be granted in accordance with the procedure laid down by the head of the intelligence agency.

2. TASKS AND MANDATE

2.1. Investigative Powers and the Role in Criminal Procedure

The VSD does not conduct law enforcement functions (pre-trial investigation, prosecution).

However, the Code of Administrative Offences of the Republic of Lithuania (CAO) empowers VSD officials to initiate administrative offences proceedings, to conduct investigations into administrative offences and to draw up administrative offence protocols in relation to such administrative offences:

- Failure to comply with a lawful order or requirement of a statutory civil servant, military police, dignitary protection service or intelligence officer.
- Insulting the honour and dignity of a statutory civil servant, military police or intelligence officer by words, gestures, insulting, insolent, provocative behaviour or other conduct.
- Avoidance of former statutory employees of the State Security Committee of the SSSR (NKVD, NKGB, MGB, KGB) and the General Intelligence Board of the General Staff of the Armed Forces to notify the VSD of the existence or becoming owners, partners, shareholders, members or founders of enterprises, institutions, organisations.
- The loss, damage or destruction of classified information, which is an official secret, committed by a person to whom the information has been entrusted in accordance with the procedure laid down by law.
- Unjustified classification of information.
- Violation of the requirements of legal acts regulating the protection of classified information, which has caused or may have caused a threat to the security of classified information.

Furthermore, the VSD conducts criminal intelligence on the grounds and in accordance with the procedure established by the Law on Criminal Intelligence. Criminal intelligence shall mean the activity of entities of criminal intelligence in collecting, recording, evaluating and using available information on objects of criminal intelligence, executed in accordance with the procedure laid down by this Law. Targets of criminal intelligence shall mean the criminal acts being planned, being or having been committed, the persons committing or having committed the criminal acts, active actions of these persons in neutralising criminal intelligence as well as other persons and events related to state national security. The data obtained in the course of conducting criminal intelligence investigation shall not constitute intelligence information. Upon initiation of the criminal intelligence investigation, collection of investigation on a specific natural or legal person shall be terminated immediately.

On the basis of received intelligence information, the VSD may initiate a criminal intelligence investigation when it obtains data on the criminal acts provided for in

Articles 114 (Coup d'Etat), 118 (Assistance to Another State in Carrying Out Activities Hostile to the Republic of Lithuania), 119 (Espionage), 121 (Creation of Anti-constitutional Groups or Organisations and Participation in Activities Thereof), 122 (Public Incitement to Infringe Upon the Sovereignty of the Republic of Lithuania by Using Violence), 124 (Unlawful Possession of the Information Constituting a State Secret), 125 (Disclosure of a State Secret), 126 (Loss of a State Secret), 296 (Seizure or Other Unlawful Acquisition of an Official Secret) and 297 (Disclosure of an Official Secret) of the Criminal Code of the Republic of Lithuania and these data prove insufficient to initiate a pre-trial investigation.

If characteristics of a criminal act are found in the course or upon the completion of a criminal intelligence investigation, the pre-trial investigation shall be immediately commenced. The pre-trial investigation may not be initiated in exceptional cases, where there is a danger to the safety of covert participants of criminal intelligence and/or the lawful interests of the entity of criminal intelligence. The VSD shall notify thereof a prosecutor who will make a decision on further criminal intelligence investigation in accordance with the procedure laid down by the Prosecutor General's Office and having agreed with the main criminal intelligence institutions until the indicated danger is eliminated.

2.2. Intelligence Gathering

The main aim of the activities of intelligence institutions shall be to strengthen the national security of the Republic of Lithuania by collecting information on risks, dangers and threats, providing it to institutions, ensuring national security and eliminating these risks, dangers and threats. Thus, the collection of information is the main function of the VSD, which is directly related to the implementation of the main purpose of the intelligence institutions.

All the activities carried out by the VSD fall under the general definition of intelligence and the information obtained is called intelligence information. For specification purposes, the field of intelligence is classified distinguishing between:

Intelligence – collection, analysis and provision of information concerning external threats to national security.

Counterintelligence – collection, analysis and provision of information concerning internal threats to national security and their neutralisation. A significant part of counterintelligence activities consists of monitoring hostile actions of foreign intelligence and security services in Lithuania and neutralising threats posed by these actions. Counterintelligence also encompasses the protection of classified information. The VSD is the main counterintelligence institution in Lithuania with extensive experience in preventing hostile behaviour of foreign intelligence and security services.

Intelligence information shall be collected in the course of:

- the application of intelligence methods
- the carrying out of actions sanctioned by court

- the obtaining of data from state and departmental registers, information systems and databases
- the obtaining of data from legal and/or natural persons.

2.3. Analytical Tasks

According to the Law on the Basics of National Security of the Republic of Lithuania, the tasks of the VSD shall be, *inter alia*, to study, analyse and forecast public political and economic processes related to threats to national security, to disclose in a timely manner threats to the state security, sovereignty, inviolability and integrity of the territory, the constitutional order, national interests, defence and economic power, to prevent these actions and eliminate them in a procedure established by laws. The VSD shall provide the President, the government and the other state institutions with intelligence and counter-intelligence information, conclusions and recommendations. The VSD shall also provide the public with the information which does not constitute a state secret.

2.4. Administrative Tasks

The VSD conducts inspections of persons and provides conclusions/carries out control in these main fields:

Control of the residence/stay of aliens in the Republic of Lithuania

The VSD conducts assessment of the threats posed by an alien to the state security and provides a conclusion. According to this conclusion, the competent institutions take decisions, e.g. the Migration Department takes a decision on the issuance of residence permits to aliens in the Republic of Lithuania, on the granting of asylum in the Republic of Lithuania or temporary protection to an alien.

Control of goods of strategic significance

A representative of the VSD takes part at the Commission which decides on the licensing of goods of strategic significance. Moreover, the VSD, in cooperation with other institutions, conducts control of the export, import, transit, intermediation and dispatch of goods of strategic significance in the European Union.

Ensuring the protection of the objects of importance to ensuring the national security of the Republic of Lithuania

The VSD submits conclusions to the Coordinating Commission for the Protection of Objects Important for Ensuring National Security regarding the investor's conformity to national security interests.

Control of nuclear energy

The VSD, in cases prescribed by the Law on Nuclear Energy, assesses individuals intending to work at nuclear facilities and provides information to the supervisory authorities or institutions, applicants or licensees.

Control of the circulation of arms and ammunition

The VSD, in cases prescribed by the Law on Control of Weapons and Ammunition, assesses persons intending to obtain a licence to engage in weapons-related activities, provides information to the licensing authority/authority issuing permits regarding threats to the state security posed by the activities of persons.

The VSD also issues permits to officers of foreign intelligence and security services to import, transport to, export, transport from the Republic of Lithuania weapons, weapon attachments, parts thereof necessary for the performance of their official tasks.

Ensuring of aviation security

The VSD provides information, prescribed by the Law on Aviation, to the enterprise managing the airport.

The process of issuing declarations of assurance

In accordance with the procedure established by the Law on the Framework for Issuing Declarations of Assurance to Legal Entities, the VSD provides the data and information, necessary to assess the legal entities intending to participate in the tenders of the North Atlantic Treaty Organisation, compliance with the statement of assurance.

2.5. ICT Security

National Cybersecurity Centre under the Ministry of National Defence (NCSC) is the main Lithuanian cybersecurity institution, responsible for the unified management of cyber incidents, the monitoring and control of the implementation of cybersecurity requirements, the accreditation of information resources. The activities of the NCSC are regulated by the Law on Cybersecurity. The NCSC and the police consult each other and cooperate in investigating cyber incidents, exchange information related to investigation of cyber incidents, which is required to perform the functions of these authorities, which fall under their competence. When required, the investigation of cyber incidents might be reported to other entities of criminal intelligence and/or intelligence institutions, including the VSD. The procedure of inter-institutional cooperation in managing and investigating cyber incidents shall be established in the National Cyber Incident Management Plan approved by the Government of the Republic of Lithuania. In accordance with this plan, at the request of the VSD, the National Cybersecurity Centre shall inform the responsible person appointed

by the VSD about the significant and dangerous cyber incidents through the cybersecurity information network or other secure means of information transmission.

2.6. Protection of Classified Information

The VSD shall engage in intelligence and counterintelligence in the areas of the protection of information comprising a state secret and an official secret. The main functions of the VSD:

- The VSD checks persons applying for permission to work or have access to classified information.
- The VSD conducts an assessment of premises, areas and other locations and declares them suitable for storing or handling classified information.
- The VSD is an institution responsible for ensuring the security of classified transactions. It assesses the reliability of suppliers and their compliance with the requirements for the protection of classified information marked 'restricted' and supervises the protection of classified information.
- The VSD issues supplier security clearance certificates and certificates confirming compliance with the requirements for the protection of classified information classified as 'restricted'.
- The VSD carries out inspections of the status of the protection of classified information of the Republic of Lithuania in secret entities.

As already mentioned, the CAO empowers VSD officials to initiate administrative offences proceedings, to conduct investigations into administrative offences and to draw up administrative offence protocols in relation to such administrative offences: loss, damage or destruction of classified information which is an official secret; unjustified classification of information; violation of the requirements of legal acts regulating the protection of classified information.

2.7. International Cooperation

Under the Intelligence Law, the VSD has the right to cooperate, with a view to ensuring the national security of the Republic of Lithuania, with intelligence and security institutions of foreign states, international organisations and institutions.

The State Defence Council shall establish guidelines for the international cooperation of intelligence institutions with the intelligence and security institutions of foreign states, international organisations and institutions.

2.8. Personal Data Protection

As an intelligence institution, the VSD processes personal data for:

- the purposes of national security and defence in compliance with the Intelligence Law, the Law on State Secrets and Official Secrets of the Republic of Lithuania (here-

inafter referred to as 'the Law on Secrets') and the Law on the Legal Protection of Personal Data that are Processed for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences, of the Execution of Criminal Penalties or the National Security and Defence of the Republic of Lithuania (hereinafter referred to as 'the Law on Data Protection') which, *inter alia*, implemented Directive (EU) 2016/680

- the purposes of criminal intelligence (prevention, detection of criminal offences) in compliance with the Law on Criminal Intelligence of the Republic of Lithuania, the Law on Secrets and the Law on Data Protection
- purposes other than those of national security and defence and/or of criminal intelligence (when national security is not involved, for instance, for administrative purposes, examination of citizens' requests) in accordance with the General Data Protection Regulation (EU) 2016/679 (hereinafter referred to as 'the GDPR') and the Law on the Legal Protection of Personal Data of the Republic of Lithuania.

Intelligence institutions shall process personal data for the purposes of national security and defence of the following categories of data subjects:

- persons whose actions may endanger or threaten the national security, state interests, defence and economic power of the Republic of Lithuania
- persons the processing of whose data is necessary with a view to evaluating information on external risks, dangers and threats to the national security of the Republic of Lithuania, the interests of the state and its defence, and economic power
- persons who have or apply for an authorisation to handle or familiarise themselves with information comprising a state or official secret
- persons whose data are provided by the law enforcement, intelligence and security institutions of the Republic of Lithuania or foreign states
- persons who are or were linked with an intelligence institution by ties of recruitment to intelligence institution, service (employment) or cooperation relations.

In general, personal data collected by the VSD, as an intelligence institution carrying out its activities in the national security domain, are classified and are subject to data secrecy and protection in compliance with the Law on Secrets. The provisions for data protection set out in the Law on Data Protection are being applied in any case.

General principles concerning the processing of personal data are equal to ones prescribed in the EU data protection legislation. The Law on Data Protection determines principles for the processing of personal data and notes that the processing of personal data shall be lawful only if and to extent that processing is necessary for the performance of tasks carried out by a competent authority for the purposes set out in Article 1(2) of this

Law (purposes of the national security and defence as well) and that is based on the EU law or that of the Republic of Lithuania (the Law on Intelligence).

The personal data collected by competent authorities for the purposes set out in Article 1(2) of this Law (for instance, national security and defence) shall not be processed for other purposes unless such processing is authorised by the legal acts of the EU or the Republic of Lithuania. This provision is applied dspite the fact that the data was obtained from the third party.

The general principal (keystone) that personal data must be processed, used and stored for no longer than it is necessary for the purposes for which they are processed is respected. When the data are obtained from registers or state information systems, the manager (administrator) of those must ensure that the transferred data are correct and up-to-date. Each competent authority shall verify the quality of personal data before they are transmitted or made available.

Intelligence institution, as a personal data controller, has to maintain a record of all categories of processing activities, to keep logs for processing operations, also to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

However, the Law on Data Protection allows for setting up a separate (different) regime from law enforcement authorities as well as other state institutions for the intelligence services (with more exceptions from general clauses) when it is processing data in the context of the missions of the intelligence services (for the purposes of national security and defence).

The main differences are: the competent authority (controller) may not inform the data subject of the fact that his or her personal data are processed in order to protect national security for as long as such an inaction (measure) constitutes a necessary and proportionate measure in a democratic society. The data subject's right of access to his or her personal data may be restricted (refused) wholly or partly on the same grounds mentioned above. In this case, the data subject must be informed in writing of any refusal or restriction of access and the reasons for it, unless such information may undermine the purpose of protecting national security. The controller (competent authority) shall inform the data subject about the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

It is worth mentioning that when data controller (registers or state information systems (databases) managers) transfers personal data to the intelligence service, the data subject and third parties may not be informed of this.

CHAPTER XIV

The Netherlands

Patrick Ouwehand

1. POSITION OF THE SERVICES IN THE DOMESTIC LEGAL SYSTEM

1.1. Position and Role of the Services in the Public Administration System

In the Netherlands, there are two distinct intelligence and security services: the AIVD and its military counterpart, the *Militaire Inlichtingen- en Veiligheidsdienst* (Military Intelligence and Security Service, MIVD). The workings of both services are governed by the Wet op de inlichtingen- en veiligheidsdiensten 2017 (Intelligence and Security Services Act 2017, 'Wiv'). The AIVD is a civilian service and was created in 2002 as the successor of the *Binnenlandse Veiligheidsdienst* (Internal Security Service) which has existed since 1945. Its military counterpart, MIVD, also formed in 2002, is the successor of the *Militaire inlichtingendienst* (Military Intelligence Service), which was formed in 1988 from several separate defence intelligence services.

The services resort under different ministries. The AIVD under the Ministry of the Interior and Kingdom Relations and the MIVD under the Ministry of Defence. Chapter 2.1 of the Wiv governs the coordination of the duties of the services. The respective ministers are responsible for the actions of the services. They are obliged to consult with each other regularly to discuss and coordinate their policies. If necessary, other ministers are invited to take part in these consultations if this is necessary in regard to the interests that they represent.

There is a Coordinator for the Intelligence and Security Services, who prepares the aforementioned consultations and coordinates the duties of the services and informs the ministers concerned. The Coordinator performs his or her duties in accordance with instructions from the Prime Minister and in agreement with the other ministers concerned.[1] The

[1] Article 4(3) Wiv.

Coordinator also chairs the Committee for the Intelligence and Security Services (CISS). This committee consists of representatives appointed by the minister concerned or their appointed deputies from the Ministries of General Affairs, of the Interior and the Kingdom Relations, of Defence, of Foreign Affairs and of Security and Justice.[2] All participants in the CISS, including the Heads of Service, are obligated to provide the Coordinator with all necessary information.[3]

The CISS has the duty to annually survey the intelligence needs of the ministers and to assess and prioritise the identified intelligence needs.[4] On the basis of this survey, a proposal is made for the *Geïntegreerde aanwijzing inlichtingen- en veiligheidsdiensten* (Integrated Security and Intelligence Order 'Integrated Order') consisting of the investigations to be conducted categorised by subject and the planning of these investigations as well as the prioritisation of the investigations.

The ministers concerned jointly determine the final version of the Integrated Order. The finalised version is valid for a four-year period.[5] The Integrated Order can, however, be subject to change or amendment, as it is reviewed annually by the ministers[6] and the CISS consults on the progress of the execution on a regular basis and issues proposals based on this consultation.[7] It is also possible for the ministers concerned to make additions in case of an imminent threat.[8] Lastly, the Integrated Order also leaves room for the services to address unknown threats.

Because of the sensitivity of these investigations, only part of the definitive Integrated Order is made public. The classified part of the Integrated Order includes the basis for the investigations, cooperation agreements and the prioritisation of the investigations. Also included is a secret appendix, allocating specific topics for investigation to a service.

1.2. Scope of Activities of the Services

The Integrated Order determines the duties of the AIVD for the so-called A task and the D task. These tasks are determined by Article 8(2) of the Wiv. The tasks of the AIVD are summed up as follows:

- to conduct investigations with regard to organisations and persons who, either because of the objectives that they pursue or through their activities, give cause for serious suspicion that they pose a threat to the continued existence of the democratic legal order or to the security, or to other vital interests of the state

2 Article 5(1) Wiv.
3 Article 7 Wiv.
4 Article 5(4) Wiv.
5 Article 6(1) Wiv.
6 Article 6(2) Wiv.
7 Article 5(4) Wiv.
8 Kamerstukken II, 2016/17, 34 588, No. 3, p. 24.

- to conduct security screenings as referred to in the Security Screening Act
- to promote measures to protect the interests referred to under (a), including measures to protect data whose confidentiality is a matter of national security and those parts of the government services and the business sector that, in the opinion of the ministers responsible, are of vital importance for the preservation of society
- to the conduct investigations concerning other countries
- to draw up threat and risk analyses at the join request of the Minister of the Interior and Kingdom Relations and the Minister of Security and Justice for the benefit of the protection of the persons referred to in Articles 4(3)(b) and 42(1)(c) of the 2012 Police Act 2012 and to guard and protect the objects and services designated pursuant to Article 16 of that Act
- upon a request to this effect from a person or body jointly designated by a regulation from the ministers concerned, to report on data processed by the service concerning persons or bodies in the cases designated by the said regulation.

The Integrated Order only gives instructions for investigations in regard to threats (A task) and for investigations concerning other countries (D task). The Integrated Order sets out the main areas of research of the services. For brevity, in this contribution we will mainly focus on provisions pertaining to the A and D tasks.

The ministers concerned are obligated to report on the execution of the duties of the services each year before the 1st of May.[9] This report includes the activities of the service over the past year and the area of focus for the activities for the current year. According to the annual report over 2021, the research of the AIVD was focused on national threats, including right-wing extremism, right-wing terrorism, anti-government extremism, left-wing extremism, jihadist terrorism and radical Islamism. Other subjects were international threats, such as cyber threats, espionage and covert influencing activities, economic security and international jihadist terrorism. Lastly, the AIVD reported on political security interests, security screenings and national resilience.

The annual report is expressly prohibited to include information that gives insight into the means used in a specific case, confidential sources or the current level of knowledge of the services. The report is submitted to both Houses of the States General. If necessary, one or both of the Houses of the States General may be informed confidentially about information that could not be mentioned in the report. The reports are published and available on the site of the AIVD,[10] in Dutch and English.

9 Article 12 Wiv.
10 http://www.aivd.nl

1.3. Oversight and Supervision of the Services

External oversight in regard to the activities of the AIVD and the MIVD is executed in four distinct parts, via parliamentary control, the CTIVD, the TIB, the District Court of The Hague and the Netherlands Court of Audit.

Firstly, parliamentary control takes place publicly as far as this is possible. Control is exercised in the Committee for Internal Affairs of the House of Representatives if the subject matter is not classified. If sensitive or classified information is to be discussed, this takes place in the Committee for the Intelligence and Security Services (*Commissie voor de Inlichtingen- en Veiligheidsdiensten*, CIVD). The CIVD is composed of the presidents of the five largest parties in the House of Representatives. The services are authorised to provide classified documents to the Committee. The CIVD convenes in secrecy with the Secretaries and the services, but reports in public (as far as possible) on its activities. Representatives who partake in the CIVD are bound to the confidentiality of what has been discussed, even in regard to their own party. Afterwards, the CIVD only discloses the time of the meeting and the fact that the meeting happened. The agenda and the discussed subjects themselves are classified. The CIVD reports on its activities annually.

Secondly, independent oversight is executed by the *Commissie voor toezicht op de inlichtingen- en veiligheids diensten* (Committee for Oversight on the Intelligence and Security Services, CTIVD). The CTIVD has two distinct parts, which are governed by Chapter 7 of the Wiv. Firstly, the CTIVD is tasked with overseeing the legality of the execution of the provisions under and pursuant to the Wiv and to provide the Minister with advice, both solicited and unsolicited. Secondly, the CTIVD is charged with addressing complaints in regard to both services. The CTIVD reports on its activities annually.[11] This report is made generally available.[12] All the information that is provided to the CTIVD shall not be made public and requests for the inspection or publication of the information shall be denied.[13]

The CTIVD consists of four members (including a chairperson) who are appointed by a Royal Decree. Three of the members are appointed to the oversight panel and one member is appointed to the complaints panel. The complaints panel consists of one member and two other persons, appointed by a Royal Decree by the Ministers of Internal Affairs and Defence. The members are appointed for six years and may be re-appointed only once. The House of Representatives of the States General (*Tweede Kamer der Staten-Generaal*) is tasked with presenting a list of three recommendations for each vacant seat in the CTIVD. The House is required to take into account a list of recommendations compiled by the Vice-President of the Council of State, the President of the Supreme Court and the National

11 Article 132 Wiv.
12 http://www.ctivd.nl/over-ctivd/jaarverslagen
13 Article 133 Wiv.

Ombudsman. From the list of recommendations, the Ministers nominate one member. It is possible for the Secretaries to request a new list of recommendations.

The CTIVD is authorised to investigate the correct application of the Wiv on its own instigation or by request from both Houses of the States General. Anyone who is involved in the execution of the Wiv is obligated to provide the CTIVD with information or otherwise provide assistance if this is conductive for the adequate execution of its tasks. If necessary, the CTIVD is granted direct access to systems. The Committee is also authorised to interview witnesses and experts (under oath if necessary) and visit any place (with the exception of domiciles). The Committee informs the Secretary concerned and both Houses of the States General of the outcomes of its investigations. It is possible that the Chambers are informed confidentially.

Complaints can be lodged by any person in relation to an act or a perceived act by the AIVD or the MIVD. The CTIVD assesses the viability of the complaint. When a complaint is taken in consideration, the Committee rules whether it is admissible. After researching the complaint, the complainer as well as the Secretary concerned are informed. The CTIVD informs the complainer about the outcome, insofar as national security concerns allow for the sharing of the result of the complaint.

Since 2018, there is also the *Toetsingscommissie inzet bevoegdheden* (Investigatory Powers Committee, TIB) in place. The TIB is governed by Section 3.2.2 of the Wiv. It reviews (*ex ante*) the legitimacy of specific special investigatory powers granted by the Minister. The TIB consists of three members (including a chairperson), appointed by a Royal Decree. The members are appointed for six years and may be re-appointed only once. At least two of the members are required to have a background as a judge. The appointment of the members follows the same procedure as that of the CTIVD. The TIB reports on its activities annually.[14] This report is made generally available.[15] All the information that is provided to the TIB shall not be made public and requests for the inspection or publication of the information shall be denied.[16]

The services are obligated to provide the TIB with all information and provide any assistance deemed necessary for the proper execution of its tasks. However, the TIB does not have direct access to systems nor the authority to interview persons. In practice, the TIB bases its decision on the written authorisation and incidentally requests clarification from the service in the form of written questions or a briefing.

The review is limited to certain 'special' investigatory powers granted by Articles 40 (surveillance), 42 (examination of places and objects), 43 (collecting DNA), 45 (interference with automated information systems), 47 (targeted interception), 48 (investigation of communications), 49 (investigation of obtained data), 50 (automated data analysis), 53 (requesting assistance for interception), 54 (request for telecommunications data),

14 Article 35(3) Wiv.
15 http://www.tib-ivd.nl/documenten
16 Article 35(3) Wiv.

57 (requesting assistance for decryption) of the Wiv. The investigatory powers will be addressed in more detail further on in this contribution.

The AIVD asks the Secretary for the authorisation to execute the power. It is up to the discretion of the Secretary to grant authorisation or not. The TIB assesses if the authorisation has been granted in accordance with the law. If the TIB rules that the authorisation has not been granted lawfully, it informs the Secretary involved, whereupon the granted authorisation will lapse by operation of the law. The Services are not allowed to execute a power until the TIB has ruled on the legitimacy of the authorisation.[17] A ruling by the TIB is binding and cannot be challenged. The Secretaries are bound to hand the TIB all information that it deems necessary for the proper execution of its tasks.

There is a special provision in place for urgent situations that cannot wait for a decision from the TIB.[18] If this is the case, the Secretary can grant authorisation if the specifics of the case are sufficiently urgent. After the authorisation has been granted, it is submitted to the TIB as usual. Then, the TIB assesses the 'regular' lawfulness of the authorisation and shall consider if the situation was urgent enough to warrant the use of the special provision.

There is also judicial control in place. For instance, for the use of investigatory powers in regard to journalists and lawyers as well as the opening of letters and other addressed consignments, authorisation is granted not by the Secretary, but by a judge of the District Court of The Hague. Courts can also play a role in cases in relation to security screenings or in regard to criminal cases that involve an employee of the service.

Lastly, the *Algemene Rekenkamer* (the Netherlands Court of Audit) is authorised to investigate the effectiveness and efficiency of the policies and finances, management, administration and organisation of the Kingdom of the Netherlands. This includes its intelligence and security services.[19] Special provisions are in place for classified elements thereof.

2. TASKS AND MANDATE

2.1. Investigative Powers and the Role in Criminal Proceedings

With respect to its tasks, the services can exercise certain investigatory powers. Article 25 lists the methods by which the services are authorised to collect data. These methods can be further subdivided into general and special investigatory powers. The general investigatory powers are mentioned in Article 25 of the Wiv and include the collection of data:

- from publicly accessible sources of information[20]
- from sources of information to whose data the service has been granted the right of access

17 Article 36 Wiv.
18 Article 37 Wiv.
19 Kamerstukken II, 2016/17, 34 588, No. 3, p. 177.
20 Further specified in Article 38 Wiv.

- through consultation with informants[21]
- within the context of cooperation between intelligence and security services and with other bodies.

Special investigatory powers can be found in Section 3.2.5 of the Wiv. The most prominent of them are:

- static and dynamic surveillance[22]
- access to places, as far as this is reasonably necessary, given certain activities[23]
- use of natural persons who, be it under the cover of an assumed identity or occupation, are tasked (under the responsibility and instruction of a service) to perform targeted data collection[24]
- examination (with or without the use of technical means) of closed places, locked objects or objects with the aim of determining the identity of a person (DNA testing)[25]
- opening of letters and other addressed consignments[26]
- scanning of and interference with automated information systems[27]
- investigation of communications[28]
- investigation of communications with respect to specific persons, organisations and numbers of technical identifiers[29]
- investigation-specific investigation of communications[30]
- asking providers of communication services for telecommunications data[31]
- accessing places.[32]

Separately mentioned in Chapter 4 of the Wiv are the authorisation to create and use legal entities in support of operational activities[33] and the authorisation to promote or implement measures to protect the interests entrusted to the services.[34] The authorisation to use such a legal entity is given for the duration of an investigation, but it may last longer

21 Further specified in Article 39 Wiv.
22 Article 40 Wiv.
23 Article 58 Wiv, referred to activities in Article 40(1)(a), Article 42 (1)(a), Articles 45, 47 Wiv
24 Article 41 Wiv.
25 Article 42 Wiv.
26 Article 44 Wiv.
27 Article 45 Wiv.
28 Article 46 Wiv.
29 Article 47 Wiv.
30 Article 48 Wiv.
31 Articles 54, 55 and 56 Wiv. In the context of those investigatory powers, it should be noted that providers of communication services can be obligated to assist the services with regard to the acquisition of telecommunication.
32 Article 58 Wiv.
33 Article 72 Wiv.
34 Article 73 Wiv.

if this is deemed necessary to face out the use of the entity in a responsible manner. As for the promotion or implementation of measures, this can include frustrating actions but may be used to address (including preventing) anti-democratic, state-threatening activities or other activities threatening any of the interests mentioned in the Wiv. Only measures that cause the least harm to the parties involved may be taken. A measure can be implemented by an agent or employee of the service or otherwise it is possible that in the process of taking the measure criminal offences are perpetrated. As with an agent, the possibility has been created that any criminal offence committed during the execution of the measure does not constitute a punishable offence.

Apart from the above-mentioned investigatory powers, if a service sees reason to collect data from a source of information other than indicated above, the minister concerned may grant such an authorisation at the request of the Head of Service. Such a request shall state the reasons why it is necessary to use the source in question.

An important difference between general and special investigatory powers is that general investigatory powers can be exercised for the benefit of any of the tasks of the services. Special investigatory powers may only be exercised to the extent necessary for the proper performance of the duties mentioned under Article 8(a) and (d) of the Wiv,[35] namely investigations with regard to organisations and persons and investigations concerning other countries.[36] There is, however, an exception to this rule. In certain situations it is permitted to invoke special investigatory powers to support the proper performance of duties by the services.[37] This means that the execution of the power is not directly related to Article 8(a) and (d) of the Wiv. A special investigatory power can be invoked, but only in two specific instances. Firstly, insofar as the power is needed to assess whether it is necessary to take special security measures for a person working for or on behalf of the service. For example, if an observation needs to be carried out to ensure the security of the operators while they are placing a beacon or microphone. Secondly, using a special investigatory power is allowed if it is necessary to assess the trustworthiness of persons who cooperate in data. This can be the case if the service suspects that a human source is reporting on its cooperation with the AIVD to an adversary. In these cases, the investigatory powers can only be invoked for a limited time (4 weeks). The authorisation needs to be given by the Minister concerned and a notification of the authorisation needs to be sent to the CTIVD.

Special investigatory powers are subject to stricter safeguards than general investigatory powers. Those safeguards are designated by the terms: necessity, subsidiarity, proportionality and limitation of the scope (*gerichtheid*). These safeguards aim to sub-

35 Article 10(2)(a), (c) and (e) Wiv for the MIVD.
36 Article 28(1) Wiv.
37 Article 28(2) Wiv.

stantiate the impact of the investigatory power towards the target and others. In short, this means that the services can only exercise that power which, in view of the specifics of the case, is necessary at the moment and will generate intelligence that is beneficial to the current investigation. Subsidiarity means that if the objective for which the power is being exercised has been achieved or can be achieved by exercising a less intrusive power, and the service is not allowed to invoke the more intrusive power. Proportionality requires weighing any conceivable harm against the legitimate interests of the person in question in comparison with the interests that the service aims to look after. Lastly, the service needs to make efforts to invoke the power in a scope that is as limited as possible. Because of the infringement that most special investigatory powers make on the interests of subjects, the service must ensure that other persons are not affected or, if it is unavoidable, they are affected as little as possible. A request for the authorisation to exercise a special investigatory power (and a request for extension) includes[38] such safeguards as well as an indication of the power requested, information about the identity of the person or organisation (if applicable) – if the person is a journalist or lawyer – and a description of the investigation concerned. Most – but not all – authorisations are granted for the duration of no more than three (3)months.[39] If the authorisation is extended, the obtained results and their significance need to be mentioned in the new request.

As for the retention of data, the services are obligated to evaluate the data acquired by a special investigatory power for relevance within a year. For some kinds of data, this period is longer.[40] If the information is relevant for the proper execution of the tasks of the AIVD, it may retain the information as long as it still has significance in regard to the purpose for which it is processed. Any data that are no longer significant shall be deleted.

The services are also authorised to apply automated data analysis to specified types of data that it has obtained or has access to. The data may be automatically analysed by comparing them in an automated manner in relation to other data or by combining them, searching them on the basis of profiles and comparing them in order to detect specific patterns. This gives a lot of room to enrich large amounts of data. However, promoting or implementing measures against a person based solely on the findings from automated data analysis is not allowed.[41]

The officials of the services are not authorised to conduct investigations into criminal offences.[42]

38 Article 29 Wiv.
39 Article 29 Wiv.
40 E.g. Article 48(6) Wiv.
41 Article 60 Wiv.
42 Article 13 Wiv.

2.2. Protection of Classified Information and Provisions for Officials

The Head of Service is responsible for ensuring the confidentiality of data, the confidentiality of the sources from which data originates and the safety of the persons cooperating with the collecting of data.[43] The Head of Service is also responsible for adequate technical, staffing and organisational measures to ensure that information is processed in accordance with the law.[44] These provisions ensure that the data that are within the care of the services are handled with proper care and serve as fundamental principles for most if not all internal policies. Both Articles 23 and 24 of the Wiv are equally applicable to the operations of the CTIVD[45] and the TIB.[46]

Confidentiality itself is governed by Chapter 8 of the Wiv. In this chapter, it is determined that all parties involved in the implementation of the Wiv and who are given access to data which they know or should reasonably suspect to be confidential in nature are obliged to observe this confidentiality. This obligation extends beyond the period of time for which the individual is involved with the implementation of the Wiv. The only exception to this is if they are required by law to disclose the data. If an official of the service is required to serve as a witness or an expert, they may only breach the confidentiality mentioned before if the official receives a written release from that obligation from the minister concerned and the Minister of Security and Justice.

Officials are prohibited to travel to certain countries designated by the ministers concerned.[47] This includes travels to countries involved in actual ongoing armed conflict. An exemption can be granted by the minister concerned. These limitations also apply to certain appointed officers from other government bodies performing activities on behalf of the services. The Heads of Service are responsible for making the necessary arrangements for the protection of the officials of the service.[48] This includes permitting the use of assumed identities in the context of their performance if that is in the interest of their personal safety.

2.3. Internal and International Cooperation

As a base rule, the Wiv utilises a closed system for the sharing of information. The services are only allowed to share information insofar as the Wiv provides rules to that effect. As such, provisions are in place for the sharing of information with other parties. This includes the sharing of information with investigative services. Information can be shared nationally as well as internationally.

43 Article 23 Wiv.
44 Article 24 Wiv.
45 Article 133 Wiv.
46 Article 35(3) Wiv.
47 Article 14 Wiv.
48 Article 15 Wiv.

The general provision for sharing data externally is Article 62 of the Wiv. This article authorises the services to share data that they have processed with the ministers concerned, other administrative authorities concerned, other persons or bodies concerned and foreign intelligence and security services – as well as *international* intelligence and security services. If the nature of the notification so requires, the notification must be authorised by the Minister. This provision gives quite a number of possibilities for sharing information, but there are some added specifics.

In the Netherlands, the sharing of data is possible in multiple forms. The most impactful of these is the so-called *ambtsbericht* ('administrative notification'). An administrative notification is declassified and is issued to a person or an entity outside of the service. In the notification, the service shares information that it has gathered in the course of its investigations. The recipient of an administrative notification is authorised to act upon the data it contains. This is not possible for other forms of data sharing as an *inlichtingenbericht* (intelligence notification). An administrative notification based on Article 62 of the Wiv may be issued if it is in the interests of the proper execution of the tasks of the service. The notification is based on an underlying dossier. The notification itself does not include the underlying (classified) documents because pursuant to Article 23 of the Intelligence and Security Services Act 2017, the service is responsible for the confidentiality of the data that it processes as well as for safeguarding the data sources and the persons engaged in the collection of data. This way, the sources of the notification remain undisclosed. The recipient of the notification is authorised to inspect in person the physical supporting dossier to verify its correctness but may only act upon the actual text of the notification.

Criminal offences encountered during investigations of the service may be shared with the Public Prosecutor, who is then authorised to start an investigation based on the administrative notification.[49] This may take place upon the service's own initiative or upon request. Unlike with the issuing of administrative notifications to another entity, the services are not limited to share information with the Public Prosecutor's office only if it is within the context of a proper performance of their duties. At the same time, there is no obligation for the services to share such information. Whether they share the data is at the discretion of the services.

If the administrative notification becomes the subject of judicial proceedings, it is possible to ask the judge to evaluate the correctness of the administrative notification. The judge is authorised to examine the underlying information without the complainant accessing these classified documents. The judge will subsequently assess the underlying information and rule if the notification is correct or not. As national security concerns are

[49] Article 66 Wiv.

an adequate reason to limit access to the underlying information the complainant will, regardless of the outcome of the ruling, not be given access to the classified documents.

If the services wish to share information with other intelligence and security services, there needs to be a cooperative relationship with those services. A cooperative relationship means that the potential partner service needs to be evaluated by a couple of standards set out in Article 88 of the Wiv. This means an evaluation of the democratic embedment of the service, the respect for human rights in that country, the professionalism and reliability of the service, the legal powers and capabilities of the service and the offered level of data protection. The assessment is meant to gain insight into the risks involved when cooperating with the service. Based on the assessment, it is also determined what the scope of the cooperation can be. If there are high risks involved, a consequence can be that cooperation with that service is limited or even that no cooperation whatsoever is allowed. If new circumstances arise after an assessment has been concluded, the service is obligated to re-assess the cooperative relationship. Once the cooperative relationship is established by the minister formalising the assessment, cooperation can take place via a couple of routes. Primarily, via Article 62 of the Wiv, when the sharing of data is in the interest of the AIVD or the MIVD, or Article 89(1) of the Wiv if that is in the interest of the partner service and the sharing of the data is not detrimental to the correct execution of the tasks of the service. As a ground rule, the services always share data with partner services under the condition that the data may not be disclosed to third parties. In addition, the AIVD and MIVD use a joint disclaimer requesting further restrictions to the use of the data that they provide to partner services. Likewise, the services never further disclose data received from partner services unless they have obtained express consent to that effect.

It remains possible to cooperate in emergency situations. Article 64 of the Wiv is the emergency provision for the situation wherein there are urgent and serious reasons for sharing information if there is no cooperative relationship or if there is such a relationship, but the risks do not allow for the regular sharing of information.

Provisions are also in place for providing or requesting technical and other forms of support in the interest of the AIVD/MIVD or the partner service.[50] Support may only be provided to a partner service if this is not incompatible with the interests of the services and the form of support is not contrary to a proper performance of duties by the services. The provided support may not entail providing the partner service with the opportunity to independently gather data in the Netherlands. It is possible that the requested or provided support encompasses the usage of special investigatory powers, but the services are under no circumstance allowed to request support that amounts to actions that they themselves would not be allowed to execute. Lastly, outgoing and incoming support may be granted

[50] Articles 84(4) and 90 Wiv.

only if this fits in the boundaries established in the assessment that is the basis of the co-operative relationship.

2.4. Personal Data Protection

The use of personal data is governed by the Wiv and Wvo. The principles in these acts are based on those in Regulation (EU) 2016/679 (GDPR). A core principle is Article 17 of the Wiv, which states that the services are authorised to process data with due observance of the requirements set out in the Wiv or the Wvo. The GDPR itself is not applicable to the activities of the services for reasons of national security. The services are, however, still held to high standards when it comes to the processing of data. Broadly speaking, the AIVD is required to act in line with the GDPR. Especially the main principles relating to the processing of personal data are adopted in comparable terms in the national legislation governing the workings of the services. For instance, the Wiv stipulates that the services shall process personal data with care and take measures to verify that the data are reliable. The Wiv also gives provisions as to how long the data can be stored. Furthermore, in regard to the processing of data, the Wiv stipulates that the AIVD may only process data if this is necessary for the correct execution of its tasks and always needs to ensure that the processing is done in accordance with the law and takes place decently and diligently. If a person suspects his or her data have been unlawfully processed by the AIVD, the Wiv offers the person the possibility of lodging a complaint with the Supervisory Committee for the Intelligence and Security Services (CTIVD).

There are, however, some differences between the Wiv and the GDPR due to the nature of the tasks of the AIVD. For instance, the right of a data subject to access his or her personal data is still in place, but only insofar as this does not give this person insight into the *modus operandi* and sources of the service. In this regard, the AIVD has the obligation to notify the data subject about the historical use of certain investigatory powers targeting him or her and only if disclosure does not interfere with ongoing investigations. Also notable is that third parties which are asked/required to supply personal data to the AIVD are exempt from the GDPR based obligation to inform the data subject about the provision of the data to the AIVD.

Article 19 of the Wiv narrows the scope of the persons in regard to whom the services are allowed to process personal data. This includes authorisation to process the personal data of persons who give cause for serious suspicion that they pose a threat to the democratic legal order or to the security, or other vital interests of the state or in the context of investigations into other countries. The services are equally authorised to process personal data for reasons of security screenings or if their information has been obtained by another intelligence or security service. The services are not authorised to process personal data on the basis of a person's religion, personal beliefs, race, membership of a trade union, health

or sexuality. The processing of such data is only allowed in addition to the processing of other data and only insofar as this is unavoidable for the purpose of processing the data.[51]

Data that have lost their significance in regard to the purpose, for which they were being processed, need to be deleted (unless there are statutory rules prohibiting their destruction).[52] It is, however, quite difficult to assess whether data have truly lost their meaning, but it does mean that the services are not authorised to store data for an unlimited period. Data which are incorrect or are being processed wrongfully shall be corrected or deleted. This also entails an obligation for the minister that if he or she has informed any other party, he or she shall inform the receiving party about the incorrectness of the data or about the fact that the data has been wrongfully processed as soon as possible.

An important topic in regard to the processing of data is the acquisition of large sets of data. In 2021, the ministers concerned composed a (temporary) regulation on how the services are to act when they acquire and process large data sets – *Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017* [Temporary Regulation on the Processing of Bulk Data Sets Wiv 2017]. Large data sets are essential for the adequate execution of the tasks of the services, in regard to known as well as unknown threats. As such, they can help identify potential targets, unknown *modi operandi* of terrorist organisations or activities of foreign intelligence and security services. The problem is, however, that the vast majority of the data in such sets are not and will never be subject of an investigation by the services. Infringing on the legitimate interests of persons to whom the data belong can therefore be disproportionate. At the same time, the possibilities of obtaining the information included in such a set that is relevant for the services are often very limited. Because of the interests involved on both sides, the temporary regulation provides additional safeguards before any set can be obtained and processed further.

51 Article 19(3), (4) Wiv.
52 Article 20 Wiv.

CHAPTER XV

Poland

Piotr Burczaniuk

1. POSITION OF THE INTELLIGENCE AND SECURITY SERVICES IN THE DOMESTIC LEGAL SYSTEM

The year 1989 brought fundamental constitutional evolution caused by the end of the communist system and authoritarian rule. In consequence, the institutional model of the intelligence and security services was significantly modified. As a result of this transformation, Poland became, as enshrined in Article 2 of the Constitution of the Republic of Poland,[1] a democratic state ruled by law, implementing the principles of social justice. The new system was based on Montesquieu's principle of triple division of power. The institutional architecture of the intelligence and security services had to be adapted accordingly.

On 6 April 1990, the Polish Parliament enacted two essential legal acts the aim of which was to liquidate the communist intelligence and security services. The first of these acts (the Act on the Police[2]) dissolved the Citizen Militia, an organisation of communist origin, and created the Police as an authority responsible for the protection of public order. The second act (the Act on the State Protection Authority[3]) liquidated the Security Service – the crucial civilian security organ and created the State Protection Authority (UOP) as a civilian authority responsible for protecting state security and its constitutional order. The UOP's tasks included identifying and countering threats against security, defence, independence, territorial integrity as well as preventing and detecting offences of espionage, terrorism and other serious offences against the state. Furthermore, the UOP was responsible for countering the unlawful use of state secrets and for providing the highest state authorities with information and analyses.

---

1 Journal of Laws of 1997, No. 78, item 483.
2 Original text published in Journal of Laws of 1990, No. 30, item 179.
3 Original text published in Journal of Laws of 1990, No. 30, item 180.

It should be noted that the political transformation triggered major structural modifications in the architecture of the military intelligence and security services. On 22 June 1990, the Military Information Services were established as an organ responsible for identifying and countering threats against defence, the unlawful use of information classified as a state secret in the military area and for providing other authorities with the information analyses relevant for the area of defence.

As far as the civilian intelligence and security services are concerned, further significant organisational changes were introduced in 2002, when the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency[4] (hereinafter referred to as 'the ABW Act') liquidated the UOP and divided it into two separate bodies: the Internal Security Agency (ABW) – acting within the territory of Poland, responsible, in accordance with Article 1 of the ABW Act, for the protection of internal security of the state and its constitutional order, and the Foreign Intelligence Agency (AW) – a service of external nature, responsible, in accordance with Article 2 of the ABW Act, for the external security of Poland. Furthermore, in 2006, the third civilian intelligence and security service was set up by the Act of 9 June 2006 on the Central Anti-Corruption Bureau[5] (hereinafter referred to as 'the CBA Act'). Its tasks comprised countering corruption in the public and economic sphere, in particular in state and local authorities, and neutralising activities that may threaten national economic interests.

In the military domain, the Military Information Services were liquidated on 30 September 2006[6] and replaced by the Military Counter-Intelligence Service (SKW) and the Military Intelligence Service (SWW). The SKW is responsible, in accordance with Article 1 of the Act of 9 June 2006 on the Military Counter-Intelligence Service and the Military Intelligence Service[7] (hereinafter referred to as 'the SKW and the SWW Act'), for the protection against internal threats to the state defence, security and combat capabilities of the Armed Forces of the Republic of Poland and other entities subordinated to or supervised by the Minister of Defence. Furthermore, the SKW and the SWW Act established the Military Intelligence Service, responsible, under Article 2 of the above-mentioned act, for the protection against external threats to the state defence, security and combat readiness of the Armed Forces of the Republic of Poland and other entities subordinated to or supervised by the Minister of Defence.

The aforementioned legal acts shaped the institutional architecture of the Polish intelligence and security services. Their powers and tasks will be examined in detail further in this chapter.

---

4 Original text published in Journal of Laws of 2002, No. 2002, items 74 and 676.

5 Original text published in Journal of Laws of 2006, items 104 and 708.

6 Pursuant to the Act of 9 June 2006 – Provisions implementing the Act on the Military Counter-Intelligence Service and the Military Intelligence Service and the Act governing the performance of the Military Counter-Intelligence Service and the Military Intelligence Service officers' duties, Journal of Laws of 2006, No. 104, item 711.

7 Original text published in Journal of Laws of 2006, No. 104, item 709.

1.1. Legal Definition of the Intelligence and Security Services

The intelligence and security services may be defined on the basis of one of three models: the material model – focused on their tasks (intelligence, counterintelligence and anti-terrorist) and powers (operational activities); the institutional model – including predefined categories of such organs; the mixed model – assuming a combination of these features.

The Polish legislator adopted the institutional model, stipulating that the legal definition of intelligence and security services shall comprise the ABW, the AW, the SKW, the SKW and the SWW (Article 11 of the ABW Act). The same definition is provided in Article 142(2) of the Standing Orders of the Sejm of the Republic of Poland (the Resolution of the Sejm of 20 July 1992).[8] This term is employed in the Polish legal acts in this sense. 'One of the consequences of such an approach of the Polish legislator is that public organs, responsible for safeguarding state security, public order and protecting the interests of the State Treasury, are divided into two groups: intelligence and security services and organs devoid of such a status. […] In the legal literature, they are jointly referred to as police organs.'[9] At the same time, it does not mean that they cannot pursue operational activities. On the contrary, the Polish legislation confers, albeit to varying degrees, the competence to carry out such actions, besides the intelligence and security services, to the Police, the Border Guards, the State Protection Service, the Military Gendarmerie and the National Fiscal Administration. It seems that the fundamental criteria differentiating the intelligence and security services from the police-type authorities are the scope of their tasks and powers, which are focused on intelligence-related issues, combating terrorism and anti-corruption efforts as well as the supervisory system, which will be further examined in this chapter.

1.2. Position of the Intelligence and Security Services in the Public Administration System

In the Polish legal system, the intelligence and security services form part of the government administration. Article 10(2) of the Constitution stipulates that executive power shall be vested in the President of the Republic of Poland and the Council of Ministers. The Council of Ministers is composed of the Prime Minister and ministers who are responsible for particular departments of the government administration (sectoral ministers) or who carry out the tasks assigned to them by the Prime Minister (non-sectoral ministers).

In accordance with Article 33a(1)(7) and (7a) of the Act of 17 September 2021 on the Act on the Public Administration Departments,[10] the Prime Minister shall supervise the activities

8 MP 2021, item 483.

9 M. Bożek, *Służby specjalne oraz kryteria ich klasyfikacji na gruncie polskiego ustawodawstwa* [The Intelligence and Security Services and Their Classification Criteria in the Polish Legal System], [in:] *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014, p. 16.

10 Journal of Laws of 2021, item 1893.

of the government administration which fall outside the scope of government administration departments, carried out, among others, by the ABW, the AW and the CBA. It proves that these organs are of non-sectoral nature. At the same time, the institutions in question have not been assigned to the government department of home affairs – hence, they are not subordinated to the minister responsible for home affairs. As far as the governmental practice in the last years is concerned, the Prime Minister, while carrying out his or her duties in the domain of the intelligence and security services, often acts through an intermediary – the Minister-Coordinator of the Intelligence and Security Services (this function is frequently combined with the function of the Minister of Home Affairs and Administration) or the authorised Secretary of State in the Chancellery of the Prime Minister. On the other hand, the military services – the SKW and the SKW – should be classified as sectoral services, since they are subordinated to the Minister of Defence. The position of the said institutions in the government administration structure is also conditioned by the position of the heads of these services.

Pursuant to Article 3 of the ABW Act, the Head of the ABW and the Head of the AW are central organs of the government administration, acting with the support of the ABW and the AW – the government administration offices. Hence, the ABW, the AW as well as the CBA, the SKW and the SWW form part of the public administration and are governed by the administrative law, in particular by the Act of 14 June 1960 – the Code of Administrative Procedure.

The Head of the ABW and the Head of the AW are directly responsible to the Prime Minister, who, according to Article 20 of the ABW Act, adopts, by way of order, the statutes that define their internal organisation,[11] in particular their organisational structure.

As far as the CBA is concerned, pursuant to Article 5 of the CBA Act, this institution is managed by the Head of the CBA – a central government administration organ supervised by the Prime Minister. He or she acts with the support of the CBA, which is a government administration office. Similarly to the ABW and the AW, the Prime Minister adopts, by way of order, its statute defining its internal structure.[12]

With regard to the military services, according to Article 3 of the SKW and the SWW Act, the heads of these bodies are central government administration organs, acting with the support of the SKW and the SWW, which are government administration organs. They are directly responsible to the Minister of Defence, subject to certain powers of the Prime Minister or the Minister-Coordinator of the Intelligence and Security Services, if appointed.

---

[11] As far as the provisions currently in force are concerned, Order No. 163 of the Prime Minister of 26 September 2018 on granting the statute of the Internal Security Agency (MP of 2018, item 927) enumerates 23 organisational entities of the ABW, whereas Order No. 174 of the Prime Minister of 26 June 2002 on granting the statute of the Intelligence Agency (MP of 2021, item 811) enumerates 8 organisational entities of the AW.

[12] As far as the provisions currently in force are concerned, Order No. 72 of the Prime Minister of 6 October 2010 on granting the statute of the Central Anti-Corruption Bureau (MP of 2010 No. 76, item 953) enumerates 23 organisational entities of the CBA.

The Minister of Defence, upon the Prime Minister's previous approval, adopts, by way of order, the statutes that define their internal organisation.[13]

It should be emphasised that all the basic legal acts determining the powers and tasks of the institutions in question stipulate that the Prime Minister is in charge of coordinating their actions and that he or she may confer these tasks on the above-mentioned Minister-Coordinator of the Intelligence and Security Services, whereas it is the Prime Minister who decides whether or not to appoint such a minister and how broad his or her powers should be.

1.3. The Scope of Tasks and Activities of the Intelligence and Security Services

As mentioned in the introduction above, an institutional model of the intelligence and security services, which differentiates them from police-type services, was adopted in the Polish legal system. The scope of tasks assigned to them, focused on threats and offences that may endanger the very existence of the Polish state, was the rationale behind such separation. Undoubtedly, the tasks in domains such as intelligence, counterintelligence or the protection of classified information, which are traditionally assigned to the intelligence and security services, have been the pillars of such tasks. However, these tasks have been influenced by new types of threats, specific to the 21st century, such as terrorism, corruption or economic offences. Furthermore, the scope of tasks conferred on the intelligence and security services in Poland fluctuates. A trend can be observed – their scope covers the new threats identified in the 21st century, involving the use of modern technologies or hybrid threats.

In this context, it should be indicated that the tasks of the ABW (the biggest intelligence and security service in Poland) include, on the one hand, identifying and preventing threats to the internal security of the state, its constitutional order and, in particular, its sovereignty and international position, independence, territorial integrity and defence, and, on the other hand, identifying, preventing and detecting the following offences:

- espionage, terrorism, unlawful disclosure or use of classified information and other prohibited acts which may threaten state security
- offences which may endanger vital national economic interests
- corruption of persons performing public functions referred to in Articles 1 and 2 of the Act of 21 August 1997 imposing restrictions on business activities of persons performing public functions[14] if such activities may threaten state security

---

[13] As far as the provisions currently in force are concerned, the Order of the Minister of Defence of 21 April 2017 on granting the statute of the Military Counter-Intelligence Service (MP of 2017, item 431) enumerates 23 organisational entities of the SKW; in the case of the SWW: the Order of the Minister of Defence of 28 May 2008 on granting the statute of the Military Intelligence Service (MP of 2008 No. 44, item 385) enumerates 13 organisational entities of the SWW.

[14] Official Journal of 2019, item 2399.

- offences concerning manufacturing and trade in goods, technologies and services of strategic importance for state security
- illicit manufacturing, possession and trade in weapons, munitions, explosives, stupefacients and psychotropic substances in international trade
- certain offences against administration of justice specified in the Act of 6 June 1997 – the Criminal Code[15] if they are related to the offences listed above.

Furthermore, the ABW's tasks comprise:

- identifying, preventing and detecting threats to the security of vital computer and information systems used by public administration organs or network systems covered by the single list of premises, installations, devices and services forming part of the critical infrastructure and IT systems used by owners and holders of premises, installations and devices forming part of the critical infrastructure referred to in Article 5b(7)(1) of the Act of 26 April 2007 on the crisis management[16]
- identifying assets subject to forfeiture in connection with the offences referred to above
- carrying out, within the scope of its competence, the tasks concerning the protection of classified information and exercising the function of the national security authority in the area of the protection of classified information in international relations
- gathering, analysing, processing and providing the information which may be of vital importance for the internal security of the state and its constitutional order to the competent authorities.

It needs to be stressed that the ABW may operate abroad only in connection with the process of pursuing its tasks within the territory of Poland and exclusively in the scope of recognising, preventing and detecting the offences referred to in the Article 5 of the ABW Act.

Furthermore, the Head of the ABW carries out the tasks of the point of contact referred to in Article 16(3) of the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.[17]

As M. Gołaszewska sums up, 'the internal security of the state and its constitutional order are the values the safeguarding of which is the ABW's primary task – a situation where the constitutional organs can act effectively and fulfil their duties imposed by the Constitution.'[18]

---

15 Official Journal of 2021, items 2345 and 2447.

16 Official Journal of 2020, item 1856.

17 Official Journal of the European Union L 210 of 6 August 2008, p. 1.

18 M. Gołaszewska, *Zadania ABW w zakresie zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny* [The Tasks of the Internal Security Agency in the Area of Combating Threats Against the Internal Security of the State and Its Constitutional Order], [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (ed.), Warszawa 2021, p. 38.

According to Article 6 of the ABW Act, the AW's tasks comprise:

- gathering, analysing, processing and providing the information which may be of vital importance for the security and international position of the Republic of Poland and its economic and defensive potential to the competent authorities
- identifying and countering external threats to the security, defence, independence and territorial integrity of the Republic of Poland
- protection of Polish representative offices abroad and their staff against the actions of foreign intelligence services and other threats which may be detrimental to the interests of the Republic of Poland
- ensuring the cryptographic protection of communications with the Polish diplomatic and consular offices abroad and of the diplomatic post
- identifying the international terrorism, extremism and international organised criminal groups
- identifying the international trade in arms, munitions, explosives, stupefacients and psychotropic substances and goods, technologies and services of strategic importance for the security of the state as well as recognising the international trade in weapons of mass destruction and threats connected with proliferation of such weapons and their carriers
- identifying and analysing threats in the areas of conflicts and international crises which may have an impact on the security of the state and undertaking actions to eliminate such threats
- identifying, countering and preventing terrorist incidents against the Polish citizens or its assets abroad, excluding the terrorist events directed against the personnel or assets of the Armed Forces of the Republic of Poland
- signals intelligence
- carrying out other actions specified in separate legal acts and international treaties.

It is important to note that the AW exercises its tasks outside the territory of the Republic of Poland. This institution may operate on Polish territory only in relation to its actions carried out abroad. In this case, the AW acts through the intermediary of the Head of the ABW.

The CBA was established in 2006 in order to combat corruption in the public and economic spheres. In particular, the scope of its competence encompasses countering corruption in public and local government bodies and actions which may undermine national economic interests. Hence, the CBA is responsible for identifying, preventing and detecting offences referred to in the CBA Act if such offences are connected with corruption or threats to the national economic interests. Furthermore, the list of its tasks includes:

- identifying assets subject to forfeiture
- identifying and countering violations of the Act of 21 August 1997 imposing restrictions on business activities of persons performing public functions

- documenting the grounds for and initiating the application of the provisions of the Act of 21 June 1990 on the return of unduly gained benefits to the disadvantage of the State Treasury (Journal of Laws of 2022, item 255, as amended)
- disclosing non-observance of procedures, laid down by law, concerning decisions in the area of: privatisation and commercialisation, financial support, granting public contracts, disposal of assets of entities or entrepreneurs referred to in Article 1(4) and granting concessions, permits, personal and transactional exemptions, allowances, preferences, quotas, ceilings, sureties and credit guarantees
- verifying the correctness of the implementation of public-private partnership contracts
- verifying the correctness and veracity of asset declarations or declarations on the conduct of business activities of persons exercising public functions
- analysing phenomena falling within the scope of the CBA's scope of competence and providing information to the Prime Minister, the President of the Republic of Poland, the Sejm and the Senate.

Similarly to the legal provisions governing the ABW's activities, the CBA may only operate abroad in connection with fulfilling its tasks on the territory of Poland in the area of identifying, preventing and detecting criminal offences.

With regard to the military intelligence and security services, the SKW's tasks encompass, in accordance with Article 5 of the SKW and the SWW Act, identifying, preventing and detecting the following offences:

- offences against peace, humanity and war crimes referred to in Chapter XVI of the Criminal Code and in other legal acts and international treaties.
- offences against the Republic of Poland referred to in Chapter XVII of the Criminal Code and such offences directed against states that guarantee reciprocity.
- assault on a unit of the Armed Forces of the Republic of Poland.
- corruption, active and passive bribery if they may threaten the security or combat readiness of the Armed Forces of the Republic of Poland or other organisational entities of the Ministry of Defence.
- offences against the protection of information if they may threaten the security or combat readiness of the Armed Forces of the Republic of Poland.
- offences concerning trade in goods, technologies and services of strategic importance for state security or for international peace with foreign entities without a permit issued by the competent authority or in a way that violates conditions set forth in such a permit and providing false or incomplete information to the competent authorities in the process of obtaining such a permit.

- other offences against the defence potential of the state, the Armed Forces of the Republic of Poland and the organisational entities of the Ministry of Defence and states that guarantee reciprocity.
- certain offences against administration of justice specified in the Act of 6 June 1997 – the Criminal Code if these offences are related to the prohibited acts referred to above as well as identifying assets subject to forfeiture in connection with such offences.

Furthermore, the catalogue of the SKW's tasks includes:

- cooperating with the Military Gendarmerie and other authorities competent for the prosecution of the offences referred to above
- identifying, preventing and detecting terrorist offences and incidents that threaten the military potential of the state, the Armed Forces of the Republic of Poland and the organisational entities of the Ministry of Defence
- exercising, without the scope of its competence, the tasks specified in the Act on the protection of classified information
- acquiring, storing, analysing, processing and providing to the competent authorities the information which may be important for the defence, security and combat readiness of the Armed Forces of the Republic of Poland or the organisational entities of the Ministry of Defence, in connection with identifying the offences and undertaking actions to eliminate detected threats
- carrying out actions in the area of radio-electronic counterintelligence and conducting projects concerning cryptography and cryptanalysis
- taking part in planning and exercising control over the implementation of international disarmament treaties
- protecting the military units, other organisational entities of the Ministry of Defence and soldiers exercising their tasks outside the territory of the Republic of Poland
- protecting the scientific research and development works commissioned by the Armed Forces of the Republic of Poland and other organisational entities of the Ministry of Defence as well as protecting the production and trade in goods, technologies and services of strategic importance commissioned by the Armed Forces of the Republic of Poland and other organisational entities of the Ministry of Defence, in connection with the offences combated by the SKW.

The SKW's tasks outside the territory of the Republic of Poland may be conducted in connection with its activities in the country, although, contrary to the ABW, in the full scope of its competence.

The catalogue of the SWW's tasks includes, in accordance with Article 6 of the SKW and the SWW Act:

- gathering, compiling, analysing, processing and providing to the competent authorities the information which may be of vital importance for the security of the military potential of the Republic of Poland, security and combat readiness of the Armed Forces of the Republic of Poland and for the conditions in which they exercise their tasks outside the territory of the Republic of Poland.
- identifying and countering external military threats to the defence of the Republic of Poland or international terrorist threats.
- identifying the international trade in arms, munitions and explosives, goods, technologies and services of strategic importance for the security of the state, as well as identifying the international trade in weapons of mass destruction and threats connected with the proliferation of such weapons and their carriers.
- identifying, preventing and countering terrorist incidents directed against the personnel and assets of the Armed Forces of the Republic of Poland abroad and neutralising the effects of such incidents.
- identifying and analysing threats in the areas of conflicts and international crises which may have an impact on national defence and combat readiness of the Armed Forces of the Republic of Poland as well as undertaking actions to prevent such threats.
- exercising actions in the area of signals intelligence for the benefit of the Armed Forces of the Republic of Poland in the domain of cryptanalysis and cryptography.
- taking part in the process of setting up the Polish military representations abroad.
- taking part in planning and exercising control over the implementation of international disarmament treaties.

The tasks indicated above are exercised outside the territory of the Republic of Poland. The SWW's activities may be carried out in Poland exclusively in connection to fulfilling its tasks abroad. Then, carrying out intelligence activities on the territory of Poland is permissible solely through an intermediary – the Head of the ABW or the Head of the SKW – depending on the circumstances of the specific case.

1.4. Control and Supervision of the Intelligence and Security Services

In Poland, the services are controlled and supervised by executive authorities as well as the legislature and judiciary.

Within the legislative power, the functions are exercised by the Parliament (the Sejm and the Senate). According to Article 95(2) of the Constitution, the Sejm shall exercise control over the activities of the Council of Ministers within the scope specified by the provisions of the Constitution and legal acts. Obviously, this includes a legalistic element of control. The principles for exercising such control are set out in three legal acts:

- The Act of 9 May 1996 on the exercise of the mandate of a member of the Parliament and senator[19]
- The Act of 21 January 1999 on the Sejm's investigative committee[20]
- The Standing Orders adopted by the Sejm on 30 July 1992.[21]

It should be emphasised that the analysis of the relevant laws governing the powers and tasks of the intelligence and security services shows that the said services are controlled by the Sejm (see Article 3(1) of the ABW Act; Article 5(2a) of the CBA Act; Article 3(3) of the SKW and SWW Act).

The most important element of parliamentary control over the services is the Committee on Intelligence and Security Services, acting since 1995. According to Article 18 of the Standing Orders, the said Committee is one of 28 permanent committees working in the Sejm. All the rules and procedures for its functioning are regulated in Chapter 12 Section II of the Standing Orders. The material scope of the Committee is defined in the Annex to the Standing Orders. The Committee's scope of competence is concentrated on three regulatory areas: legislative, advisory, and supervisory area.

Unlike the Sejm, the powers of the Senate to exercise control over the services are rather marginal and strictly limited. The Senators may ask the Prime Minister and the heads of the services about matters relating to the duties of a senator.

Apart from the organs referred to above, the control and supervision of the intelligence and security services is also exercised by the organs of state control and for defence of rights – the Supreme Audit Office (NIK) and the Ombudsman. According to Article 203(1) of the Constitution, the Supreme Audit Office shall audit the activity of the organs of government administration, the National Bank of Poland, state legal persons and other state organisational units regarding the legality, economic prudence, efficacy and diligence. The Ombudsman shall safeguard the freedoms and rights of persons and citizens specified in the Constitution and other normative acts. In case of suspected violation of fundamental freedoms and rights, the Ombudsman may open his or her clarification proceedings or ask other competent authorities to start their investigation.

Within the executive branch, the control is exercised by the Prime Minister, the Minister-Coordinator of Intelligence and Security Services and the President.

It should be noted that 'the role of the executive branch in supervising the services is focused on the effectiveness – the intelligence and security services, forming part of the executive, in general, are accountable for achieving their targets set out by the government

[19] Journal of Laws of 2018, item 1799.
[20] Journal of Laws of 2016, item 1024.
[21] MP 2021, item 483.

(the Prime Minister)'.[22] Under Article 146 of the Constitution, the Council of Ministers shall conduct the internal affairs and foreign policy of the Republic of Poland and manage the government administration. The tasks of the Council of Ministers include, *inter alia*, ensuring the internal and foreign security of the state and maintaining public order. These tasks are carried out by the administration with the essential role of the services, administratively subordinated to the Council of Ministers with a leading position of the Prime Minister. According to Article 13 of the ABW Act, the Prime Minister may issue instructions and request information from the Heads of the ABW, the AW and the CBA as well as from the Minister of Defence who supervises the military services, i.e. the SKW and the SWW. Moreover, the Prime Minister may request information about all planned operations and actions that were taken to ensure the necessary level of cooperation between the services (Article 13(6) of the ABW Act). The scope of competence of the Prime Minister is thus extensive and related to the issuing of administrative acts.

The Minister-Coordinator of the Intelligence and Security Services is also a key element of the system of control and supervision of the services. He or she fulfils the tasks of the Prime Minister in this domain, if appointed.

In contrast, the powers of the President are narrow. His or her role is mostly consultative – the President is responsible for providing opinions on various procedures concerning the services. However, the President is the most important recipient of information obtained by the services. These institutions are obliged to provide him or her with information whenever he or she decides so.

The judiciary controls the legality of the services' activities, especially in the area of operational activities. The judiciary is empowered to draw consequences in the event of the misuse of the rules on operational activities (identification of unlawfulness). The courts evaluate the evidence collected during the preparatory proceedings by the public prosecutor's office in cases against service officers who have committed violations. In addition, it is the ordinary court that decides whether the services are entitled to conduct their activities, in particular operational activities.

Actions carried out by the officers are evaluated, from the perspective of their legality, by the prosecution, having powers resulting from the Code of Criminal Proceedings. In this respect, the prosecutor's office, supervised by the General Prosecutor, is entitled to a full spectrum of control and supervisory tools concerning investigative as well as operational activities undertaken by the services.

---

[22] P. Burczaniuk, *System nadzoru i kontroli nad służbami specjalnymi w Polsce – stan obecny na tle analizy prawno-porównawczej wybranych państw. Postulaty* de lege ferenda [Supervision and Control System of Intelligence and Security Services in Poland – State of Play with the Comparative Law Analysis of Selected Countries: *De Lege Ferenda* Proposals], [in:] *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, P. Burczaniuk (ed.), Warszawa 2017, p. 30.

Attention should be drawn to the fact that the civil society and its organisations may exercise control over the services using the right of access to public information under the terms of the Act of 6 September 2001 on access to public information.[23] [24]

1.5. Legal Status of the Officers

In describing the legal status of service officers in Poland, it should be pointed out that given the nature and importance of the tasks performed by these services, the legislator has shaped the legal relationship between an officer and a given service according to specific principles, differentiating it from other forms of employment based on labour law or civil law.

As B. Skowronek points out, 'the legal relationship of a person serving in a uniformed formation is considered to be of a public-law nature (more precisely – administrative law). It is a relationship between an officer and a given uniformed formation. The creation of the functional relationship, its change, and termination are based on administrative decisions (orders). Orders issued by the administrative authorities have the character of unilateral legal acts, the content of which is determined by the provisions of the Code of Administrative Procedure, the so-called service pragmatics (i.e. laws regulating the creation and functioning of uniformed services) as well as executive acts issued on their basis'.[25]

The pragmatic provisions of the intelligence and security services regulate in detail: the conditions and procedure of admission to service, the course of service, the prerequisites for dismissal from service, the principles of disciplinary liability as well as the entitlements of officers concerning their salaries and other service-related benefits. In principle, an officer's relationship with the service is established by way of appointment, through the issuance of a personnel order which specifies the date of entry into the service and the position in the service. Such an order is therefore an administrative decision. Similarly, all significant changes in the scope of this functional relationship connected, *inter alia*, with a change of the duty station, official position, change of remuneration or termination of this relationship, are specified in personnel orders.

---

23 Journal of Laws of 2022, item 902.

24 See R. Klejc, Szef ABW jako podmiot zobowiązany do udostępnienia informacji publicznej w trybie ustawy z dnia 6 września 2001 o dostępie do informacji publicznej na tle dotychczasowej praktyki orzeczniczej sądów administracyjnych [The Head of the ABW as an Entity Obliged to Share Public Information under the Act of 6 September 2001 on Access to Public Information within the Case-Law of Administrative Courts], [in:] Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego, P. Burczaniuk (ed.), Warszawa 2021, pp. 271–295.

25 B. Skowronek, *Charakterystyka stosunku służbowego funkcjonariuszy ABW ze szczególnym uwzględnieniem analizy fakultatywnych i obligatoryjnych przesłanek zwolnienia ze służby na podstawie wybranych orzeczeń sadow administracyjnych* [Characteristics of the Functional Relation of ABW Officers with Particular Consideration of the Analysis of Optional and Obligatory Grounds for Dismissal from Service on the Basis of Selected Administrative Court Judgments], [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (ed.), Warszawa 2021, pp. 249–250.

What is important, these orders benefit from guarantees allowing for the judicial control of their legality. The control is exercised by the Provincial Administrative Courts and the Supreme Administrative Court, under the provisions governing the administrative court proceedings.

As far as the military services are concerned, there are also soldiers of the Armed Forces of the Republic of Poland army who perform service in these institutions, whose status, also shaped by personnel orders, is similar to that of non-military officers.

Moreover, it should be added that the competence acts of the services allow for the employment of civilian employees (under the Labour Code), but their positions are of exclusively auxiliary nature – they cannot exercise the powers reserved for officers.

2. STATUTORY TASKS AND POWERS OF THE INTELLIGENCE AND SECURITY SERVICES

The scope of powers assigned to service officers varies. In the case of the ABW, under Article 21 of the ABW Act, within the limits of the tasks, discussed earlier, the officers are responsible for:

- Intelligence gathering (operational activities) and investigatory activities in order to identify, prevent and detect offences and prosecute their perpetrators
- Intelligence gathering as well as analytical-information activities in order to obtain and process information important for protecting the security of the state and its constitutional order.

Moreover, the ABW performs its activities on the order of the court or prosecutor, within the scope defined in the Code of Criminal Proceedings[26] and the Code of Execution of Criminal Sentences.[27]

The AW officers, following Article 22 of the ABW Act, within the scope of the tasks referred to in Article 6, carry out intelligence gathering and analytical activities.

In the case of the CBA, under Article 13 of the CBA Act, the CBA officers shall undertake:

- intelligence gathering activities in order to identify, prevent and detect offences, and also investigative activities, if needed, to prosecute perpetrators of offences
- intelligence gathering activities, analytical-information activities and control activities in order to detect cases of corruption in state institutions and local self-government as well as cases of abuse by persons performing public functions, and also activities detrimental to the economic interests of the state.

[26] Act of 6 June 1997 – the Code of Criminal Proceedings, Journal of Laws of 2021, item 534.
[27] Act of 6 June 1997 – the Code of Execution of Criminal Sentences, Journal of Laws of 2021, item 53.

Like the ABW, the CBA performs activities on the order of the court or prosecutor within the scope defined in the Code of Criminal Proceedings and the Code of Execution of Criminal Sentences. As R. Brzozowski points out, 'since the ABW and the CBA are both empowered in the area of criminal prosecution, the model of functioning of both these formations is described as a mixed intelligence-police model. Thus, apart from typically intelligence tasks, these services have powers characteristic for law enforcement and investigative bodies'.[28]

In the case of military services, the SKW officers, under Article 25 of the SKW and the SWW Act, within the scope of the tasks referred to in Article 5, carry out intelligence gathering and analytical-information activities as well as tasks under the Act of 5 August 2021 on the protection of classified information.[29]

It should be noted that, as opposed to the ABW and the CBA, officers of the SKW do not have investigative powers. The SWW, under Article 26 of the SKW and SWW Act, gathers the intelligence and undertakes analytical-information activities. Importantly, since the legislator allowed soldiers to perform service in military services, which was indicated earlier, under Article 24 of the SKW and the SWW Act, they were granted rights analogous to the officers.

2.1. The Investigatory Powers

As indicated above, the officers of the ABW and the CBA have investigatory powers. These powers may be defined as the competence to exercise, within the scope of their competence, procedural actions upon a request issued by the court or public prosecutor, in accordance with the Code of Criminal Proceedings and the Code of Execution of Criminal Sentences. In particular, such actions may be carried out in the course of preparatory proceedings initiated on the basis of the information gathered by the services referred to above.

2.2. The Intelligence-Gathering Powers

It may be said that, historically, this type of powers has always been the core of the intelligence and security services. Nonetheless, the Polish legal doctrine points out that the intelligence-gathering activities have not been defined yet. In the course of fulfilling their statutory tasks, each service entitled to exercise such actions defines the essence and detailed operating procedures of such actions in internal, classified legal acts. Only the most complex types of intelligence-gathering powers are governed by the universally binding legal acts, with regard to their purposes, legal and factual bases and the mode of operation.

---

[28] R. Brzozowski, *Czynności wykonywane przez funkcjonariuszy ABW na tle zadań ABW* [The Activities of the ABW Officers in the Light of the ABW's Tasks], [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (ed.), Warszawa 2021, p. 146.

[29] Journal of Laws of 2019, item 742.

They include operational control, the controlled purchase of goods, the controlled giving or accepting of material benefits, the acquisition and processing of telecommunications data and cooperation with agents (HUMINT).[30]

2.3. The Analytical-Information Powers

Along with the intelligence gathering powers, the analytical-information activities constitute one of the fundamental aspects of fulfilling the tasks of the intelligence and security services. The legislator laid down some form of a definition of the said powers in Article 5(1)(4) of the ABW Act which stipulates that the ABW is responsible for acquiring, analysing, processing and providing to the competent authorities information which may be of vital importance for the protection of the internal security of the state and its constitutional order (whereas in the case of the AW, the legislator refers to the information which may be of vital importance for the security and international position of the Republic of Poland and its economic and defensive potential, and in the case of the CBA, a reference is made to information concerning phenomena identified within its scope of competence). The Polish legal doctrine points out that 'it seems reasonable to conclude that exercising such information tasks by the Head of the ABW [and the heads of the other intelligence and security services – P.B.] is the essence of the ABW's actions, i.e. informing the constitutional organs of the executive about threats to the internal security of the state and its constitutional order'.[31]

2.4. Powers in the Area of ICT Security

The ABW's tasks in this domain are the most comprehensive and wide-ranging among all the Polish intelligence and security services. First, this organ identifies offences of espionage and terrorism committed with the use of ICT instruments.

Second, on the basis of the Act on the anti-terrorist activities, the legislator assigned to the ABW the tasks of identifying, preventing and detecting threats to the security of the IT systems vital for the functioning of the state, used by the public administration bodies and forming part of the critical infrastructure (Article 5(1)(2a) of the ABW Act). It can be added that in accordance with the legal act mentioned above, the ABW gained new, wide-ranging powers in the area of ICT security, such as:

- assessing the security of the ICT systems (Article 32a of the ABW Act)
- issuing requests to provide information on the architecture, functioning and rules of exploitation of the ICT systems (Article 32b of the ABW Act)

---

30 S. Hoc, P. Szustakiewicz, *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz* [A Commentary to the Act on the Central Anti-Corruption Bureau]. LEX/el.2012, Article 13.

31 P. Burczaniuk, *Zadania Szefa ABW w zakresie obowiązków informacyjnych* [The Tasks of the Head of the ABW in the Area of Information and Analysis], [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (ed.), Warszawa 2021, p. 20.

- applying to the court for blocking the accessibility of specified ICT data or ICT services connected with terrorist incidents in the IT systems (Article 32c of the ABW Act)
- keeping a register of incidents threatening the security of the ICT systems (Article 32d of the ABW Act)
- issuing recommendations in order to raise the levels of security of the ICT systems (Article 32e of the ABW Act).

Third, according to the Act of 5 July 2018 on the national cybersecurity system,[32] the Government Computer Security Incident Response Team (CSIRT), run by the Head of the ABW, was set up as a part of this system. It operates on the national level. The CSIRT is tasked with the coordination of handling ICT security incidents, in particular the incidents identified in the systems used by the public administration bodies. By virtue of this act, the ABW is entitled to run the early warning system identifying threats on the internet.

2.5. Tasks in the area of the Protection of Classified Information

Under the Act on the protection of classified information, the ABW and the SKW shall supervise the system of the protection of classified information in Poland. In this regard, according to the ABW Act, this institution is responsible for preventing and detecting crimes against classified information and exercising tasks of the national security authority in the area of the protection of classified information in international relations. The SKW carries out the same tasks in the military domain.

2.6. Tasks in the Area of International Cooperation

The heads of the intelligence and security services (the ABW, the AW, the SKW, the SWW and the CBA) are entitled, within the scope of their competence, to cooperate with competent foreign authorities and services in order to fulfil their tasks. As far as the ABW, the AW and the CBA are concerned, such cooperation may be initiated upon previous approval of the Prime Minister, whereas in case of the SKW and the SWW the Prime Minister, prior to granting such approval, is obliged to consult the Minister of Defence.

2.7. Tasks in the Area of the Protection of Personal Data

In accordance with the Act of 10 May 2018 on the protection of personal data,[33] the provisions of which apply to the protection of individuals with regard to the processing of personal data to the extent specified in Articles 2 and 3 of the General Data Protection Regulation (GDPR), its provisions and the said Regulation shall not apply to the activities undertaken by the intelligence and security services. As pointed out in the explanatory memorandum

[32] Journal of Laws of 2020, item 1369.
[33] Journal of Laws of 2019, item 1781.

to this act, the legislator decided to define the extent to which the provisions governing the protection of personal data apply to the area of national security. The Polish legislation does not contain a fixed catalogue of actions which are considered to fall within the scope of the notion of 'national security'. According to the legislator, the decision whether or not certain activities should be considered as falling within the scope of this definition should be taken after a meticulous analysis of each individual case by the controller or by the processor.[34] This issue is discussed further in the chapter by M. Nowiński.

[34] Explanatory Memorandum to the Government's Draft Act on the protection of personal data, https://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2410

CHAPTER XVI

Romania

Eduard Raul Hellvig

1. POSITION OF THE SRI IN THE DOMESTIC LEGAL SYSTEM

1.1. Legal Definition of Special Services

All Romanian intelligence services share the following features[1]:

- They are organised and operate under the law and are financed from the central state administration budget.
- They have a military organisational structure and are part of the national defence system.
- Their activity is coordinated by the Supreme Council of National Defence, which is informed through annual reports or whenever necessary.
- They collaborate with each other and with other state authorities in order to achieve their own missions, while third party institutions are obliged, within the legal competencies, to provide support in fulfilling the attributions stipulated by the law.
- Their activity is overseen by Parliament.
- With the approval of the Supreme Council of National Defence, they can establish relations and ratify cooperation agreements with similar foreign organisations.
- The intelligence activity aimed at achieving national security is classified as state secret.
- The staff of the intelligence bodies and of the entities in charge of national security cannot be members of parties or of other political or secret organisations and shall not be used for political purposes.
- The people who have been found guilty of acts contrary to the fundamental human rights and freedoms cannot work within the intelligence services.

---

[1] Article 8 of Law No. 51/91 on the National Security of Romania, republished, with subsequent amendments and supplements.

- The personnel of the intelligence bodies and of the structures in charge of national security shall be bound to preserve the state and professional secret, including after leaving active service in any way.

1.2. Position and Role of the Service in the Public Administration System

The Romanian Intelligence Service is the state body specialised in intelligence relevant for the national security of Romania, a component of the national defence system, whose activity is organised and coordinated by the Supreme Council of National Defence.[2]

According to the National Defence Strategy for 2020–2024,[3] Romania's national security is the outcome of the coherent and coordinated action taken by the state on several levels of strategic action, which, according to the specialty of the relevant public institutions, define the dimensions of achieving security as well as the perception of the latter by citizens, first of all, but also by the public institutions, by the international public opinion, and by the allies and partners our country. All the activities carried out and the actions undertaken within the range of these dimensions define the national security as the general state of the Romanian society.

The intelligence activity for achieving national security goals shall be conducted by the Romanian Intelligence Service, the state body specialised in handling internal intelligence matters, the Foreign Intelligence Service, the state body specialised in obtaining data relevant for the national security from abroad, and the Protection and Guard Service, the state body specialised in ensuring the protection of Romanian and foreign dignitaries during their stay in Romania as well as the security of the offices and residences thereof.

In order to carry out its tasks, the Romanian Intelligence Service collaborates with the Foreign Intelligence Service, the Protection and Guard Service, the Ministry of National Defence, the Ministry of Internal Affairs, the Ministry of Justice, the Public Ministry, the Ministry of Foreign Affairs, the Ministry of Economy and Finance, the General Directorate of Customs as well as with the other public administration bodies. These bodies are required to provide one other with support with a view to fulfilling the tasks stipulated by law.

1.3. Scope of Activities of the Service

According to Law No. 51/1991,[4] the national security of Romania means the state of lawfulness, balance and social, economic and political stability that is necessary for the Romanian national state to exist and develop as a sovereign, unitary, independent and

[2] Article 1 of Law No. 14/1992 on the Organisation and Operation of the Romanian Intelligence Service, with subsequent amendments and supplements.
[3] Approved by Parliament Decision No. 22/2020.
[4] Law on the National Security of Romania, republished, with subsequent amendments and supplements.

indivisible state, to maintain the rule of law as well as the climate needed for the unimpeded exercise of the fundamental rights, freedoms and duties of citizens, pursuant to the democratic principles and rules stipulated by the Constitution.

National security is achieved by acquiring knowledge of, preventing and eliminating the internal or external threats that may cause damage to the national security values mentioned above.

As an expression of their loyalty to the country, Romanian citizens shall have the moral duty to contribute to the achievement of national security.

The following constitute threats to Romania's national security:

- the plans and actions aimed at suppressing or undermining the sovereignty, unity, independence or indivisibility of the Romanian state
- the actions aimed, directly or indirectly, at provoking war against the country or a civil war, facilitating foreign military occupation, enslaving to a foreign power or assisting a foreign power or organisation to commit any of these deeds
- treason by helping the enemy
- armed actions or any other violent actions aimed at weakening the state power
- espionage, transmission of state secrets to a foreign power or organisation or to the agents thereof, illegal procurement or holding of state secret documents or data with a view to transmitting them to a foreign power or organisation or to the agents thereof or for any other purpose, unauthorised by law, as well as disclosure of state secrets or negligence in storing them
- undermining, sabotage or any other actions that aim to remove by force the democratic institutions of the state or that seriously harm the fundamental rights and freedoms of Romanian citizens*) or may damage the defence capability or other similar interests of the country as well as the acts aimed at destructing, deteriorating or bringing into disuse the structures necessary for the proper unfolding of the social and economic life or the achievement of national defence
- the actions that threaten the life, physical integrity or health of the persons holding important state positions or of the representatives of other states or of international organisations, whose protection must be ensured during their stay in Romania, according to the law, the treaties and conventions concluded as well as to international practice
- initiation, organisation, perpetration or assistance provided in any way to the totalitarian or extremist actions of communist, fascist, legionary or of any other origin, racist, anti-Semitic, revisionist, separatist actions that may endanger in any way the unity and territorial integrity of Romania as well as incitement to deeds that may endanger the rule of law
- terrorist acts, as well as the initiation or support provided in any way to any activities whose purpose is the perpetration of such deeds

- attacks perpetrated by any means against a community
- unauthorised removal of weapons, ammunition, explosive or radioactive, toxic or biological materials from the units authorised to hold them, the smuggling thereof, the manufacturing, possession, alienation, transport or their use under conditions other than those provided for by the law as well as the illegal bearing of weapons or ammunition, if such deeds endanger national security.
- initiation or establishment of organisations or groups, or joining or supporting them in any way, with a view to performing any of the activities provided for in para. a) to k), as well as the covert performance of such activities by organisations or groups established pursuant to the law.
- any actions or inactions that harm the strategic economic interests of Romania, those that result in jeopardising, illegally managing, degrading or destroying natural resources, forestry, hunting and fishing funds, water and other such resources, as well as establishing monopoly on or blocking access to them, with consequences at national or regional level.

The state bodies in charge of national security are the following: the Romanian Intelligence Service, the Foreign Intelligence Service, the Protection and Guard Service as well as the Ministry of National Defence, the Ministry of Internal Affairs and the Ministry of Justice, through dedicated internal structures.

In situations that pose threats to the national security, the Romanian Intelligence Service, through personnel assigned for this purpose, shall carry out activities specific to intelligence gathering that involve restricting the exercise of certain fundamental human rights and freedoms, which are performed according to the procedure provided for in Law No. 51/1991, with subsequent amendments, which is applied accordingly.

The operational personnel of the Romanian Intelligence Service shall carry out their activity in an overt or covert manner, as required by the needs of achieving national security.

The Romanian Intelligence Service shall ensure protection and employment in other units or labour compartments of the operational personnel who, while working undercover, are exposed under circumstances that exclude their guilt.

1.4. Control and Supervision of the Service

The activity relevant for achieving national security is organised and coordinated by the Supreme Council of National Defence.

The activity of the Romanian Intelligence Service is subject to parliamentary oversight. Every year or when the legislative body decides so, the Director of the Romanian intelligence Service submits to Parliament reports on the fulfilling the attributions incumbent on the Romanian intelligence Service, under the law.

A joint committee of the two Chambers of the Parliament shall be set up in order to exercise actual and permanent oversight.

The organisation, operation and ways of exercising oversight shall be established by Parliament Decision No. 30/1993.[5]

The Committee oversees the fulfilment by the Romanian Intelligence Service of the tasks incumbent on it, under the legal provisions in force, and performs an actual and permanent control of the activities carried out by the Romanian Intelligence Service.

With a view to fulfilling the tasks assigned to it, the Committee asks the Romanian Intelligence Service, through its director, for reports, intelligence briefings, accounts, documents, data and information and may hear persons in connection with the analysed issues.

The Romanian Intelligence Service is bound to make available to the Committee, within seven working days, the reports, intelligence briefings, accounts, documents, data and information requested and to allow the hearing of the military and civilian personnel indicated by the Committee.

The Committee may be notified *ex officio* on those actions that could impact on or raise suspicions about the lawfulness of the activity of the Romanian Intelligence Service.

1.5. Legal Status of the Officers

The staff of the Romanian Intelligence Service shall consist of permanent military personnel and civilian employees who fulfil operational and administrative tasks.

The military personnel of the Romanian Intelligence Service enjoy all the rights and responsibilities provided for the Romanian armed forces military by the legal provisions, the military statutes and regulations.

Civilian employees are subject to the stipulations of the Labour Code and other legal and statutory provisions of the Romanian Intelligence Service.

The people who committed abuses when working for the repressive structures of the totalitarian state, the informers and collaborators of the Securitate, as well as former communist party activists who are guilty of acts directed against fundamental human rights and freedoms are not allowed to work within the Romanian Intelligence Service.

The selection, enlistment, appointment to ranks and promotion to higher rank and positions, transfer, retirement, cessation or termination of the employment contract are done according to the law, the Rules of Procedure of the Romanian Intelligence Service, the statutes of the corps of officers, military foremen and non-commissioned officers and other legal provisions.

---

[5] Decision on the Organisation and Operation of the Joint Standing Committee of the Chamber of Deputies and the Senate for the Exercise of the Parliamentary Oversight of the Activity of the Romanian Intelligence Service, republished, with subsequent amendments and supplements.

According to Law No. 80/1995,[6] the active-duty military personnel is entitled to:

- a monthly salary, consisting of the salary determined by the military rank, the salary determined by the position held, a seniority-based allocation and benefits as well as to bonuses, awards, hazard pay and other monetary entitlements, whose rates shall be determined by the government's decision
- equipment, food, healthcare assistance, medication, lodging provided free of charge as well as to paid vacation and medical leave, under the conditions set by the government's decision
- tax or rent reductions or exemptions, aids and other entitlements, according to the regulations in force
- free transportation, under the conditions set by the government's decision
- funding granted by the Romanian Intelligence Service to cover the military staff's legal representation in the event of deeds committed in the exercise of their duties, under the law, pursuant to the order of the Director of the Romanian Intelligence Service.

According to GO No. 26/1994,[7] in times of peace, the personnel of the Romanian Intelligence Service is entitled to food allowance, pursuant to the provisions of this ordinance.

According to Law No. 223/2015,[8] the right to pensions and social security granted to military, is guaranteed by the state and is be exercised pursuant to this law through the state military pension system.

According to GO No. 121/1998,[9] material liability shall be incurred, under this ordinance, in the event of damage related to the set-up, administration, and management of the financial and material resources that are caused by the military through their own fault and in connection with the fulfilment of the military service or their duties within the military institutions they work for.

2. TASK AND MANDATE

2.1. Investigative Powers

In case a flagrant offence against the national security regime laid down by law, a terrorist attack or act or attempts, or preparatory acts to commit such offences are found, if punished under the law, the Romanian Intelligence Service personnel may detain the perpetrator,

6 Law on the Status of Military Staff, with subsequent amendments and supplements.
7 Government Ordinance on the Food Allowance Granted, in Times of Peace, to the National Defence, Public Order and National Security Personnel and to People Held in Custody, republished, with subsequent amendments and supplements.
8 Law on Military Pensions, with subsequent amendments and supplements.
9 Government Ordinance on the Material Liability of Military Staff, with subsequent amendments and supplements.

handing them over immediately to the relevant judicial bodies together with the statement of findings and the evidence.

Upon the request of the relevant judicial bodies, duly designated staff of the Romanian Intelligence Service may provide support in carrying out certain criminal investigation activities into crimes against national security.

The criminal prosecution bodies shall be bound to provide the Romanian Intelligence Service with any data or information relevant for national security that resulted from the criminal investigation activity.

The bodies of the Romanian Intelligence Service may not carry out criminal investigation acts, enforce the measure of detention or remand and have their own detention facilities.

2.2. Intelligence Gathering

According to Law No. 14/1992 on the Organisation and Operation of the Romanian Intelligence Service, with subsequent amendments and supplements, the SRI organises and carries out activities aimed at collecting, checking and turning to good account the information necessary with a view to acquiring knowledge of, preventing and thwarting any actions that, under the law, pose threats to the national security of Romania.

In this regard, through its units, the Romanian Intelligence Service:

- carries out intelligence and technical activities aimed at preventing and countering terrorism
- carries out counter-terrorist interventions at the facilities attacked or occupied by terrorists, in order to capture or annihilate the latter, set hostages free and restore law and order. Counterterrorist interventions are conducted with the approval of the Executive Bureau of the Romanian Intelligence Service
- ensures antiterrorist protection of Romanian and foreign dignitaries as well as of other officials, according to the norms set out by the Supreme Council of National Defence.

The Romanian Intelligence Service shall contribute to ensuring the counter-terrorist protection of dignitaries guarded by the Protection and Guard Service when they are the targeted by terrorist threats.

The Romanian Intelligence Service acts to detect and thwart the actions aimed at initiating, organising or establishing on Romania's territory of intelligence structures that may cause damage to national security, the activities of joining or supporting such structures in any way, or the unlawful manufacturing, holding or use of means of communications interception, as well as the activities of collecting and disseminating secret or confidential information.

With a view to establishing the existence of threats against national security, provided for in Article 3 of Law No. 51/1991 on the National Security of Romania, with subsequent amendments, the intelligence services may, under the law, carry out checks by:

- requesting and obtaining items, written documents or official information from public institutions or authorities and, respectively, from legal entities of private law or from natural persons
- asking for expert advice
- receiving notifications or information reports
- documenting certain relevant operational stages by photographing, videotaping or by any other technical means or personal findings regarding activities carried out in public places, if not performed systematically
- obtaining the data generated or processed by the providers of public electronic communications networks or by the providers of publicly available electronic communications services, other than their content, and stored by the providers in question under the law.

The dedicated laboratories and experts of the Romanian Intelligence Service shall make findings ordered or requested under the law.

According to Law No. 535/2004,[10] the SRI is the national authority in preventing and countering terrorism. Through the Centre for Operational Anti-Terrorist Coordination (CCOA), the SRI is in charge of the technical coordination of the National System for Preventing and Combating Terrorism (SNPCT), while the Supreme Council of National Defence acts as a strategic coordinator.

To prevent and combat terrorist acts, the public authorities and institutions that are members of the SNPCT shall perform specific activities, either individually or in cooperation, pursuant to their legal powers and competences and to the provisions of the General Protocol on the Organisation and Operation of the Supreme Council of National Defence.

The Romanian Intelligence Service is the national authority in the field of Air Marshals on board aircraft and for intelligence exchange purposes relevant to their activity.

In order to prevent terrorist acts on board civilian aircraft registered in Romania or owned by air carriers licensed by the Romanian state, the Romanian Intelligence Service assigns and coordinates air marshals on board aircraft, in compliance with the national security policy or the obligations undertaken by Romania through the international acts that it is part of.

The ministries and the other public authorities and institutions entitled to enforce the provisions of this law are required to notify the Romanian Intelligence Service with regard to the natural and legal persons that are suspected of having committed or favoured terrorist acts in any way.

---

[10] Law on Preventing and Countering Terrorism, with subsequent amendments and supplements.

In case of an imminent or actual terrorist act on the country's territory, at the proposal of the director of the Romanian Intelligence Service, the Supreme Council of National Defence may issue a decision on declaring the terrorist crisis situation.

In case of an act of terrorism, the Romanian Intelligence Service, through its specialised unit, performs counter-terrorist intervention, independently or in cooperation with other authorities and public institutions, throughout the country, with a view to releasing hostages, capturing or annihilating terrorists, neutralising the devices they use, freeing the attacked or occupied facilities as well as re-establishing law and order.

The counter-terrorist intervention is subject to approval by the Supreme Council of National Defence. By way of exception, in case of imminent casualties or significant damage, when the Supreme Council of National Defence cannot be urgently convened, the execution of the counter-terrorist intervention shall be approved by the president of the Supreme Council of National Defence.

The public authorities and institutions may transfer the operational control to the Romanian Intelligence Service, upon the latter's request.

The counter-terrorist intervention and the transfer of operational control are performed according to the Methodology elaborated by the Romanian Intelligence Service following consultation with the relevant SNPCT institutions, approved by decision of the Supreme Council of National Defence.

2.3. Analytical Tasks

The Romanian Intelligence Service is authorised to hold and use adequate means for obtaining, checking, processing and storing information relevant for national security, under the law.

2.4. Administrative Tasks

In order to ensure its logistics, the Romanian Intelligence Service:

- elaborates and substantiates the draft budget of the Romanian Intelligence Service, which consists of its own budget administered by the chief authorising officer and the budgets of the units with legal personality administered by third-party authorising officers, ensures the financing of its units, coordinates and oversees the administration, earmarking, and use of the funds, as approved through the state budget law, by the authorising officers under its command
- approves, within the remit of its competences, the technical and economic documentation for its own investment works, and monitors the execution thereof within the set deadlines
- performs activities consisting of the import and export of equipment and technology specific to the intelligence activity and of the provision of appropriate technical assistance, under the law

- establishes norms on the use, maintenance and repair of weapons, equipment and other assets as well as consumption norms for ammunition and other materials
- sets out norms on material and financial provision, reimbursement, evidence and oversight of the material and monetary means necessary to the subordinated units
- exercises any other powers conferred by law.

The Romanian Intelligence Service is equipped with the weapons, ammunition, and combat equipment necessary to carry out the defence and counterterrorism missions, the transport of secret correspondence, its own guard and other service tasks.

The funds necessary to carry out the activities within the Romanian Intelligence Service are ensured as follows: from the state budget, from extrabudgetary revenues, from external credits, and from other legally constituted sources.

The buildings, means of transport, technical equipment, and the other material means necessary to the Romanian Intelligence Service are provided by Government decision or are purchased under the law.

The plots of land and the buildings where the Romanian Intelligence Service carries out its activities are the public property of the state. The Romanian Intelligence Service receives and administers the public and private property of the state and is able to rent it according to its legal regime, keeping a 50% share of the rent charged as extrabudgetary revenues.

The Romanian Intelligence Service has its own fleet of means of transport for the central apparatus and the subordinated units, which is provided for in the endowment charts of the units, as approved by the director of the Romanian Intelligence Service.

2.5. ICT Security

As regards the relationship with the providers of publicly available electronic communications, the National Centre for Interception of Communications within the Romanian Intelligence Service has been designated to obtain, process and store information relevant for national security.

2.6. Protection of Classified Information

The SRI safeguards the state secret and prevents the leakage of information whose disclosure is prohibited under the law.

With a view to enforcing the legal provisions relevant for safeguarding the state secret, the Romanian Intelligence Service organises and performs the transport of the official correspondence that is assigned that classification level throughout the territory of Romania.

According to Law No. 182/2002,[11] the general coordination of the activity and the control of the measures concerning the protection of state secret information is carried out by a dedicated unit within the Romanian Intelligence Service.

In this regard, the Romanian Intelligence Service, fulfils the following main tasks:

- It elaborates the national standards for classified information and their implementation objectives, in cooperation with the public authorities.
- It supervises the activities undertaken by public authorities in order to enforce this law.
- It provides expert advice on the programmes aimed at preventing the leakage of classified information that are drafted by public authorities and institutions, self-managed public companies and trading companies holding such information.
- It checks the manner in which the legal norms regarding the protection of classified information are observed and enforced by the public authorities and institutions.
- It conducts on-site checks and reviews the programmes aimed at protecting classified information.
- It cooperates with the National Registry Office for Classified Information and with the National Security Authority on all matters related to the enforcement of this law.
- It provides support for the setting of facilities and places of particular importance for the protection of classified information, at the request of the heads of public authorities and institutions, of economic operators and legal persons governed by private law, and submits centralised records to the government for approval.
- It organises and is responsible, under the legal provisions, for the collection, transport and distribution across the country of the state secret correspondence and of the restricted official correspondence, in compliance with the provisions of the law.
- It analyses and establishes measures in connection with the complaints and suggestions regarding the implementation of the programmes for the protection of classified information.
- It ascertains any infringement of the norms on the protection of classified information, applies the penalties provided for by the law and notifies the criminal investigation bodies of any offences.

[11] Law on the Protection of Classified Information, with subsequent amendments and supplements.

CHAPTER XVII

Slovakia

Michal Aláč

1. POSITION OF THE SERVICE IN THE DOMESTIC LEGAL SYSTEM

1.1. Legal Definition of Special Services

The legal order of the Slovak Republic does not provide a legal definition of the term 'intelligence service' or 'special service'. Taking into account several definitions of legal theories, intelligence service can be defined in the Slovak Republic as a state body that conducts intelligence activities and performs intelligence tasks. The main task of intelligence services is to obtain and analyse information related to the state's security and other relevant interests and subsequently pass it on statutory recipients, i.e. state bodies that use this information in the state-power decision-making process. In short, therefore, intelligence service can also be defined as a state body responsible for obtaining and evaluating information and then passing it on its statutory recipients.[1]

1.2. Position and Role of the Services in the Public Administration System

Intelligence services of the Slovak Republic are a specific type of state bodies of the Slovak Republic that collect and evaluate information in the performance of tasks related to the constitutional system, internal order, security of the state, protection of foreign policy and the economic interest of the state or intelligence provision for the defence, defence capability of the Slovak Republic, as far as the Military Intelligence is concerned.

The Slovak intelligence services do not have executive powers; they are not law enforcement authorities. Their role is to provide information support to the authorities with

[1] Aláč, M. (2015). *Získavanie informácií na spravodajské účely a na účely trestného konania*, pp. 2–3. ISBN: 9788089603329.

executive powers. The activities of the intelligence services as well as information provided to the external environment are subject to secrecy and are non-public.[2]

The intelligence services of the Slovak Republic have a purely intelligence character, they do not have the status of a law enforcement authority and do not participate directly in criminal proceedings. They do, however, provide information of an operational character to the law enforcement authorities.

The Slovak intelligence community is composed of the Slovak Information Service and the Military Intelligence.

The main tasks of the Slovak Information Service and the Military Intelligence under the legal order of the Slovak Republic include, in particular, intelligence activities, which involve obtaining, accumulating and evaluating information on the subject of intelligence interests as well as security activities, the essence of which is the implementation of measures of a security character. Intelligence services also carry out tasks arising from the Slovak Republic's international obligations, tasks carried out within the framework of international intelligence cooperation as well as tasks laid down by special laws.[3]

Intelligence activities are also carried out by other state authorities within the scope of their competence, namely the Police Corps, the Criminal Office of the Financial Administration and the Prison and Judicial Guard Corps, but they cannot be classified as intelligence services.[4]

1.3. Scope of Activities of the Services

Within the security system of the Slovak Republic, it is possible to identify the civilian intelligence service – the Slovak Information Service, which is the only representative of the civilian intelligence of the Slovak Republic, and the military intelligence service – the Military Intelligence, which is the only representative of the military intelligence focus of the state.

The Slovak Information Service

The Slovak Information Service was established by the Act of the National Council of the Slovak Republic, No. 46/1993 Coll. on the Slovak Information Service (hereafter referred to as 'the Act on the Slovak Information Service'), which defines its tasks, statues, organisation, system of external control by the National Council of the Slovak Republic,

---

2 Kočan, Š. and Selinger, P. (2013). *Bezpečnostné služby v Slovenskej republike*, p. 150. ISBN: 978-80-8054-555-0.

3 § 2 of the Act of the National Council of the Slovak Republic, No. 46/1993 Coll. on the Slovak Information Service and § 2 of the Act of the National Council of the Slovak Republic, No. 198/1994 Coll. on the Military Intelligence.

4 Aláč, M. (2015). *Získavanie informácií na spravodajské účely a na účely trestného konania*, p. 19.

duties and powers. The Slovak Information Service is a general security and intelligence service of the Slovak Republic.

The Slovak Information Service is 'a state body of the Slovak Republic which shall fulfil tasks in the protection of the constitutional establishment, public order, security of the State and interests of the State concerning the foreign policy and economy to the extent circumscribed by this Act. It shall conduct activities in accordance with the Constitution, constitutional laws, regular laws, and other universally binding legal regulations.'[5]

The main tasks of the Slovak Information Service under the Act on the Slovak Information Service include obtaining and analysing information on:

- activities threatening the constitutional establishment, territorial integrity and sovereignty of the Slovak Republic
- activities directed against the security of the Slovak Republic
- activities of foreign intelligence services
- organised criminal activity
- terrorism, including information on involvement in terrorism activities, their funding and/or supporting
- political and religious extremism, violent extremism and harmful sectarian groups
- activities and threats within the cyberspace if they pose a threat to the national security
- illegal international smuggling and migration of people
- matters potentially capable of seriously threatening and/or inflicting damage upon the economic interests of the Slovak Republic
- threats and/or disclosure of information and matters protected according to special regulations or international agreements, or international protocols.[6]

As regards the remit of the Slovak Information Service regarding the foreign intelligence, the service 'shall collect, accumulate and analyse information on activities arising abroad which are directed against the constitutional establishment and security of the Slovak Republic and information necessary for the implementation of its interests concerning foreign policy.'[7]

The security activities of the Slovak Information Service are carried out through the implementation of so-called appropriate security measures when necessary to protect the object of the service's intelligence interest (i.e. to prevent activities or threats to information of interest to the service) or to implement the foreign policy interest of the Slovak Republic.

---

5 § 1, para. 2 of the Act of the National Council of the Slovak Republic, No. 46/1993 Coll. on the Slovak Information Service.

6 § 2, para. 1 of the Act of the National Council of the Slovak Republic, No. 46/1993 Coll. on the Slovak Information Service.

7 § 2, para. 2 of the Act of the National Council of the Slovak Republic, No. 46/1993 Coll. on the Slovak Information Service.

The main task of the Slovak Information Service is to obtain and analyse information that is legally defined and then to transmit it to the external environment to the relevant recipients (state authorities), in order to use this information in the state-power decision-making process in the area of competence of the recipient. The provision of the information support is primarily directed to the National Council of the Slovak Republic, the President of the Slovak Republic and the government of the Slovak Republic, including its members, to whom the Slovak Information Service provides information necessary and relevant for their activities and decision-making. The Slovak Information Service provides information on criminal activities (in particular on the commission of organised crime) to the Police Corps and Prosecutor's office. The Slovak Information Service also provides necessary information to other state authorities when they need it to prevent unconstitutional or other unlawful activity. Intelligence information shall be provided solely for the fulfilment of the stated purpose.

The President of the Slovak Republic, the President of the National Council of the Slovak Republic (Parliament) and the Prime Minister of the Slovak Republic have a special status of recipients, in relation to whom the Director of the Slovak Information Service is obliged to provide, within a specified period and to the required extent, the information requested in writing by any of them.

The provision or withholding of certain information to an external environment is subject solely to the discretion of the Slovak Information Service, which is limited by the statutory purpose for which the information is provided. At the same time, the decision to dicelose information to an external environment is constrained by the Act, according to which the Slovak Information Service carries out a security assessment before disclosing information in the context of the possibility of a threat to the interests that could be jeopardised by the disclosure of the intelligence information to the external environment. If the security assessment results in a conclusion that the performance of a specific task under the Act on the Slovak Information Service and sources of the Slovak Information Service could be exposed or that the identity of its officers or persons acting for the Slovak Information Seivice could be exposed, and the consequences of not disclosing that information are not manifestly more serious that the conseauence of disclosing it, the legal barrier to the disclosure of the information in question to the external environment in accordance with the Act on the Slovak Information Service is met and the information will not be provided.

The Slovak Information Service's intelligence activities are based on the principles of an integrated state intelligence model, i.e. they include external intelligence and technical intelligence.

In order to achieve the objectives of intelligence activities, the Act on the Slovak Information Service authorises the use of so-called special means, namely technical intelligence means and operational intelligence means. The Slovak Information Service is also

authorised to use special financial means for the performance of its tasks, to use special means of disposal of the state's property, to ensure the protection of its members who, on the territory of the Slovak Republic or abroad, exercise their rights and duties in accordance with the law in the performance of the tasks of the Slovak Information Service, to possess dangerous substances and prohibited items and also to use intelligence covert entities, which contribute to the effective and covert obtaining of intelligence information in a risky operational environment. The Slovak Information Service may exercise these invasive powers and means only strictly in accordance with and within the scope of legally permissible resrictions on the rights and freedoms of citizens, and therefore their exercise is subject to the control provided for by law.

In relation to the subject of intelligence interest, the following area can be outlined in accordance with the Strategie Direction of the Slovak Information Service (a document defining the priorities of the Slovak Information Service's intelligence and information activities). In the area of security, the Slovak Information Service focuses in particular on assessing security risks in the fight against terrorism, organised crime and criminal activities threatening the foundation of the Republic and its security, extremism, illegal migration, the legalisation of proceeds of criminal activities and illegal trade in arms and dual-use items. In the economic field, the Slovak Information Service monitors, in particular, wasteful and fraudulent use of the state's and local government's property, corruption and clientelism in the state and the local government, serious tax and customs fraud and the threats to the energy security of the Slovak Republic. In the field of foreign security, the Slovak Information Service focuses mainly on crisis and conflict regions and on the possible consequences of emerging security and economic crises abroad for the interests of the Slovak Republic, its security and economy. In the area of intelligence security, the Slovak Information Service pays particular attention to threats to classified information, the activities of foreign intelligence services and participates in the process of conducting personnel and industrial security vetting.

The Slovak Information Service actively cooperates with partner intelligence services and international organisations in countering security threats to the common space shared by the Slovak Republic with the EU and NATO member states as well as in protecting the security of the international community.

In the performance of its tasks, the Slovak Information Service cooperates with central government authorities (Ministries) and other government bodies. In particular, the Slovak Information Service intensively cooperates with the Security Forces of the State, both at the level of departmental leadership, executive departments and inter-departmental structures (e.g. the Expert Coordination Body for the Fight Against Crime). The Slovak Information Service cooperates in particular with the Police Corps and its specialised units, the Military Intelligence, the Ministry of Interior of the Slovak Republic, the Ministry of Foreign and

European Affairs of the Slovak Republic, the Ministry of Economy of the Slovak Republic and the Nuclear Regulatory Authority of the Slovak Republic.

Cooperation between the Slovak Information Service and other Security Forces of the Slovak Republic has been intensified and made more effective by the establishment of the National Security Analytical Centre. The Centre is an analytical, communication and co-operation unit included in the structure of the Slovak Information Service. The main tasks of the Centre include the preparation of comprehensive analytical assessment of security incidents based, *inter alia*, on reports received from the state authorities of the Slovak Republic, monitoring the security situation in the Slovak Republic and providing analytical products on security threats in the Slovak Republic to the designated recipients. At the national level, the Centre brings together a number of subjects in the field of counter-terrorism and countering serious security threats.

Organisation of the Slovak Information Service

The Slovak Information Service is managed and represented in public by the Director of the Service who is accountable to the Security Council of the Slovak Republic for the performance of her or his duties. The Director of the Slovak Information Service is appointed and dismissed by the President of the Slovak Republic on the basis on a proposal of the government of the Slovak Republic. The Director of the Slovak Information Service is in the service employment relation to the Slovak Information Service. The President of the Slovak Republic decides on matters concerning the employment of the Director of the Slovak Information Service. At least once a year, the Director of the Service shall submit a report to the National Council of the Slovak Republic on the fulfilment of the service's tasks.

In relation to the Slovak Information Service, the Security Council of the Slovak Republic is authorised to impose tasks on the service. In peacetime, the Security Council of the Slovak Republic is an advisory body to the government of the Slovak Republic and participates in the creation and implementation of the security system of the state, the fulfilment of international obligations in the field of security and assesses the security situation in the Slovak Republic and in the world. The Security Council of the Slovak Republic has *nine* members and is chaired by the Prime Minister of the Slovak Republic. To prepare and carry out its tasks, the Security Council of the Slovak Republic establishes committees, namely the Foreign Policy Committee, the Defence Planning Committee, the Civil Emergency Planning Committee, the Intelligence Coordination Committee, the Energy Security Committee and the Cybersecurity Committee. The Slovak Information Service is represented in the Intelligence Coordination Committee (the Director of the Service is a member of the Committee), the Foreign Policy Committee and the Cybersecurity Committee (a Slovak Information Service's representative approved by the Security Council of the Slovak Republic and appointed by the Chairman of the Security Council of the Slovak

Republic is a member of these Committees). The Security Council of the Slovak Republic, through its chairman, may assign tasks, in written form, to the Slovak Information Service, within the scope of the Service. The Director is permanently invited to attend meetings of the Security Council of the Slovak Republic.

The Slovak Information Service is one of the initiators of the inter-departmental Expert Group for the Coordination in the Field of Counter-Terrorism at the national level, which operates under the Security Council's of the Slovak Republic Intelligence Coordination Committee. All key actors in the Slovak Republic involved in counterterrorism are represented in the Expert Group which coordinates the operational and analytical activities of the various state bodies in the field of counterterrorism.

The details of the focus, organisation and management of the Slovak Information Service are regulated by the Statue of the Slovak Information Service, and the Slovak Information Service's Organisational Regulations issued on its basis.

Military Intelligence

The Military Intelligence was created by the Act of the National Council of the Slovak Republic No. 198/1994 Coll. on the Military Intelligence (hereinafter referred to as 'the Act on the Military Intelligence'). The structure of the Military Intelligence was originally composed of two basic services, namely the Military Defence Intelligence Service – the Military Counter-Intelligence – and the Military Intelligence Service. In 2013, the Military Intelligence Service underwent a significant organisational change and these services were merged into one under the competence of the Ministry of Defence of the Slovak Republic. The Military Intelligence is 'an intelligence service that performs the task of intelligence provision for the defence, defence capability and security of the Slovak Republic within the competence of the Ministry of Defence of the Slovak Republic'.[8]

The tasks of the Military Intelligence are defined in Section 2 of the Act on the Military Intelligence, according to which the Military Intelligence performs tasks related to obtaining, accumulation and evaluation of information important for ensuring the defence and defence capability of the Slovak Republic on the territory of country and abroad, with a focus on activities threatening the sovereignty, constitutional establishment, independence, territorial integrity and defence capability of the Slovak Republic, the activities of foreign intelligence services, terrorism, cyber-terrorism, political extremism or religious extremism, harmful sectarian groups, organised crime and criminal activities against the defence of the Slovak Republic, illegal trade in defence industry products, weapons of mass destruction or dual-use items, activities and threats in cyberspace, illegal international transportation

[8] § l, para. 1 of the Act of the National Council of the Slovak Republic No. 198/1994 Coll. on the Military Intelligence.

of persons, facts which may seriously threaten or harm the military-economic interests of the Slovak Republic, threats or leaks of data containing classified information.

The Military Intelligence, like the Slovak information Service, implements appropriate security measures where necessary to prevent activities and threats.[9]

The Minister of Defence of the Slovak Republic provides the National Council of the Slovak Republic, the President of the Slovak Republic and the government of the Slovak Republic with information obtained by the Military Intelligence that is relevant to their decision-making and activities. Necessary information is also provided by the Minister of Defence of the Slovak Republic to other state authorities if they need it to prevent unlawful activities. The information obtained shall be provided solely for the purposes established by the Act.[10]

The Military Intelligence is managed by the Director who is accountable for the performance of his or her duties and the fulfilment of the tasks of the Military Intelligence to the Minister of Defence, who appoints and dismisses the Director from his or her post. The Minister of Defence of the Slovak Republic is required to submit a written report on the performance of the tasks of the Military Intelligence to the National Council of the Slovak Republic at least one a year.

The number of the Military Intelligence's staff is determined by the government of the Slovak Republic. The government of the Slovak Republic, on the proposal of the Minister of Defence, approves the Statute of the Military Intelligence, regulating its focus and organisation in more detail.[11]

1.4. Control and Supervision of the Services

Given the special position of the Intelligence Services in the security apparatus of the state and the nature of their, in some cases invasive, powers, the activities of the Slovak Information Service are also subject to external oversight by the legislative, the executive and the judiciary power. In addition, there are internal control mechanisms within the Slovak Information Service.

External oversight control of the Slovak Information Service

The external oversight of the Slovak Information Service is carried out *at the parliamentary level* through the Special Oversight Committee of the National Council of the Slovak Republic for the Oversight of the Slovak Information Service, composed of MPs from the

---

9 § 2, para. 2 of the Act of the National Council of the Slovak Republic, No. 198/1994 Coll. on the Military Intelligence.

10 § 2, para. 2, 4 and 6 of the Act of the National Council of the Slovak Republic, No. 198/1994 Coll. on the Military Intelligence.

11 §§ 3 and 4 of the Act of the National Council of the Slovak Republic, No. 198/1994 Coll. on the Military Intelligence.

political parties in the government and the political parties in opposition, and it is chaired by a representative of the opposition, as is customary; the Director of the Slovak Information Service also submits a report at least once a year on the fulfilment of the tasks set out in the law. The Parliament also plays a key oversight regulatory role, namely on approving the Slovak Information Service's budget.

In relation to the control exercised by the judiciary power, mention should be made in particular of the *ex ante* control of the use of technical intelligence means, which is subject to prior consent of the judge. The above-mentioned legal condition is related to the guarantee of fundamental human rights and freedoms under the Constitution of the Slovak Republic, according to which a right of freedom may be interfered with only in cases and in the manner proided for by law. At the same time, the provision of the Act on the Slovak Information Service cannot be disregarded, according to which a legal person or a natural person who operates a website or provides a domain name is obliged to prevent the operation of the website or access to the domain on the basis of a court order issued on the basis of an Slovak Information Service's request if the operation of such a website or domain is conducive to the dissemination of ideas supporting or promoting terrorism, political or religious extremism, extremism manifested in a violent manner or harmful sectarian groups.

In relation to the control exercised by *the executive power*, it should be mentioned that in the event of a violation of the Act on the Slovak Information Service, the Parliamentary Committee is obliged, according to the nature of the case, to inform, *inter alia*, the government of the Slovak Republic. The government also determines the total number of the Slovak Information Service's staff and approves the Statue of the Slovak Information Service. The Security Council of the Slovak Republic is also relevant, whose director is accountable to the Slovak Information Service for the performance of her or his duties. The fact that the Slovak Information Service's Director is appointed (and dismissed) based on a proposal from the government of the Slovak Republic cannot be overlooked.

The Special Oversight Committee of the National Council of the Slovak Republic for the oversight of the activities of the Slovak Information Service

One of the external oversight authorities is the Special Oversight Committee, through which the general parliamentary oversight of the Slovak Information Service's activities is carried out to the extent specified by the Act on the Slovak Information Service. It is an independent, permanent authority of the Parliament. Members of the Committee may only be members of the National Council of the Slovak Republic, and the members have the right to enter the Slovak Information Service's premises and facilities accompanied by the Slovak Information Service's officers.

Meetings of the Committee are not public and are held at least once a quarter. The Committee conducts deliberations in accordance with its Rules of Procedure, and any member

may request that the Committee is convened. Members of the Committee and other persons attending or being present at the deliberations of the Committee (after approval of their attendance by the members of the Committee) shall be bound to maintain the confidentiality of the facts of which they become aware at the deliberations and to observe the protection of classified information in accordance with special regulations.

In accordance with the Act on the Slovak Information Service, this Special Committee controls compliance with the law in the performance of the Slovak Information Service's tasks and discusses, in particular:

- the Statue of the Slovak Information Service
- the budget chapter of the Slovak Information Service for the following calendar year and the documents necessary for controlling the implementation of the budget
- internal regulations governing the focus and organisation of the Slovak Information Service, the conditions for the use of special means
- types and methods of record-keeping
- the service employment as laid down in a special regulation
- a report on the activities of the Slovak Information Service and its results
- proposals, complains and suggestions in the field of the Slovak Information Service.

If the Committee finds a violation of the Act on the Slovak Information Service in the exercise of its powers, it is obliged to notify the National Council of the Slovak Republic, the Attorney General of the Slovak Republic and, depending on the nature of the matter, the Committee shall also inform the government of the Slovak Republic.

Another committee in charge of controlling the activities of the Slovak Information Service is the Committee for the Protection and Security of the National Council of the Slovak Republic. This Committee carries out control of the use of technical intelligence means pursuant to the Act on Protection Against Interception.

Similarly to the Slovak Information Service, the parliamentary oversight of the Military Intelligence is carried out by the Special Oversight Committee of the National Council of the Slovak Republic for the oversight of the activities of the Military Intelligence to the extent specified in §§ 5 and 6 of the Act on the Military Intelligence.

Internal Control of the Slovak Information Service

The internal control of the Slovak Information Service shall be exercised in relation with all aspects of the Slovak Information Service's activities, both at the various levels of management and through a specialised control unit within the service with competence in all areas of the service's remit. Implementation of control activities, rights and obligations of control bodies and control entities are regulated by internal regulations that define the structure and organisation of the internal control system and the relations between them.

The Committee for the Control of the Use of Information-Technical Means

Pursuant to the Act on Protection Against Interception, a Committee for the Control of the Use of Information-Technical Means is to be established in the National Council of the Slovak Republic (the object of control activities will be the Police Corps, the Slovak Information Service, the Military Intelligence, the Prison and Judicial Guard Corps and the Financial Administration, i.e. the state bodies authorised to use information-technical means).

The Committee has *eight* members, three from the coalition and three from the opposition, the members are chosen in twos among the members of the Defence and Security Committee, the Slovak Information Service's Oversight Committee and the Military Intelligence Oversight Committee (special oversight committees). The remaining two members of the Committee shall be experts. The proposal shall be submitted to the National Council of the Slovak Republic by the chairman of the Parliamentary Committee for Defence and Oversight, after prior agreement with the chairman of the Special Oversight Committee for the oversight of the Slovak Information Service's activities. The prerequisites are the age of 40 years and a certificate from the National Security Authority for the Top Secret level, a second-level university degree and at least 10 years of experience (as judges, prosecutors or in the Police Corps, the Intelligence Service or in the legal and security or diplomatic field).

The Committee should carry out an inspection once a year, either on its own initiative, on the initiative of one of the above-mentioned committees or on the basis of a complaint from a citizen who believes that in interception means have been used against them.

The members of the Committee are entitled to request access to a special technical intelligence register (containing data on the type of means, the duration, the identity of the citizen against whom the means have been used, the reason for the use of the means etc.), to inspect the minutes of the destruction of the record, to enter the premises where the record and the record of the destruction of the record are located, to request the assistance of the competent state body, to take notes, extracts and copies, to use the information to draw up a record on the results of the inspection, which shall subsequently be submitted to the competent committee, together with the minutes of the discussion with the head of the state body. If, following the discussion of the protocol, the committee concerned finds a violation of the law in the use of the technical intelligence means, it shall inform the Chairman of the National Council of the Slovak Republic and submit the protocol to the Attorney General.

1.5. The Legal Status of the Personnel of National Security Services

Civil service regarding the Slovak Information Service officers

The Slovak Information Service officers perform activities of active duty that is vested in the state (the Slovak Republic). On entering the service employment, a citizen takes the oath of office, without which the civil service cannot be established.

I pledge allegiance to the Slovak Republic. I shall be an honest, brave and disciplined officer of the Slovak Information Service. I shall perform my official duties to the best of my ability and in my activities. I shall be guided by the Constitution, constitutional laws, laws and other generally binding legal regulations and I shall protect the constitutional order of the Slovak Republic as well as the rights of citizens. To this end, I am prepared to exert all my strength and abilities and to put my life on the line. This I swear!

The civil service of the Slovak Information Service officers, as well as legal relations connected with the establishment, changes and termination of civil service are regulated by the Act on the Civil Service of the Officers of the Police Corps, the Slovak Information Service, the Prison and Judicial Guard Corps of the Slovak Republic and the Railway Police. As can be deduced from the title, this regulation is common for various security forces.

A citizen of the Slovak Republic over 21 years old can become a Slovak Information Service officer, who applies for admission in writing and meets all legal requirements (is of a good character, reliable, meets the level of education required for the post to which he or she is to be appointed, is proficient in the national language, has permanent residence on the territory of the Slovak Republic, is not a member of a political party or a political movement on the date of admission to the civil service, has full legal capacity, ceases to be engaged in prohibited activities on the date of admission to the civil service).

In order to establish eligibility, applicants for the civil service in the Slovak Information Service have to undergo a medical examination, a psychological examination, a proficiency test in the national language, a physical fitness test (except for citizens who have reached the age of 50 years if male and 40 years if female).

A citizen who has validly been convicted for a deliberate criminal offence or who has validly been sentenced to an unconditional term of imprisonment is not considered to be of good character. In the admission process, integrity is proved by an extract from the criminal record. In the admission process, in order to prove integrity, the citizen provides necessary data for requesting an extract from the criminal record.

As reliable is not considered a citizen who demonstrably consumes alcoholic beverages in excess or ingests narcotic drugs, psychotropic substances or preparations capable of producing dependence on them, or otherwise does not warrant the proper performance of the civil service. For establishing reliability, a citizen may also be subjected to psychophysiological verification of truthfulness.

The condition of citizenship of the Slovak Republic and the other above-mentioned conditions have to be fulfilled by the Slovak Information Service officer throughout the entire duration of the service, unless the Act on the Civil Service stipulates otherwise. The basic extent of the rights follows on from the Act on the Civil Service that the Slovak Information

Service officers have throughout active duty, as well as the obligations that he or she is obliged to fulfil. The Slovak Information Service officer is obliged to respect the honour, esteem and dignity of his or her own as well as those of others and ensure that no person is harmed in relation with any of his or her activities which follow from the civil service.

The specific status is taken into account within the special social care, which is extracted from the general social insurance system and it forms a separate and organisationally self-independent system. Act No. 328/2002 on Social Security for the Police Officers and Soldiers regulates sickness security, accident security, retirement security and social security services of the Slovak Information Service officers, thereby it grants them a special employment status along with the officers of other security forces.

Another particularity is an exemption from military service of the Slovak Information Seivice officers subjected to conscription (only during the active duty in the Slovak Information Service) in time of an imminent danger or disruption of national security and when the constitutional authorities can declare a war, a state of war, state of emergency or state of extreme emergency under the conditions laid down in a Constitutional Act (Act on State Security in Times of War, a State of War, a State of Emergency and a State of Extreme Emergency).

The government of the Slovak Republic determines the total number of the Slovak Information Service officers.

The employment within the Slovak Information Service

Within the Slovak Information Service, besides the officers in the civil service, there are employees who also participate in the fulfilment of the service's tasks. The Labour Code and Act No. 553/2003 on Remuneration of Some Employees Performing Works of Public Interest regulate their employment within the Slovak Information Service.

The conditions of the Slovak Information Service employees' recruitment are similar to those for the Slovak Information Service officers.

Taking into consideration the specific tasks that the Slovak Information Service performs, the Act on the Slovak Information Service provides a general obligation, for the officers and anyone who performs tasks under this Act, to maintain secrecy with regard to facts which have come to their knowledge in connection with the activities of the Slovak Information Service and which, in the interest of natural or legal persons, have to remain secret. For the sake of completeness, it is necessary to mention that there is another legal form which regulates the handling of a sensitive information. It is the Act on the Protection of Classified Information. Given the fact that there is no position (office) to be performed without authorisation designated to be acquainted with classified information within the Slovak information Service, all officers and employees are obliged to have such authorisation and they have to meet the legal requirements of the protection of classified

information. The security clearance establishes whether the requirements are met. The requirements have to be fulfilled during the entire period of the validity of the certificate for classified information according to the classification level (Top Secret for 5 years, Secret – 7 years, Confidential – 10 years). The certification's validity issued on the basis of the security clearance (conducted by the service itself, not by the National Security Authority) ceases to be valid on the date of termination of employment or similar employment, including service employment.

2. TASKS AND MANDATE

2.1. Investigative Powers and the Role in Criminal Procedures

As already stated, the intelligence services of the Slovak Republic are only of intelligence character, which means that they are not law enforcement authorities and, therefore, they do not have investigating powers. In order to achieve a set criminal proceedings' goal, in specific cases, however, cooperation between the law enforcement authorities and intelligence services is inevitable. The intelligence forces of the state are authorised, in the process of obtaining significant information for criminal proceedings, to apply special authorisations and means that are described in more detail in the following subchapter. These means allow for gaining and analysing the information effectively, and subsequently this information is helpful for the criminal proceedings to detect, investigate, register and supress criminal activities.[12]

2.2. Intelligence Gathering

It is possible to say that information gathering, which makes up the intelligence cycle together with the evaluation and processing of information by the intelligence service, is one of the most important and difficult parts of the intelligence cycle and is the essence of the intelligence activity itself. There are several ways of gathering information. The Slovak Information Service uses the following sources of intelligence: HUMINT (intelligence using human sources), MASINT (intelligence via technical resources), SIGINT (signal intelligence), OSINT (open-source intelligence) and FININT (financial intelligence).

As mentioned earlier, the Slovak Information Service is authorised to use special means (operational intelligence means and technical intelligence means) through which information is obtained within operational intelligence activities in the first place.

The category of operational intelligence means includes surveillance of individuals and things, legally authorised alias documentation, the use of individuals who act for the benefit of the Slovak Information Service (or the Military Intelligence), covert replacement of things and simulated transfer of the ownership of things. The legally authorised alias documentation

[12] Aláč, M. (2015). *Získavanie informácií na spravodajské účely a na účely trestného konania*, p. 44.

is documents and items the purpose of which is to hide the true identity of the officer. Cards of members of the National Council of the Slovak Republic and ministers of the government of the Slovak Republic, service cards of judges and prosecutors, cards of editors-in-chief, editors, presenters, employees and the assistant staff of the periodical press or other mass media must not be used as legally authorised alias documents. A person who acts for the benefit of the Slovak Information Service (or the Military Intelligence) is a natural person who is older than 18 and is engaged in the voluntary and undercover provision of services to the Slovak Information Service (or the Military Intelligence). The law sets forth the persons who cannot be the person acting for the benefit of the Slovak Information Service (or the Military Intelligence). Covert replacement of things is the replacement of an item that causes no greater damage than the omission thereof would. The simulated transfer of the ownership of things consists in simulating the purchase, sale or other type of transfer of a thing on the basis of a previous written approval of the judge. The Slovak Information Service is required to keep a record on how operational intelligence means are used.

The second category of special means is technical intelligence means. The Slovak system of law regulates this domain through a special Act on Protection Against Interception. Technical intelligence means are some of the most important and dependable instruments of obtaining intelligence for the purpose of fulfilling operational duties.

Technical intelligence means are mainly electro-technical, radio-technical, photo-technical, optical, mechanical, chemical and other technical means or equipment, or their sets, used covertly to search for, open, examine and evaluate mail and other transported postal items, learn about the content of the messages transmitted over electronic communication networks, including eavesdropping on phone communications, and make audio, audio-visual and other recordings.[13]

As this measure is of invasive character, technical intelligence means can only be used as necessary in democratic society to protect the Constitution, internal order, foreign political interests, security and defence of the state, obtain information from foreign sources, prevent and solve crimes and protect the rights and freedoms of others when it would be substantially more difficult or ineffective to reach this objective otherwise. When a technical intelligence means is used, fundamental rights or freedoms may only be restricted as necessary and for no longer than is deemed necessary to achieve the legally accepted purpose.[14] Technical intelligence means can only be used on the basis of a prior written approval of a legitimate judge and for a required time which must not exceed 6 months

[13] § 2, para. 1 of Act No. 166/2003 Coll. on the Protection of Privacy Against the Unauthorised Use of Technical-Intelligence Measures and on Amendment and Supplementation of Certain Laws (Act on Protection Against Interception).

[14] § 3, para. 1 of Act No. 166/2003 Coll. on the Protection of Privacy Against the Unauthorised Use of Technical-Intelligence Measures and on Amendment and Supplementation of Certain Laws (Act on Protection Against Interception).

provided that other statutory couditions have been met.[15] The Slovak Information Service may also use technical intelligence means outside the Slovak Republic when they are used in the scope of tasks according to special regulations.

Other methods of obtaining information include:

- Obtaining data that are subject to privacy of telecommunications[16]: the content of the messages transmitted, the information about the communicating party (the phone number, the business name and the headquarters of a legal person, the business name and the place of business of a self-employed person, the personal data of a natural person, that is, the name, the sumame, the degree and the permanent address), the traffic data and the localisation data.
- Obtaining data that are subject to tax secrecy[17]: access by the Slovak Information Service to data that are subject to tax secrecy is regulated by the law on the administration of taxes (the tax law), according to which the reporting or accessing tax secrets to the Slovak Information Service for the purpose of fulfilling its duties is not classified as a breach of tax secrecy.
- Obtaining data that are subject to banking secrecy[18]: the Slovak Information Service has access to such data under the Act on Banks.
- Obtaining data that are subject to secrecy of correspondence[19]: the Slovak Information Service has access to these data under the Act on Postal Services, according to which items subject to secrecy of correspondence are accessed to the Slovak Information Service for the purpose of fulfilling its duties on the basis of a written request and by a court order.
- Obtaining assistance, underlying documentation and information from state and other authorities, as well as legal and physical persons, that may help clarify the facts considered important for the fulfilment of duties.[20] In the fulfilment of its statutory duties,

---

15 § 4 of Act No. 166/2003 Coll. on the Protection of Privacy Against the Unauthorised Use of Technical Intelligence Measures and on Amendment and Supplementation of Certain Laws (Act on Protection Against Interception).

16 § 117, para. 1 of Act No. 452/2021 Coll. on Electronic Communications.

17 Information on the tax subject obtained during tax administration.

18 The subject of banking secrecy is all information and documents on the matters of a client of a bank or a branch of a foreign bank that are not publicly available, in particular information on their transactions, account balances and deposit balances. Pursuant to the Act on Banks, a bank and a branch of the Slovak Information Service shall, at the written request of the Service and without the consent of the client, provide a report on matters concerning the client that are subject to banking secrecy for the purpose of conducting security vetting pursuant to the Act on The Protection of Classified Information. In addition to the above-mentioned, the Slovak Information Service is also entitled to request the mentioned information for the purpose of fighting organised crime and terrorism.

19 The subject of the secrecy of correspondence may be: 1) information and data on postal consignment and postal services already provided or being provided in relation thereto, except for information of a statistical nature which does not reveal who the consigner or consignee was, 2) the content of correspondence, 3) the content of other postal consignments.

20 § 15 of the Act of the National Council of the Slovak Republic, No. 46/1993 Coll. on the Slovak Information Service

the Slovak Information Service cooperates with state and non-state authorities, legal and physical persons[21] and has the right to access and obtain information and personal data from the information Systems of public-power authorities – these data are provided and accessed without the consent of the person concerned and such a person is not notified of the fact that their data have been accessed or provided. Public-power authorities are obliged to grant the request by the Slovak Information Service to access or provide information/personal data from their information systems.[22]

- Obtaining information through cooperation that is subject to a contractual legal regulation. Such information may, for instance, include information obtained through cooperation with a special unit of the Police Force's financial police service (the Financial Intelligence Unit) as part of the fulfilment of duties in the area of protecting against laundering proceeds of crime and financing terrorism. The Financial Intelligence Unit provides the Slovak Information Service with all information and underlying documentation that has been acquired under the law on protecting against laundering proceeds of crime and financing terrorism so that the Slovak Information Service can fulfil its statutory duties in combatting terrorism and organised crime.

These methods of obtaining information are an analogy to using special means. The Slovak Information Service uses them operationally to support its goals.

2.3. Analytical Tasks

Analytical activities are the key element of information processing. More generally, analytical activities are part of all processes of obtaining and processing information, and of decision-making in the framework of intelligence activities and the entire intelligence cycle, which consists of the following fundamental activities:

- planning intelligence activities – setting tasks
- gathering information
- processing the information and making intelligence products
- providing the intelligence products to recipients and getting feedback from the recipients.

Regarding its content, the analytical activity is a process of performing analysis by continually evaluating and analysing the information obtained, processing the information for the recipient, providing the information to the recipient in a standardised format and

[21] § 16 of the Act of the National Council of the Slovak Republic, No. 46/1993 Coll. on the Slovak Information Service.

[22] § 15, para. 2 of the Act of the National Council of the Slovak Republic, No. 46/1993 Coll. on the Slovak Information Service.

mediating the feedback and information requests for the information source or the intelligence service unit that gained the information.

The analytical activity takes place at three closely connected levels (operational, tactical and strategic).

At the operational level, the primary selection of information (who, what, how, where, when and why) is carried out. The entity, the activity, the modus of the activity, the place, the time and the motive are identified. These primary data are checked for accurateness and completeness. The information is systemised – identification data are assigned to it for further processing and the information is verified. Other specific activities, such as the analysis of the operational environment, assessment of the source's dependableness, tasking the source and covering the source when the information is sent out, also take place at this level. This level includes continued analytical support throughout the operational activity.

The tactical analysis is based on the processing of information from a single type of source. It is focused on information indicating identifiable threat. It is sector-oriented and focused on development (security, economic, foreign political and social), e.g. in terrorism, organised crime, migration, cyber threats, hybrid threats etc. At the tactical level, the analysed information is already pre-processed, pre-verified and supplemented with information from other sources and databases at the level of the source unit.

The strategic analysis represents cross-sectional (i.e. more sectional) evaluation of the security situation from all available sources of information with an impact on national security (multisource analysis). Conceptual and more comprehensive analyses are made at this level, which are usually focused on the most serious security threats and risks, prognoses and scenarios of the further development of the security situation in a given area.

The analytical activity is a part of all key activities mediated by the information flow (they are also an important part of this flow):

- planning and tasking – the needs of the recipient (i.e. the information request)
- analysis of the operationally acquired information
- multisource analysis and processing of information for recipients
- feedback from recipients regarding the intelligence products.

2.4. Administrative Tasks

Intelligence services are actively involved in several types of administrative proceedings, specifically by providing information to administrative bodies that proceed on the matter in question. For instance, the Slovak Information Service provides opinions in proceedings to determine whether physical persons should be given a certain status (asylum proceedings, permanent or temporary residence proceedings or citizenship proceedings), proceedings to determine whether an entity is sufficiently reliable to perform certain activities, or in

licence and permission proceedings. In some cases, the service's opinions (statements) are binding for the administrative body that proceeds on the matter or determines the matter.

Just for completeness, it should be noted that the Slovak Information Service cooperates with the Ministry of Interior of the Slovak Republic in asylum proceedings when the Ministry of Interior of the Slovak Republic asks the Slovak Information Service (and the Military Intelligence) for an opinion to determine the asylum applications of applicants who are older than 14. In this case, both services will send their statements containing their approval or disapproval of the grant of asylum or subsidiary protection to the Ministry of Interior of the Slovak Republic within 20 days. In the statement, the Slovak Information Service and the Military Intelligence will assess the applicant's danger to the security of the Slovak Republic in terms of threats posed to the interest the protection of which is within the remit of the Slovak Information Service (or the Military Intelligence).[23] If either service denies the asylum/subsidiary protection claim in its statement, the Ministry of Interior of the Slovak Republic will not grant asylum or subsidiary protection to the applicant.[24]

The Act on Foreigners' Residence provides for a similar legal regime. Under this law, the police unit will ask the Slovak Information Service (and the Military Intelligence) for an opinion to determine the application for temporary residence or permanent residence submitted by third-country nationals who are older than 14. The services will send their negative statement within 15 days if they deny the claim. Within the scope of their authority, both services will take into account the interests of the state in their respective opinions.[25] If the statement contains the disapproval of the grant of temporary residence or permanent residence, the police unit will reject the application.[26]

The Slovak Information Service also participates in citizenship proceedings if the Ministry of Interior of the Slovak Republic asks for an opinion. In the citizenship proceedings, the Ministry of Interior of the Slovak Republic takes into account the public interest (especially the security aspect) and the opinions of the Police Force, the Slovak Information Service and other state bodies concerned.[27]

The Slovak Information Service cooperates with the Ministry of Economy of the Slovak Republic in licence and permission proceedings and gives its opinion, for instance, on applications for licences to trade in defence products, applications for licences to carry out mediation activities regarding these products, and applications for import/export licences.[28]

---

23 § 19a, para. 9 of Act No. 480/2002 Coll. on Asylum and Amendment of Certain Acts.

24 § 13, para. 4 of Act No. 480/2002 Coll. on Asylum and Amendment of Certain Acts.

25 § 125, para. 6 of Act No. 404/2011 Coll. on Residence of Aliens and Amendment and Supplementation of Certain Acts.

26 § 33, para. 3, point o) and § 48, para. 2, point h) of Act No. 404/2011 Coll. on Residence of Aliens and Amendment and Supplementation of Certain Acts.

27 § 8a, para. 3 of the Act of the National Council of the Slovak Republic, No. 40/1993 Coll. on the Citizenship of the Slovak Republic.

28 Act No. 392/2011 Coll. on Trade in Defence-Related Products and on Amendments of Certain Acts.

As for these areas of participation of the Slovak Information Service in administrative proceedings, it can be noted that the negative opinions are based on intelligence that certifies the negative information in respect of the person examined, which the originator of the intelligence (the Slovak Information Service) has at its disposal. This information is not part of the substantiation of the decision of the decision-making (administrative) body, because it is considered classified information. Yet it serves as the basis for the issuance of individual administrative acts by means of which the person concerned is held responsible via a negative statement. This procedure is absolutely necessary to ensure effective protection to the interests of the Slovak Republic and Slovak citizens.[29]

2.5. ICT Security

The security of technical devices as a component of the classified information protection is in general regulated by Act No. 215/2004 Coll. on the Protection of Classified Information (Act on the Protection of Classified Information) and relevant implementing regulation (National Security Authority Decree on the Security of Technical Devices). Under the above-mentioned legislation, only the certified technical devices given operational approval may be used for work with classified information. Regarding that domain, the competence of the National Security Bureau (the national authority for classified information protection) has been conferred to and the technical devices used within the operation of the Slovak Information Service are being certified and given operational approval by the Slovak Information Service itself. Any technical device that was given operational approval shall be operated in compliance with the approved security project and with the conditions specified in the certificate as well as with the guidelines on the use of the technical device. Similarly, the assessment of the security settings of system devices used within the area of Slovak Information Service's competences is performed by the Slovak Information Service itself.

As for the transfer of classified information by technical devices outside the protected areas, the classified information concerned shall be protected by an information protection encryption device in compliance with the above-mentioned Act and National Security Authority Decree setting out detailed arrangements regarding the encryption protection of information. In addition, the technical devices are safeguarded against a leakage of classified information through undesirable electromagnetic radiation in accordance with the security standards for protection from undesirable electromagnetic radiation (issued by the National Security Authority), defining also requirements for the technical devices used by the Slovak Information Service.

[29] Aláč, M. (2015). *Získavanie informácií na spravodajské účely a na účely trestného konania*, pp. 38–39.

The Slovak Information Service enjoys a specific position within the domain of security of technical devices, its competence being further governed by internal regulations on the protection of classified information processed and transferred by technical devices.

2.6. Protection of Classified Information

The protection of classified information within the competence of the Slovak Information Service is provided in compliance with the precepts laid down in the national law (Act on the Protection of Classified Information and relevant implementing regulations).

The Slovak Information Service enjoys a particular status in the domain of classified information protection, and the law confers it, within the specified framework, the status of national authority, i.e. that of the National Security Authority. Under the Act on the Protection of Classified Information, the Slovak Information Service director general has established specialised units for classified information protection and departmental encryption office. The units are involved in all domains of classified information protection (personnel security, administrative security, security of technical devices, encryption protection of information, physical security and building security). Specific tasks are carried out by the security employees holding valid certificates of having completed the security employee examination and valid authorisation by the Slovak Information Service's Director.

In the domain of personnel security, the Slovak Information Service performs a security clearance, if the nominee concerned is an officer or employee of the Slovak Information Service or applicant for admission into employment or state service within the Slovak Information Service. Moreover, the Slovak Information Service carries out security employee examinations and their re-examinations and issues certificates of having completed the security employee examination.

An analogous specific status is enjoyed by the Slovak Information Service in the domain of security of technical devices and of information protection encryption devices as well; as mentioned above, the Slovak Information Service gives operational approval and certifies technical devices used by the Slovak Information Service and certifies and gives operational approval to methods, systems and devices of information encryption protection for the protection of classified information of the Top Secret and Secret security classification levels intended for the provision of classified information to intelligence services of other states within the international cooperation. The information sharing between the Slovak Information Service and its partner intelligence services of other States is not performed through the central register (managed by the National Security Authority) or through the Slovak Information Service's register of classified information (the Slovak Information Service keeps separate registers for classified information transmitted or received within the international cooperation). The classified information sharing is conditional on the consent of the heads of the intelligence services concerned.

A specific regulation applies also to the handling of classified information containing intelligence findings originating within the competence of intelligence agencies (special provisions of the National Security Authority Decree on the Administrative Security).

To offer a comprehensive picture, there should be mentioned the cooperation with the National Security Authority as the national authority in the domain; The Slovak Information Service provides the National Security Authority, at the latter's request, with information on the security reliability of nominees from its records; performs security clearance, within the scope of its competences and at the request of the National Security Authority, on the reliability of nominees at the place of residence of the nominee, and provides information from these clearances to the National Security Authority; performs security clearance, within the scope of its competences and at the request of the National Security Authority, on the security of the environment in which the nominee lives and the occurrence of potential security risks, and provides the information from these clearances to the National Security Authority; and it provides, at the request of the National Security Authority, information reqiuired to determine the industrial security of entrepreneurs.

In compliance with the statutory and implementing regulations, the Slovak Information Service has issued, in the form of internal regulation, the list of classified information of the Slovak Information Service; the Slovak Information Service Director thereby defines (in compliance with the relevant government regulation) the information contents protected as classified information, specifying their security classification levels and substantiation of the need for their classification on the indicated levels (any originator of classified information shall, when creating it, specify its security classification level in conformity with the list).

Owing to the status of the Slovak Information Service and nature of its activities, all officers and employees of the Slovak Information Service are persons authorised to be acquainted with classified information; certainly, with respecting their real need learn more about classified information and taking into account their assignment, it is decided individually up to what security classification level the person concerned may get acquainted with classified information (the need-to-know principle is applied, i.e. persons are being acquainted with a specific scope of classified information only if the need to become familiar with it results from the performance of their service or employment duties).

2.7. International Cooperation

The international cooperation between intelligence agencies is an important tool in the domain of protection of relevant interests of states and in ensuring security to their citizens. Reflecting the above, the law has authorised the Slovak Information Service to cooperate in pursuing its missions with the authorities of similar missions and competences in other countries (i.e. intelligence agencies), as well as with international organisations.

The international cooperation must be understood as integral part of the activity of the Slovak Information Service as such. Concrete steps within the field of international cooperation (for instance, the establishment of new bilateral contact) are authorised by the Director General of the Slovak Information Service, well within his remit via application of traditional intelligence diplomacy tradecraft. The decision to initiate, or positively react to proposal of potential partner, lies with the director general. Further steps are regulated by internal, classified regulations.

The Slovak Information Service is trying to maintain balanced and fair partnership with intelligence agencies in the domains of common interest. The relations and cooperation have been developed furthest with the intelligence agencies of the US, the UK, France, Germany and neighbouring countries of Slovakia, especially those of the Visegrad Group countries. The Slovak Information Service has been actively participating in several international intelligence platforms and it has participated in an appropriate form within the framework of the EU and NATO. The Slovak Information Service is among the founding members of the international intelligence forum Middle European Conference (MEC), established in Amsterdam in 1994. Important tools for pursuing the international cooperation are the Slovak Information Service liaison officers operating abroad.

As for the priorities of cooperation within the international intelligence community, there could be mentioned the countering of international terrorism, illegal migration, arms proliferation (illegal traffic win the dual use items), extremism, operations of foreign intelligence agencies, and monitoring of evolution in crisis and conflict regions.

If one takes into account legal regulation, the Slovak Information Service is:

- Generally speaking, entitled to cooperate with public and private entities. However, the case of the cooperation with private entities is usually limited to the cooperation with domestic ones, the cases of the international cooperation are very rare.
- Concerning the international organisations, in certain cases (NATO, EU), the Slovak Information Service is obliged to cooperate. This obligation emanates directly from the character of both mentioned organisations and linked intelligence services platforms.

2.8. Personal Data Protection

In order to align the national legal order with the content of the Regulation (EU) of the European Parliament and of the Council of 27 April 2016, Act No. 18/2018 Coll. on Protection of Personal Data was adopted. However, when dealing with personal data, the Slovak Information Service is primarily governed by its status legal norm (the Act of the National Council of the Slovak Republic, No. 46/1993 Coll. on the Slovak Information Service).

In this regard, we would like to point out that on the basis of § 17, para. 9 of Act No. 46/1993 Coll., the application of the Personal Data Protection Act to the processing of personal data by the Slovak Information Service, to the records and information systems

maintained within the scope of the Slovak Information Service and to the disclosure of the data, is precluded. Moreover, that fact is explicitly expressed in the Data Protection Act, according to which the Data Protection Act does not apply to the processing of personal data by the Slovak Information Service.

The handling of personal data by the Slovak Information Service is governed by a special legal regime regulated in particular by Act No. 46/1993 Coll. However, the above-mentioned cannot be interpreted in a way that the handling of personal data by the Slovak Information Service is not subject to any legal restrictions under any circumstances.

The processing of personal data by the Slovak Information Service takes place solely in classified information systems, (i.e. in the legal regime of Act No. 215/2004 Coll. on the Protection of Classified Information). Unclassified information systems are not used for processing of personal data. The records of the Central Lustration Console, which contain personal data, are a special case. However, these records are not under the control of the Slovak Information Service, they are non-departmental records (the Ministry of Interior of the Slovak Republic, the Ministry of Foreign and European Affairs of the Slovak Republic) where the rights of the Slovak Information Service are at the 'read' level. The data extracted from these records are transferred to classified systems where they are subsequently processed.

For instance, it follows from § 17, para. 4 of Act No. 46/1993 Coll. that, if inevitable, the Slovak Information Service is authorised to process special categories of personal data (e.g. data on racial or ethnic origin, political opinions, religious beliefs etc.) in the performance of the tasks defined in this Act and for the purposes of the cooperation defined in this Act (including international intelligence cooperation) solely to the extent provided for by the Act on the Protection of Personal Data. Thus, when processing of personal data belonging to special categories, the Slovak Information Service is obliged to respect their extent given in the Data Protection Act.

A certain limitation in relation to the lawful operation of the records is also embodied in the limit according to which data on the behaviour of a person under the age of 14 must not be stored in the records.

In relation to the principles governing the handling of personal data within the scope of our service's activities, we state that the focus is always on ensuring the protection of personal data held within the scope of the Slovak Information Service, which is expressed in § 17, para. 3 of Act No. 46/1993 Coll. According to the Act, the Slovak Information Service shall ensure the protection of personal data processed in its information systems and records against disclosure, misuse, damage, unauthorised destruction, theft or loss.

Act No. 46/1993 Coll. creates a reasonable scope for the Slovak Information Service to obtain personal data and their subsequent processing in the records and information systems maintained within the Service's competences. One of the ways of obtaining personal

data is enshrined in § 15, para. 1, according to which the Slovak Information Service is entitled, within the scope of its competence, to request from the state or other authorities, legal entities or natural persons the provision of assistance, documents and information which may contribute to the clarification of facts relevant to the performance of the tasks provided for by this Act. In § 15, para. 2 of the cited Act, this authorisation is subsequently expressed in relation to Public authorities in such a way that, to the extent necessary for the performance of the tasks provided for by law, the Slovak Information Service has the right to access and provide information and personal data from information systems of the Public authorities, by which these data shall be provided and made available to the Slovak Information Service without the consent of the data subject, and these persons shall not be informed about the provision and disclosure of the data. The Public authorities shall comply with the Service's request to disclose and provide information and personal data from their information systems. The law also establishes the obligation of the state authorities to provide the Slovak Information Service with the requested assistance, documents and information, unless a specific law provides otherwise.

With regard to the collection of personal data, § 17, para. 5 of Act No. 46/1993 Coll. provides that the service is entitled to process personal data necessary for the performance of their tasks under this Act without the consent of the natural person concerned, to obtain the data from publicly available information sources or to obtain them under cover in another way or by another activity. When the performance of Service's tasks requires so, the Service may usefully pool or distribute the information systems and the created records.

The protection of data held within the competence of the Slovak Information Service is generally embodied in a way that, when the data held in the records are no longer necessary for the performance of the tasks laid down or when there is any other lawful reason for doing so, the Information Service is authorised to store the data in a way which prevents anyone, except for the Court, from having access to them.

§ 17, para. 1 of Act No. 46/1993 Coll., according to which, for the purposes of the performing tasks under this Act or a special act within the scope of its competence, the Slovak Information Service is entitled to create and operate information systems and to process there personal data of natural persons and data on matters or facts directly related to the performance of the tasks under this Act or the tasks under special acts, and to this extent the service is entitled to maintain information systems and records of such tasks, can be considered as a general provision concerning the management of personal data within the scope of the Slovak Information Service.

CHAPTER XVIII

Spain

Esperanza Casteleiro Llamazares

1. POSITION OF THE CNI WITHIN THE NATIONAL LEGAL SYSTEM

1.1. Nature, Legal Framework and Structure of the CNI

The main rule of law regulating the nature and the functions of the *Centro Nacional de Inteligencia* ('the CNI' or 'the service') is Act 11/2002 of 6 May regulating the Centro Nacional de Inteligencia (Act 11/2002), whose Section 1 defines it as follows:

> ***Article 1.*** *El Centro Nacional de Inteligencia*
> *The Centro Nacional de Inteligencia is the public institution responsible for providing the President of the Government and the Government of the Nation with information, analyses, studies or proposals that allow for the prevention and avoidance of any danger, threat or aggression against the independence or territorial integrity of Spain, its national interests and the stability of its institutions and of the rule of law.*

Nature

The Additional Provision 1 of Act 11/2002 envisages the CNI as a special public organisation included among those referred to under Additional Provision 10 of Act 6/1997 of 14 April on the Organisation and Operation of the State General Administration (LOFAGE). Following the abrogation of the LOFAGE, the CNI's regime was established in Additional Provision 18 of Act 40/2015 of 1 October regulating the Legal Regime of the Public Sector (Act 40/2015) that states:

> ***Additional Provision 18.*** *Legal Regime of the Centro Nacional de Inteligencia*
> *The administrative action of the competent organs of the Centro Nacional de Inteligencia shall be governed by the provisions of its specific regulations and, in*

matters compatible with its nature and functions which are not envisaged by them, by the provisions of this Act.

Act 40/2015 stablishes the general legal regime for the whole Spanish public sector. Therefore, the exception in the above-mentioned additional provision illustrates the legislator's intention to provide the service with specific legal status in order to allow it to efficiently perform the specific functions entrusted to it under Article 4 of Act 11/2002 (see below).

The CNI, in order to discharge its missions, has been provided with functional autonomy, legal personality and full capacity to act. Therefore, the CNI – regardless of the ministry under which the government may place it from an organisational point of view – will keep its legal specific nature and functional autonomy. At present, under Royal Decree 139/2020 of 28 January establishing the basic organisational structure of the ministerial departments, the CNI is organisationally under the Ministry of Defence, although Act 11/2002 establishes that its attachment may be changed. In fact, between 2011 and 2018, the CNI was under the Ministry of the Presidency.

The autonomy that the legislator pursued to grant to the CNI is also reflected in the specific legal regime regarding personnel, budget and hiring. In fact, Article 8.4 of Act 11/2002 establishes that, concerning its patrimonial and hiring system, the CNI may be subject to private law, which represents an exception among public organisations.

Therefore, irrespective of the undeniable contribution that the specific missions and functions of the CNI make to the defence of the state, the CNI is not an organisation included in the law enforcement agencies: its main goal and purpose is to produce intelligence to be provided exclusively to 'the President of the Government and the Government of the Nation'.

Moreover, it is worth emphasising that, unlike other countries in the area, in Spain, the CNI has a national and an international scope, since it assumes and covers domestic and foreign security responsibilities.

Rules and regulations that form the CNI legal regime

The legal framework that regulates the CNI is made up of the following rules:

- Act 11/2002 of 6 May regulating the Centro Nacional de Inteligencia.
- Organic Law 2/2002 of 6 May regulating prior judicial control of the Centro Nacional de Inteligencia.
- Royal Decree 436/2002 of 10 May establishing the organisational structure of the Centro Nacional de Inteligencia.
- Royal Decree 240/2013 of 5 April passing the personnel statute of the Centro Nacional de Inteligencia.

Within this legal framework, it should be emphasised, particularly Article 5.1 of Act 11/2002 of 6 May establishes the secret nature of the activities conducted by the CNI as follows:

> ***Article 5.*** *Activities of the Centro Nacional de Inteligencia*
> 1. *The activities of the Centro Nacional de Inteligencia as well as its organisation and internal structure, resources and procedures, personnel, facilities, data centres and databases, sources of information, and the information or data that could lead to the knowledge of the matters above, are classified information marked top secret or the highest classification level in accordance with the legislation regulating official secrets and International Agreements.*

Article 5.2, which enshrines the principle of collaboration and coordination with other Administrations, provides the following:

> 2. *If applicable, the Centro Nacional de Inteligencia shall maintain the necessary relations of cooperation and coordination with the rest of the Public Administration, for the proper discharge of its functions in accordance with the legislation in force in each case and preserving the legal protection of the activities of the Service.*

Structure

The structure of the CNI is governed by Royal Decree 436/2002 of 10 May that establishes the organisational structure of the Centro Nacional de Inteligencia. Under Section 1 of the Royal Decree, the CNI's organisation includes a Secretariat of State-Direction, a General Secretariat, three General Directorates dealing respectively with intelligence, support to intelligence and resources, and the correspondent jobs to be determined in the List of Job Positions. It is worth mentioning that the Secretary of State Director will appoint the holders of some positions having the rank of Deputy Director General as per the List of Job Positions. The reminding units and jobs will appear in the List of Job Positions.

The Secretary of State-Director, appointed by Royal Decree of the Government upon the proposal of the Minister of Defence, will be at the helm of the CNI. The Secretary of State-Director, apart from performing the direction and representation tasks established by Act 11/2002, acts as the National Intelligence and Counter-Intelligence Authority, presides over the National Cryptological Centre and is the Delegate National Authority for the protection of NATO/EU/ESA classified information (hereinafter referred to as 'the ANS-D'). Moreover, the Secretary of State-Director is part of the National Security Council and acts as the Secretary in the meetings held by the Government Delegate Commission for Intelligence Affairs, which ensures the appropriate coordination among all the information and intelligence services of the state.

1.2. Control and Oversight of the CNI

Article 2 of Act 11/2002 establishes that the CNI action will be governed by the principle of subjection to the legal system and to the oversight by the executive, the legislative and the judiciary, by means of four main mechanisms:

Oversight by the executive

The Government Delegate Commission for Intelligence Affairs (Section 6 of Act 11/2002) and the Ministry of Defence are responsible for the political oversight of the CNI.

The Delegate Commission for Intelligence Affairs is made up of members from several ministries and shall ensure the appropriate coordination of all the information and intelligence services of the state to form an intelligence community.

Notwithstanding the above, incumbents from other higher institutions and senior officials of the State General Administration may be summoned to Commission meetings as deemed necessary.

The functions of the Delegate Commission are listed in Article 6.3; they include, among others:

a) *To propose to the President of the Government the annual objectives of the Centro Nacional de Inteligencia that should be included in the Intelligence Directive.*
b) *To monitor and assess the development of objectives of the Centro Nacional de Inteligencia.*
c) *To enforce the coordination between the Centro Nacional de Inteligencia, the information services of the Law Enforcement Agencies and the civil and military administrations.*

Apart from the oversight by the Delegate Commission, the law provides for the oversight by the Ministry of Defence. This Ministry controls both the efficiency of the CNI's performance by evaluating the compliance of its goals and the appropriate use of the funds allocated to it (Article 8 of Royal Decree 593/2002 of 28 June developing the financial budgetary regime of the Centro Nacional de Inteligencia).

Parliamentary oversight

Parliamentary oversight is specifically provided for in Article 11 of Act 11/2002 of 6 May as well as in the Regulations of the Congress of 10 February 1982. This parliamentary oversight is carried out in three ways: the Oversight Commission of money allocations to reserved funds; questions and interpellations and appearances; and through the National Court of Auditors.

First, it should be highlighted that the Commission that supervises the money allocated to reserved funds, in the fulfilment of its duties, shall have access to the information on classified matters except for information related to the sources and means used by the CNI as well as information provided by foreign intelligence services or international organisations.

The members of the Commission are obliged to keep the information and documents received secret.

Concerning its composition and performance, it should be mentioned that the Chairman of the House presides the Commission and the content of the sessions and the deliberations shall be kept secret.

In the fulfilment of its oversight duties, the Commission 'shall have access to the Intelligence objectives annually established by the Government and to the annual report drafted by the Director of the Centro Nacional de Inteligencia on the assessment of activities, situation and fulfilment of objectives set for the previous period.'

Concerning the second way to oversee the CNI through interpellations, questions and appearances, all of them fall under the ordinary oversight by the legislative over the executive.

Judicial oversight

Article 12 of Act 11/2002 refers, as the preliminary judicial oversight is concerned, to Organic Law 2/2002 of 6 May, regulating preliminary judicial oversight of the Centro Nacional de Inteligencia.

Judicial oversight is exerted over those activities of the CNI affecting fundamental rights provided for in those articles of the Spanish Constitution (Articles 18.2. *Inviolability of Home* and 18.3. *Secrecy of Communications*), which require a legal warrant.

In order to fulfil the oversight, a judge of the Supreme Court (Chamber 2 for criminal matters or Chamber 3 for contentious-administrative proceedings) shall be elected and, through a reasoned decision, will authorise the warrant or not.

The CNI, apart from being subject to the preliminary judicial oversight, is also subject to the ordinary judicial control set out in Article 106 of the Spanish Constitution.

Article 106 of the Spanish Constitution establishes that 'The courts control the power to issue regulations and to ensure that the rule of law prevails in administrative action, and to ensure that the latter is subordinated to the ends which justify it.'

Economic-budgetary oversight

The economic-budgetary oversight is the responsibility of the Delegate Comptroller as established in Articles 157 and 158 of the Spanish Budget Act, Act 47/2003 of 26 November.

Royal Decree 593/2002 of 28 June regulating the economic budgetary regime of the Centro Nacional de Inteligencia, establishes in its Article 7:

Article 7. *Oversight Regime*

The Centro Nacional de Inteligencia shall be subject to permanent economic oversight with the aim of verifying that its economic-financial procedures comply with the principles of legality, economy, efficiency and effectiveness, and it shall be the responsibility of the Delegate Comptroller assigned to the CNI.

The General Comptroller of the State Administration shall inform the Delegate Comptroller assigned to the Centro Nacional de Inteligencia of the accounts to be submitted and the dates of issue under the Plan of audits and economic oversight actions.

After accomplishing their objective of improving the economic-financial techniques, the financial accounts shall be kept in the Delegate Comptroller's Office of the Centro Nacional de Inteligencia and only those accounts specifically requested shall be submitted to the General Comptroller of the State Administration.

The General Intervention Board of the State Administration (IGAE) is responsible for the permanent oversight in order to verify compliance with the appropriate regulations as well as compliance with the principles of good administration, budgetary stability and financial balance. The IGAE also audits and passes the annual accounts of the CNI prior to submitting them to the Court of Auditors. In the fulfilment of its duties, the IGAE shall draft the appropriate reports, including the audit report that the Secretary of State-Director submits to the Courts of Auditors through the IGAE. The action of the IGAE follows the principles of legality, economy, efficiency and effectiveness in accordance with the directions issued each financial year.

The last mechanism of budgetary oversight is the responsibility of the Court of Auditors which, as envisaged in Article 136 of the Spanish Constitution and Organic Law 2/1982 of 12 May, shall exert the external control of the economic-financial activity of the public sector and conduct the investigation of the accounting responsibility.

1.3. Legal Status of the CNI Personnel

Article 8.1 of Act 11/2002 establishes that the personnel of the Centro Nacional de Inteligencia, regardless of their professional background, shall be subject to a single statute of personnel applicable to all members, which shall be approved by the government. For this reason, the personnel of the CNI are considered 'statutory personnel'.

The legal regime of the personnel of the CNI is regulated by Royal Decree 240/2013 of 5 April, which passes the Statute for the Personnel of the Centro Nacional de Inteligencia (hereinafter referred to as 'the Statute'), and only when established by the specific legislation, in accordance with Article 4 of the Basic Statute of Public Employees, Legislative Royal Decree 5/2015 of 30 October, will this Basic Statute be applicable to the CNI.

The statutory personnel, despite being the gross of the personnel in the CNI, is one of the three legal regimes envisaged by the Statute.

Statutory personnel

The statutory personnel of the CNI are defined in Article 2 of the Statute that also establishes its legal regime, as it stipulates that: 'Statutory personnel of the CNI are those who, by virtue of appointment by the Secretary of State Director, once they have passed the selection process, are incorporated into the CNI with a statutory relationship of professional services, being paid from the general budgets of the State. These personnel, regardless of their origin, shall be subject to the provisions contained in this Statute and to the regulations issued for its development'.

The statutory relationship may be of a temporary or permanent nature. Temporary personnel shall be considered to be those who, by virtue of an appointment of this nature, hold this position in accordance with the provisions of this Statute. Permanent statutory personnel shall be those who, after serving on a temporary basis and fulfilling the requirements determined in this Statute, receive an appointment as permanent personnel.

The acquisition or loss of the consideration of statutory personnel is regulated in Title IV of the Statute, whose Article 6 enshrines the following general principles:

Article 6. *General Principles*

1. *Admission to the CNI shall be by means of the competitive examination system.*
2. *Likewise, to the extent that they are compatible with the provisions of Article 5 of Act 11/2002 of 6 May 2002 regulating the Centro Nacional de Inteligencia, the principles indicated below shall be guaranteed:*
   a) *Impartiality and professionalism of the members of the staff selection bodies.*
   b) *Independence and technical discretion in the actions of the staff selection bodies.*
   c) *Adequacy between the content of the selection processes and the functions or tasks to be performed.*
   d) *Agility, without prejudice to objectivity, in the selection processes.*
3. *Due to the aforementioned principle of confidentiality, the publicity of the calls for access to the CNI may be exempt.*

The requirements to take part in the selection processes are included in Article 7 of the Statute. It should be emphasised, with regard to the requirement of holding the Spanish nationality, that the principle of access to public employment by nationals of other European

Union member states in conditions equal to those of Spanish nationals is a principle that applies, as a general rule, to the rest of the public sector and does not apply to the CNI, in compliance with Article 8 of the Statute.

The causes for the loss of the status of statutory personnel are included in Article 28 of the Statute, which establishes:

> ***Article 28.*** *Causes for the Loss of the Status of Statutory Personnel*
> *The following are causes for loss of the status of statutory personnel:*
> *a) Resignation from the status of statutory personnel.*
> *b) The loss of Spanish nationality.*
> *c) The use of the previous nationality by those who have acquired Spanish nationality by option, letter of naturalisation or residence.*
>
> *Notwithstanding the foregoing, the Secretary General may authorise, for justified reasons, the use of another nationality.*
> *d) Failure to pass the suitability assessment period.*
> *e) Failure to accept the offer of permanent integration.*
> *f) Not being considered suitable for integration on a permanent basis.*
> *g) Failure to pass the tests established for the acquisition of the status of permanent statutory personnel.*
> *h) Voluntary retirement, forced retirement due to age or permanent incapacity for the service of the statutory personnel.*
> *i) The principal or accessory penalty of absolute or special disqualification for public office that has become final.*
> *j) The disciplinary sanction of separation from service and suspension of functions for a period of more than one year.*
> *k) Access to the condition of member of parliament or senator of the Cortes Generales, member of the legislative assemblies of the autonomous communities, member of the Government or of the governing bodies of the autonomous communities and local councils.*
> *l) Failure to request the transfer to active service within a maximum period of one month after the termination of the suspension of functions as a result of a criminal conviction.*
> *m) Failure to request the transfer to the active service situation before the end of the maximum period in the situation of leave of absence referred to in Article 45.*
> *n) Declaration of loss of the suitability that determined the access to the condition of permanent statutory personnel in accordance to Article 26.*

Rights and duties of statutory personnel are included in Title VII of the Statute. Article 48 provides a list of rights, which are:

Article 48. *Rights*

1. *The statutory personnel of the CNI shall be entitled to:*

a) *Remaining as permanent statutory personnel as a guarantee of objectivity, professionalism and impartiality, which should be the basis for their professional performance.*

b) *To be classified in the subgroup or group of professional classification corresponding to the position of initial assignment or to the one achieved by internal promotion.*

c) *To hold, under the conditions established in this Statute, one of the jobs in the professional classification subgroup or group in which they have been classified.*

d) *To effectively perform the functions or tasks inherent to their position in accordance with the progression achieved in their professional career and under the conditions set forth in this Statute.*

e) *To progress in the professional career according to the constitutional principles of equality, merit and ability through the implementation of objective and transparent evaluation systems.*

f) *To receive the remuneration that corresponds to them in accordance with the provisions of this Statute and the compensation for reasons of service to which they are legally entitled.*

g) *To participate in the achievement of the objectives attributed to the unit where they render their services and to be informed of the purposes, organisation and operation thereof and, in particular, of their hierarchical dependence and of the attributions, duties and responsibilities incumbent upon them.*

h) *Continuous training and permanent updating of their knowledge and professional skills, preferably during working hours and under the terms established in this Statute.*

i) *Respect for their privacy, sexual orientation, self-image and dignity at work, especially with regard to harassment on the grounds of sex, morality and work.*

j) *Non-discrimination on account of birth, race or ethnic group, sex or sexual orientation, religion or convictions, opinions, impairment, age or any other personal or social condition or circumstance.*

k) *The adoption of measures that favour the reconciliation of their personal, family and work life, in accordance with the provisions of this Statute.*

l) *Freedom of expression within the limits of the legal system.*

m) Personnel shall receive effective protection in matters of occupational health and safety

n) Vacations, breaks, leaves and licences established in this Statute.

ñ) Retirement in the terms and conditions established in the applicable regulation.

o) The social security benefits corresponding to the applicable regime.

p) The adoption of the measures foreseen in the applicable regulations in relation to female victims of gender violence.

2. Statutory personnel shall be entitled to receive protection and support from the CNI concerning their regular actions as members of the CNI and the CNI will be responsible for requesting the appropriate legal assistance in court in accordance with the provisions of the legislation on legal assistance to the State and public institutions.

Likewise, the Secretary of State Director will agree to offer legal assistance, if necessary, to senior officials and the rest of statutory personnel serving at the CNI in the course of legal proceedings that may arise from their actions in the fulfilment of their duties. Once authorised, legal assistance will include coverage of the corresponding fees of lawyers and solicitors, the pecuniary bonds that may be required in relation to the precautionary measures agreed by the competent judicial body, as well as the expenses arising from the proceedings and from gathering evidence at the request of the interested parties, whatever their status in the judicial process.

The CNI shall meet the civil liability and the patrimonial liability in which senior officials and the rest of the personnel serving at the CNI may have incurred as a result of actions or omissions that have been legitimately ordered and derived from the fulfilment of their duties, without prejudice to the provisions of Chapter II of Title X of Law 30/1992 of 26 November 1992 on the Legal Regime of the Public Administrations and Common Administrative Procedure.[1]

3. In the exercise of the rights and public freedoms recognised in the Constitution, statutory personnel shall abide by the limitations legally established in accordance with their status as members of the CNI.

Concerning the duties, Article 73 states that 'The statutory personnel of the CNI, in view of the mission and functions established in its regulatory Act, shall maintain the strictest neutrality towards politics and trade unions, adapting their actions and conduct, with regard to the provision of the service, to the higher national interest, acting above the criteria and interests advocated by social, political, economic or religious groups.'

[1] Following the abrogation of Law 30/1992 of 26 November, the provisions referred to are now established in Act 40/2015 of 1 October regulating the legal regime of the public sector.

Article 74 envisages the basic principles of conduct while Article 75 provides for the duty of secrecy and confidentiality that continues to be fulfilled by the statutory personnel even after they no longer hold this position. Article 75 states:

Article 75. *Duty of Secrecy and Confidentiality*

1. *The personnel of the CNI shall be obliged to maintain professional secrecy regarding the activities of the CNI, its internal organisation and structure, means and procedures, personnel, facilities, databases and data centres, sources of information and information or data that may lead to the knowledge of the foregoing matters, in accordance with their classification as secret by Article 5.1 of Act 11/2002 of 6 May regulating the CNI as well as regarding the existence and content of documents, identities, objects or elements related to the foregoing aspects of which the personnel have knowledge. They may not disclose this information or communicate it to any person or have it in their possession in any medium not included in the legislation regulating official secrets. This obligation shall extend to those classified matters in accordance with the international agreements signed by Spain as well as to matters of the same level of classification owned by other Intelligence Services with which collaboration and reciprocity protocols exist.*

   Failure to comply with this duty, even in the case of no longer holding the position of statutory personnel, will give rise to the corresponding criminal liability as determined by the relevant judicial bodies, without prejudice to its consideration as a disciplinary infraction.

   For these purposes, the CNI will conduct the appropriate legal actions for the prosecution and, if appropriate, criminal conviction for the proved breach of this duty.
2. *Likewise, the personnel of the CNI shall maintain due confidentiality and professional secrecy with respect to unclassified facts or information, of which they have become aware in the performance of their duties or due to their position, and may not make use of the information obtained for their own benefit or that of third parties, or to the detriment of the public interest.*

Additionally, Article 5.4 of Act 11/2002 provides that CNI members shall not be considered law enforcement agents, with the exception of those whose professional activity is related to the protection of the personnel and the facilities of the service.

It is important to highlight that the personnel of the CNI are subject to a specific incompatibility regime – more extended than that of the rest of the personnel of the public service – provided for in Article 76 of the Statute. It envisages that, in general,

the members of the service shall be obliged to perform their functions with absolute and exclusive dedication and may not combine their activity with the performance, by themselves, by a substitute or by a representative, of any post, position, profession or activity, whether of public or private nature, on their own account or on behalf of others. The sole activities exempt from this regime are those related to the management of personal and family assets as well as those previously authorised by the Secretary General of the CNI under the said Article.

In the interests of guaranteeing the fulfilment of obligations imposed in the Statute and in the legislation regulating the CNI, as well as preserving the necessary confidentiality and security to pursue the aims entrusted to the service, Title IX regulates the disciplinary regime to which the statutory personnel are subject, without prejudice to the criminal and civil liabilities that may have been incurred.

Lastly, certain fundamental rights of the personnel of the CNI are also subject to a specific regime, under the terms provided for in the Statute, such as the freedom of association, right to go on strike or the freedom of residence.

Labour staff

According to Article 8 of Act 11/2002 and the first additional provision of the Statute, the Service may hire labour staff. This relation shall be governed by the labour law and not by the rules set out in the Basic Statute of Civil Servants, Royal Decree 5/2015 of 30 October, related to the labour staff of the public service.

This staff shall meet maintenance and operational needs of the service through positions within the areas of maintenance and preservation of buildings, equipment and facilities or through the performance of specific tasks.

Under no circumstances shall labour staff perform functions linked to those entrusted to the CNI under this Act.

In general, the selection of this staff shall be subject to the same participation requirements and selective systems provided for in the Statute of the CNI for statutory personnel.

Both the hiring and the provision of services are subject to the fulfilment of the necessary conditions to have the corresponding security clearance.

Temporary staff

The second additional provision of the Statute defines the temporary staff as follows 'The non-statutory personnel of the CNI who, by virtue of the appointment by the Secretary of State Director and on a non-permanent basis, under the conditions established by law, perform functions regarded as of trust, direct assistance or special advice in the Private Office of the Secretary of State-Director, are called temporary staff, and may not, in any case, hold a position or perform the functions of statutory personnel.'

Concerning its legal regime, the above-mentioned provision states that: 'The temporary staff shall be governed by the provisions expressly established for such staff in the Statute of Personnel of the CNI. Additionally, the regime of obligations and, if appropriate to their position, the regime of rights included in the aforementioned Statute will be applicable to them. Likewise, this staff must hold or be in a position to obtain a favourable security report, in accordance with the characteristics of the position to be occupied.'

2. FUNCTIONS AND MANDATE OF THE CENTRO NACIONAL DE INTELIGENCIA

As it has been previously said, the CNI's function is enshrined in Article 1 of Act 11/2002 of 6 May, its mission being 'to provide the President of the Government and the Government of the Nation with the information and intelligence needed to prevent and avoid any risk or threat that could affect the independence and integrity of Spain, its national interests and the stability of its institutions and of the rule of law.'

As Section 4 of the said Act further elaborates that precept by listing the specific functions of the CNI, providing for:

> ***Article 4.*** *Functions of the Centro Nacional de Inteligencia*
> *The Centro Nacional de Inteligencia shall perform the following functions to achieve its objectives:*
> *a) To collect, assess and interpret information and disseminate the necessary intelligence to protect and promote the political, economic, industrial, commercial and strategic interests of Spain, both inside and outside the national territory.*
> *b) To prevent, detect and provide for the neutralisation of the activities of any foreign service, group or person that endanger, threaten or attack the constitutional order, the rights and freedoms of Spanish citizens, the sovereignty, integrity and security of the State, the stability of its institutions, its national economic interests and the well-being of the population.*
> *c) To promote relations of co-operation and collaboration with Intelligence Services of other countries or international organisations in order to meet its objectives more efficiently.*
> *d) To obtain, evaluate and interpret the traffic of strategic signals in fulfilment of the intelligence objectives assigned to the Service.*
> *e) To coordinate the activities of the Government institutions that use cypher means or procedures; to guarantee the security of information technology in this field; to report on the coordinated collection of cryptological material; and to train its own experts or those of other Government Agencies so as to ensure the proper discharge of the functions of the Service.*

f) To monitor the compliance with the regulations on the protection of classified information.

g) To guarantee the security and protection of its own facilities, information, material and personnel resources.

Complementary to what has been previously set out, according to Article 3, the Government shall determine and approve the objectives of the Centro Nacional de Inteligencia on an annual basis by means of the Intelligence Directive, which shall be classified as secret.

As Article 2 sets out, the principles governing the development of the functions of the Centro Nacional de Inteligencia, in accordance with the Intelligence objectives set by the government, are as follows:

- Subjection to the legal system. The Centro Nacional de Inteligencia shall carry out its specific activities within the framework of the vetting set out in this Act and in the Organic Law 2/2002 of 6 May regulating the prior judicial control of the Centro Nacional de Inteligencia.
- Efficiency.
- Specialisation.
- Coordination.

As for the nature of the activities carried out by the CNI, it should be highlighted that they are classified information in accordance with what is set out in Article 5.1, as it has been previously quoted from the paragraph discussing the legal framework.

Regarding the specific functions discharged by the Centro Nacional de Inteligencia, the following aspects are worth noting.

2.1. Competences in Connection with Criminal Proceedings

As it has been previously pointed out, the Centro Nacional de Inteligencia is not embedded in the law enforcement agencies. For this reason, its objectives and missions do not encompass investigation and prosecution of crimes – whether serious or non-serious crimes, discovery and apprehension of offenders in connection with criminal proceedings. The Centro Nacional de Inteligencia does not have the character of a judicial police force; this responsibility belongs with the law enforcement agencies. The Centro Nacional de Inteligencia has not the mission to gather evidence to be used in criminal proceedings. There is nothing, though, that may prevent the CNI from articulating the means of collaboration to that effect to provide the law enforcement agencies with the evidence that may be required.

Notwithstanding, Act 11/2002 in its Article 5.2 establishes that the CNI shall cooperate with the rest of the public administration, when it states:

2. *If applicable, the Centro Nacional de Inteligencia shall maintain the necessary relations of cooperation and coordination with the rest of the Public Administration, for the proper discharge of its functions in accordance with the legislation in force in each case and preserving the legal protection of the activities of the Service.*

If in the course of discharging its functions the CNI comes across information related to the commission of a crime, it will communicate it to the law enforcement agencies or to the Attorney General, always in compliance with Act 11/2002, Article 5 cited above. The jurisprudence supports this course of action.

2.2. Gathering and Analysis of Information

Concerning the functions related to the gathering and analysis of information, these are categorised in the above-mentioned Act 11/2002, Article 4 which entrusts the CNI to collect, assess and interpret information and disseminate the necessary intelligence to protect and promote the political, economic, industrial, commercial and strategic interests of Spain. Likewise, among its functions are ones to prevent, detect and provide for the neutralisation of the activities of any foreign service, group or person that endanger, threaten or attack the constitutional order, the rights and freedoms of Spanish citizens, the sovereignty, integrity and security of the state, the stability of its institutions, its national economic interests and the well-being of the population.

The CNI's legal framework quoted above authorises it to directly obtain any information, as stipulated in Article 5.5 which sanctions the Centre to, in accordance with the Organic Law regulating the judicial oversight of the Centro Nacional de Inteligencia, to vet individuals or entities in accordance with Act 11/2002. Furthermore, in order to conduct these vetting, the above-mentioned provisions allow the CNI to call on public and private organisations and institutions for the necessary collaboration.

2.3. Administrative Functions

The intelligence activity goes hand in hand with the administrative activity in matters of selection, contracting and continuous training of its personnel in the terms stated in the regulation of its application.

Regarding the administrative functions, one may refer to the activities of the National Security Office (NSO), which is a CNI body that acts as the working office of the ANS-D for the CNI to discharge its functions.

The NSO was created in 1983 as the working body of the CNI's Secretary of State-Director to fulfil his or her duties regarding the protection of classified information.

The NSO's fundamental mission is to make sure that the regulations regarding the protection of classified information are abided by; this applies to both domestic classified

information and that given to the administration or to companies in accordance with international treaties or agreements signed by Spain.

Within its administrative duties, it is worth mentioning that the NSO is the body in charge of, among other aspects, the vetting process of individuals as well as companies.

Likewise, the functions of the National Cryptologic Centre (CCN) can be mentioned within its administrative framework.

The National Cryptologic Centre (CCN) is regulated by Royal Decree 421/2004 of 12 March. Its nature, scope and functions are included in Article 2, para. 1 and 2, of the above-mentioned decree:

1. *The scope of National Cryptologic Centre's (CCN) is the following:*
   a) *The security of the public sector's information technology systems that processing, storing or disseminating information in an electronic format, which require legal protection, and include cyphered tools.*
   b) *The security of the information technology systems processing, storing or disseminating classified information.*

[…]

3. *The National Cryptologic Centre (CCN) is part of the Centro Nacional de Inteligencia (CNI) and shares its tools, regulations and resources, and its functions are included in Act 11/2002 regulating the Centro Nacional de Inteligencia. The National Cryptologic Centre's personnel shall be organically and functionally integrated in the CNI, which is why all legal provisions applied to it, set out in Act 11/2002 of 6 May, and its regulation implementing the said law, particularly its Statute.*

Regarding the administrative functions, the CCN is the Certification Body for the National Security Evaluation and Certification Framework, for application to products and systems within its scope. Likewise, among its functions, the CCN assesses and accredits the ability of encryption products and information technology systems to process information in a secure fashion.

2.4. ICT Security

Concerning the aforementioned Article 4.e) of Act 11/2002, in the field of ICT security, it is worth noting that Article 1 of Royal Decree 421/2004 of 12 March designates the Secretary of State-Director of the CNI as the authority responsible for 'coordinating the activities carried out by different Government bodies that use encryption resources and procedures, ensuring information technologies security in this area, notifying coordinated

procurement of cryptology equipment and training Government staff who specialise in this field. In this regard, the Director of the CCN is the certification authority for information technologies security and the crypto approval authority.

Likewise, it is responsible for ensuring compliance with rules and regulations on protection of classified information regarding information and communications systems pursuant to Articles 4.e and 4.f of Act 11/2002 of 6 May.'

Articles 2 of Royal Decree 421/2004 of 12 March lists the CCN tasks on this matter conferred on the CCN including the following powers:

a) To prepare and disseminate standards, instructions, guidelines and recommendations to ensure information and communications technology security within the Public Administration. Activities arising from these tasks shall be proportionate to the risks to the information processed, stored or transmitted through systems.

b) To provide training for Government personnel who specialise in the field of information and communications technology systems security.

[…]

e) To coordinate the promotion, development, acquisition and operation and use of security technologies of the aforementioned systems.

[…]

g) To establish any required relations and sign any relevant agreements with similar organisations in other countries for the fulfilment of these tasks.

To fulfil these tasks, the CCN may coordinate as appropriate with those national committees with responsibilities conferred on them by law in the field of information and communications technology systems security […].

It is also worth noting the existence of the National Cybersecurity Council that was created by the National Security Council Agreement on 5 December 2013. The National Cybersecurity Council is a professional association that supports the National Security Council acting as a Select Committee for National Security. The Council is presided by the Secretary of State-Director of the Centro Nacional de Inteligencia and Director of the Centro Criptológico Nacional (National Cryptology Centre).

The Council's tasks include promoting relationships and collaboration on cybersecurity not only among the different government agencies, but also between the public and private sector. Likewise, it conducts analysis and research and makes proposals for initiatives at both the national and international level to support the National Security Council.

2.5. Protection of Classified Information

Concerning protection of classified information under Section 4 of Act 11/2002, it falls to the CNI to ensure compliance with rules and regulations on protection of classified information.

The Oficina Nacional de Seguridad (ONS) (National Security Office) is a CNI body acting as the ANS-D working body in the exercise of its duties.

2.6. International Collaboration

Concerning international collaboration, it is worth noting that Article 4 of Act 11/2002 specifically confers on the CNI the task to promote cooperation and collaboration relationships not only with other countries' intelligence services, but also with international agencies.

Regarding classified information, Spain's membership of several international organisations involves the ratification of international treaties and conventions as well as the assumption of security policies and agreements within such organisations.

A major duty to be taken on is to have a National Security Authority responsible for guaranteeing compliance with security rules and regulations.

In Spain, the Ministers of the Presidency, Defence, and Foreign Affairs and Cooperation are designated jointly as the National Security Authority for the protection of classified information within NATO/the EU/the ESA. These ministers have delegated this task on the Secretary of State-Director of the Centro Nacional de Inteligencia.

As for the above information about treaties that the state may enter into, the CNI can also execute agreements and conventions on this matter.

CHAPTER XIX

Sweden

Carl Rundström Frödén, Fredrik Hugo, Maria Sertcanli

1. POSITION OF THE SAEPO IN THE DOMESTIC LEGAL SYSTEM

1.1. Position and Role of the SAEPO in the Public Administration System

The Swedish Security Service (SAEPO) is both a security service and a police service, with a nationwide remit. It works to increase the level of security in Sweden. It does this by detecting and reducing threats to the security of Sweden and its critical assets and by reducing the vulnerabilities of these assets.

Organisation

The remit of the Swedish Security Service is governed by the Police Act, the Ordinance containing instructions for the Security Service, and an annual letter of appropriation from the government. According to the Ordinance containing instructions for the Security Service, the service in its capacity as a security service is to carry out intelligence and security work. In addition, the Security Service is to participate in the cross-agency work to counter serious organised crime. Swedish legislation contains no definition of special services.

The Swedish Security Service used to belong to the Swedish Police Authority. However, since 2015, the service has been an independent government agency under the Ministry of Justice. The Swedish Security Service carries out its remit independently, meaning that neither the Ministry of Justice nor the government has any influence over the decisions that the service makes in any particular case. As a government agency, the service is directed by the Head of the Swedish Security Service.

The service has an Oversight Council consisting of a maximum of eight politically appointed members. The role of the Oversight Council is to ensure public transparency. The exercise of oversight does not pertain to the types of tasks for which insight could

jeopardise the service's cooperation with other security and intelligence services or that concern the management of police activities in individual cases.

1.2. Scope of activities of the SAEPO

The Swedish Security Service has five main remit areas:

Counterintelligence involves preventing and detecting espionage and other unlawful intelligence activities targeting Sweden and Swedish interests abroad, foreign interests in Sweden and refugees.

Counterterrorism involves preventing and detecting terrorism targeting Sweden, Swedish interests abroad, foreign interests in Sweden, acts of terrorism in other countries and international terrorist networks in Sweden as well as support to and financing of terrorism.

Countersubversion involves countering violence, harassment, threats, coercion and corruption aimed at negatively affecting the basic functions of Sweden's democratic form of government.

Protective security involves raising the level of security across society via analyses, records checks, oversight of and recommendations to government agencies and companies whose activities are related to Sweden's security.

Dignitary protection involves protecting and ensuring the security of the central government and foreign diplomatic representatives as well as state visits and similar events.

The service's work also includes counter proliferation which involves preventing the proliferation, procurement and production of weapons of mass destruction (WMDs). The primary task of the Swedish Security Service in this area is to prevent the transfer of expertise, products, substances and micro-organisms from or via Sweden to actors seeking to procure or develop WMDs or their means of delivery. This work is carried out in close cooperation with other government agencies.

The Swedish Security Service is also tasked with preventing individuals who pose or may come to pose a security threat to Sweden from staying or settling in Sweden. A key part of the preventive work in this area is the service's role set out in aliens legislation and as a referral body for the Swedish Migration Agency in aliens cases.

1.3. Oversight of the Swedish Security Service

A number of government agencies are responsible for overseeing the Swedish Security Service's compliance with regulations.

The Swedish Commission on Security and Integrity Protection oversees the Security Service's processing of personal data in its law enforcement work. It also oversees the Security Service's use of covert intrusive measures and qualified protected identities. The

Commission also oversees the Security Service's use of information provided by the National Defence Radio Establishment.

The Swedish Commission on Security and Integrity Protection consists of eight members nominated by all the Riksdag (parliament) parties and a chairman and deputy chairman who serve, or have served, as permanent judges.

The Commission exercises its oversight through inspections and has the right to access all information at the Swedish Security Service that is required for this oversight.

The Commission may express criticism as a result of its inspections but has no power of authority to impose sanctions. However, if the shortcomings that come to light during such oversight are sufficiently serious, the Commission may transfer the case to a government agency that has such power of authority.

The Swedish Authority for Privacy Protection is an oversight agency that overlaps the Swedish Commission on Security and Integrity Protection in terms of overseeing the Security Service's processing of personal data in its law enforcement work. The Swedish Authority for Privacy Protection is also responsible for the oversight of the Security Service's processing of personal data in its administrative activities. In practice, it is quite rare for the Swedish Authority for Privacy Protection to exercise its oversight of the Security Service.

The Parliamentary Ombudsman and the Office of the Chancellor of Justice are responsible for the general oversight of national government agencies' compliance with regulations. The oversight exercised by the Parliamentary Ombudsman is largely a result of reports from the public. The Office of the Chancellor of Justice has a more generalised oversight function, meant mainly to discover systematic shortcomings in public sector activities.

1.4. Legal Status of the Officers/Employees

The Swedish Security Service employs civilian personnel and personnel with police training. AU the close protection officers in the service's Dignitary Protection Unit have police academy training. Under the Police Act, a police officer may use force to carry out an official duty if other means are inadequate and if this is justified in view of the circumstances. In certain situations, a police officer also has the right to take a person into temporary custody, remove a person or carry out a search of a person. Swedish Security Service staff that have police training have the right to carry weapons. The service's civilian staff does not have any such special powers of authority.

Enhanced secrecy protection applies to personal data stored for the Security Service's personnel administrative purposes, regardless of whether the staff member concerned has police training or not. This enhanced secrecy also applies to the staff members of other government agencies that are at a relatively greater risk of being subjected to violence.

Security Service staff members who are tasked with surveillance or investigative work related to serious crime or who are tasked with preventing such crime may in certain cases be assigned qualified protected identities, the use of which is governed by the Qualified Protected Identities Act.

2. TASKS AND MANDATE

2.1. Investigative Powers and the Role in Criminal Procedure

The Security Service is responsible for detecting and prosecuting:

- espionage and other crimes against Sweden's security
- terrorist crime and related offences such as the financing of terrorism
- sabotage and related offences aiming to jeopardise Sweden's security or seriously threaten or harm essential services
- industrial espionage and unlawful handling of an industrial secret if there is reason to suspect that this act was directed or assisted by a foreign power or by someone acting on behalf of a foreign power
- offences where violence, threats or force have been used for political purposes against a person whose security and close protection is the responsibility of the Security Service or against an important public interest
- certain offences related to sanctions legislation, war material or dual-use products.

The service's powers of authority for criminal investigation purposes are governed by the Code of Judicial Procedure and the Act on Equipment Interference. When investigating crime, the service has the possibility of using pre-trial supervision measures (such as house searches and seizures) and/or covert intrusive measures. The covert intrusive measures that may be used for criminal investigation purposes are covert interception of electronic communications, covert surveillance of electronic communications, covert video surveillance, covert audio surveillance and equipment interference. As a rule, covert intrusive measures may only be used when there is a person who is suspected on reasonable grounds. However, covert surveillance of electronic communications, covert video surveillance and equipment interference may be used in certain circumstances to investigate persons who may be suspected on reasonable grounds. Permission to use a covert intrusive measure may only be granted if the measure is of particular importance for investigating the crime and if the reasons for the measure outweigh the intrusion or other detriment caused to the suspect or another conflicting interest.

A prosecutor employed by the Prosecution Authority, which operates independently from the Swedish Security Service, always heads criminal investigations carried out by the Service. The decision as to which intrusive measures will be implemented in a criminal investigation is made by the prosecutor. The prosecutor must, however, ask a court's per-

mission to use covert intrusive measures. The exception to this is in cases where a significant delay in the investigation would ensue while awaiting the court's permission; in such cases, the prosecutor may decide on the measure without the court's permission. However, this decision must be presented to the court as soon as possible for consideration and if the court finds that there are insufficient reasons for the measure, it may reverse the decision.

2.2. Intelligence Gathering

The service's powers of authority for the purpose of carrying out intelligence activities

The Security Service is also responsible for preventing, pre-empting and detecting the type of criminal activities whose detection and prosecution fall under the service's remit, i.e.:

- espionage and other crimes against Sweden's security
- terrorist crime and related offences such as the financing of terrorism
- sabotage and related offences aiming to jeopardise Sweden's security or seriously threaten or harm essential services
- industrial espionage and unlawful handling of an industrial secret if there is reason to suspect that this act was directed or assisted by a foreign power or by someone acting on behalf of a foreign power
- offences where violence, threats or force have been used for political purposes against a person whose security and close protection is the responsibility of the Security Service or against an important public interest
- certain offences related to sanctions legislation, war material or dual-use products.

The service may also use covert intrusive measures for the purpose of carrying out intelligence activities. This is governed by the Act on Measures to Prevent Certain Particularly Serious Crimes and the Act on Equipment Interference. All the covert intrusive measures with the exception of covert audio surveillance may be used for the purpose of carrying out intelligence activities. A condition for using covert intrusive measures is that there is a substantial risk that a person will engage in criminal activities involving certain offences stated in legislation, e.g. espionage and terrorist offences. Covert intrusive measures may also be used if there is a substantial risk that such criminal activities will be conducted within an organisation or a group and it can be suspected that a person belonging to or acting on behalf of that organisation or group will knowingly promote these activities. Permission to use a covert intrusive measure may only be granted if the measure is of particular importance in preventing the criminal activity and if the reasons for the measure outweigh the intrusion or other detriment caused to the person subject to the intrusive measure or another conflicting interest.

Just as for the covert intrusive measures used for criminal investigation purposes, it is the court, upon request by a prosecutor, that grants permission to use covert intrusive

measures for the purpose of carrying out intelligence activities. The exception to this is in cases where a significant delay in the investigation would ensue while awaiting the court's permission; in such cases, the prosecutor may decide on the measure without the court's permission. However, this decision must be presented to the court as soon as possible for consideration and if the court finds that there are insufficient reasons for the measure, it may reverse the decision.

In carrying out its intelligence activities, the Security Service has the right to partake in signals intelligence gathered by the National Defence Radio Establishment. However, the signals intelligence information may not be used within the framework of a criminal investigation.

Gathering of information from private-sector actors

The service has the right to gather certain information from private-sector actors both for criminal investigation purposes and for the purpose of carrying out intelligence activities. For instance, the service has the right, under the Act on Measures Against Money Laundering and Terrorist Financing, to partake in information about financial transactions from banks and other financial actors if this is necessary for an investigation into money laundering or the financing of terrorism. Sweden's Financial Intelligence Unit (FIU) within the EU legal framework is, however, not a part of the Swedish Security Service, but a part of the Swedish Police Authority.

Under the Electronic Communications Act and the Act on the Gathering of Electronic Communications Data as Part of the Intelligence Activities of Law Enforcement Agencies, the Swedish Security Service also has the right to gather information about electronic Communications cases other than those stipulated in the above-mentioned regulations regarding covert intrusive measures. The Security Service may make independent decisions regarding the gathering of subscription data (e.g. who a certain IP address belongs to), but traffic and location data may only be gathered upon decision by a prosecutor. Telecom providers have an obligation to retain certain data for a time period ranging from two to ten months, depending on the specific type of data.

The required data retention time was reduced following the so-called Tele2 Judgment issued by the European Court of Justice (CJEU). A government inquiry is reviewing the mentioned legislation in order to assure that law enforcement agencies' access to information is improved and maintained over time to keep pace with technological developments and changes in communication patterns while ensuring that human rights are respected.

Under the Patient Safety Act, the Security Service has the right to gather healthcare data if necessary for its dignitary protection work. The purpose of this is to enable the service to gather personal data about individuals, who potentially pose a threat to a protectee of the service, to make it possible to assess any concrete threats against such a protectee.

As a rule, the service may only gather data from foreign private-sector actors that do not operate in Sweden via a European arrest warrant or a formal request for international legal assistance. If the foreign private-sector actor has the right, under the legislation of country where they are established, to disclose data to the Swedish Security Service, there is nothing preventing the Swedish Security Service from gathering such information through other means as well if the information is needed in the scope of the service's activities.

The service's powers of authority in alien cases

Under the Act Concerning Special Controls in Respect of Aliens, the Security Service may submit an application to the Migration Agency to have an individual expelled from Sweden if this is deemed necessary for reasons of national security or if, in view of what is known about the alien's previous activities and other circumstances, it may be feared that they will commit, or be an accessory to, a terrorist offence. Pending the decision of the Migration Agency, the service may take the alien into custody. When it is not possible to enforce an expulsion order, the alien in question may be made subject to a duty to report daily to a police station. In certain circumstances, the Security Service may also have the right to use covert intrusive measures against the alien.

2.3. Administrative Tasks

Swedish government agencies, including the Swedish Security Service, must perform certain administrative duties related to the principle of public access to official documents and public transparency. For instance, they have the obligation to register, archive and provide public documents, and reply to enquiries from the public. The Security Service has no other particular administrative duties besides these and the ones mentioned above concerning protective security. However, other government agencies must consult with the Swedish Security Service in certain situations related to the security of Sweden. For instance, it is stipulated in the Electronic Communications Act that the Post and Telecom Authority must consult with the Security Service when considering applications for permits to use radio transmitters. This was done when the Swedish 5G spectrum auction was taking place and the outcome of this was that the Post and Telecom Authority forbade the operators who won the auction from using the two above-mentioned companies' products in the building of the 5G network. The Post and Telecom Authority's decision in this case was appealed. The decision was upheld in the first instance (the Administrative Court) and the case is still pending in the highest instance.

Under the Protection Act, the Swedish Security Service may use security guards to guard any of its buildings that are considered critical assets. The security guards may make decisions regarding carrying out a search of a person, vehicle, vessel or aircraft, if necessary, for guarding purposes. In certain cases, the security guards have the right to refuse entry of, remove or temporarily take into custody an individual in or near a critical asset.

The security guards also have the right to intervene by using violence against an unmanned aerial vehicle (drone) located within, near or above a critical asset.

2.4. Protection of Classified Information

Protection of classified information and of security-sensitive activities is governed by the Protective Security Act. The Security Service is the oversight body for the protective security in the civilian agencies which run the nation's critical assets. The oversight of protective security is also carried out by the Armed Forces, certain county administrative boards and various sector-specific agencies that are responsible for the oversight of the protective security of private businesses within certain sectors such as electricity supply operations. In certain cases, the Security Service may assume the oversight duties of one of the other agencies responsible for oversight in the civilian area.

Oversight is meant to ensure that the entities concerned follow protective security regulations in terms of both classified information and security-sensitive activities. Within the framework of its oversight function, the Security Service has the right to gather information from the entity and the right to access areas, premises or facilities where the entity's security-sensitive activities are being carried out. Upon request by an entity, the service may also carry out a penetration test to check the entity's cybersecurity.

The service may issue injunctions and impose administrative sanctions for breaches of the Protective Security Act. An entity subject to the oversight of the Security Service which is going to carry out a procedure (e.g. an outsourcing or a transfer of the security-sensitive activities) involving protective-security risks must consult with the service before carrying out the procedure. In association with the consultation, the service may order an entity to take protective security measures prior to carrying out the procedure or forbid the entity, in whole or in part, from carrying out the procedure.

The Security Service issues regulations on protective security for the entire civil sector, not only for the government agencies subject to the service's oversight. Within the framework of security screenings, the service also carries out records checks of the employees and contractors at all the entities that carry out security-sensitive activities.

Four designated government agencies share the responsibility of international cooperation in protective security matters: the Ministry for Foreign Affairs, the Security Service, the Armed Forces and the Defence Material Administration. The Ministry for Foreign Affairs and the Defence Material Administration are responsible for issuing security certificates; however, the Security Service issues security certificates, as required, for its own staff members. In terms of oversight, the role of the Security Service is mainly to ensure that Swedish international agreements pertaining to protective security in the civil sector are upheld and, if stipulated in the relevant international agreement, to be the point of contact for the corresponding foreign competent national security agency.

2.5. Internal Cooperation

The Swedish Security Service's most important national cooperation partners are other intelligence and lawenforcement agencies, such as the Military Intelligence and Security Service, the National Defence Radio Establishment, the Police Authority and the Economic Crime Authority. While much of such cooperation is intended for purposes of exchanging experience and information, it also serves to provide investigative and operational support, for instance, by providing the Police Authority with expertise, threat assessments, surveillance and analyses. In terms of dignitary protection, the Security Service works closely with the local police to plan and implement protective measures within their various districts.

The service also cooperates with government agencies, local authorities, county councils and certain companies that are encompassed by protective security legislation.

The Counter-Terrorism Cooperation Council is made up of 15 Swedish government agencies and is meant to strengthen Sweden's ability to counter and respond to terrorism. The Security Service leads and convenes the Council, which is also composed of the Economic Crime Authority, the National Defence Radio Establishment, the Armed Forces, the Prison and Probation Service, the Coast Guard, the Migration Agency, the Civil Contingencies Agency, the Police Authority, the Tax Agency, the Radiation Safety Authority, the Defence Research Agency, the Transport Agency, Customs and the Prosecution Authority.

Another cooperation platform between Swedish government agencies is the Cooperation Council Against Organised Crime which is meant to combat organised crime by implementing various crime prevention measures through joint efforts at national and regional levels. The focus lies on combating serious crime which poses a threat to Sweden and on organised crime in vulnerable areas. Besides the Security Service, the Cooperation Council Against Organised Crime is comprised of the Public Employment Service, the Economic Crime Authority, the Social Insurance Agency, the Prison and Probation Service, the Enforcement Authority, the Coast Guard, the Migration Agency, the Police Authority, the Tax Agency, Customs and the Prosecution Authority.

Another example of cooperation between public agencies is the National Centre for Terrorist Threat Assessment (NCT). This is a permanent working group staffed by personnel form the Swedish Security Service, the National Defence Radio Establishment and the Military Intelligence and Security Service. The NCT is tasked with producing long-term and short-term assessments of the terrorist threat to Sweden and Swedish interests.

As instructed by the government, a national Cybersecurity Centre has been established by the Swedish Security Service, the National Defence Radio Establishment, the Swedish Armed Forces and the Swedish Civil Contingencies Agency. Within the framework of the Cybersecurity Centre, these government agencies are meant to coordinate their work to prevent, detect and respond to cyber attacks and other IT incidents. They are also meant to provide advice and support regarding threats, vulnerabilities and risks and to serve as

a national platform for the coordination and exchange of information with private- and public-sector actors in the area of cybersecurity.

2.6. International Cooperation

The Ordinance Containing Instructions for the Security Service stipulates that the service is to cooperate with foreign government agencies or bodies and international organisations to the extent necessary for Security Service activities and as decided by the government.

The Security Service's cooperation with international partners is well developed. To facilitate this cooperation, the service has stationed liaison officers abroad, at e.g. the EU law enforcement agency Europol. The Swedish Security Service's closest cooperation partners are the security services of the Nordic countries, the EU countries and the USA.

In the framework of the Counterterrorism Group (CTG), the Swedish Security Service works with the security services of the European Union, Norway, Switzerland and the UK. Another important cooperation platform is the international police organisation Interpol.

The UN and the EU are two important international players whose decisions and activities often have a bearing on the service's work. This can be the case, for instance, when these bodies make decisions on enforcement measures in the form of sanctions.

2.7. The Processing of Personal Data

Neither the FU Data Protection Directive nor the EU General Data Protection Regulation applies to the Swedish Security Service's processing of personal data for national security-related purposes. Most of the service's processing of personal data is for national security-related purposes. The processing of personal data by the Security Service in a law enforcement context is regulated by the Act Concerning the Swedish Security Service's Processing of Personal Data. Although the EU data protection regulations do not apply to the Security Service's processing of personal data related to national security, the configuration and principles of Swedish legislation in this matter are essentially the same as those of the Data Protection Directive.

One of the fundamental principles of the governance of the processing of personal data related to the Security Service's operational activities is that the personal data being processed must be of necessity for certain specified, permissible purposes. To put it concisely, these purposes relate to the service's operational areas and form the legal basis for the processing of personal data within the service's law enforcement activities.

For the processing of personal data for administrative purposes, the Security Service applies the EU General Data Protection Regulation.

CHAPTER XX

National Security Clause in the EU Law and Its Implications for Intelligence and Security Services

Marcin Nowiński

Within the legal framework of the European Union law, there are some issues, which are crucial for the vested interests of member states as well as for the intelligence and security services. One of the inherent and key features of these issues is ongoing discussion and considerations about their role, meaning, proper legal interpretation. Such issues often give rise to disputes, in which different points of view rub each other up the wrong way. It is natural and obvious that one of such issues is the national security clause, which is one of the most important and significant legal matters for all – intelligence and security services and its countries. It is worth mentioning that there is no legal definition of the national security clause within the EU law. In its judgements, the CJEU frequently gives guidelines and directives to the proper understanding of this issue, but there are still divergences and different opinions concerning the national security clause. Particularly, there is significant discrepancy between member states and EU bodies with regard to the understanding of the scope of the national security. In this paper, I would like to have a second look at the concept of the national security as well as to resolve this issue, taking into account the recent jurisprudence of the CJEU and publications in this matter.

I hope that such research will contribute to the better understanding of national security concept.

1. INTRODUCTION

Many years ago, Steve Peers, a great European law expert, stated that most or all legal systems, whether national or international, provide for the suspension of obligations in the

event of emergencies or threats to national security.[1] This statement is certainly true, as we consider and think about key points of national security. One of the most meaningful aspects of national security is how to perceive this issue, which approach should be applied to figure out what national security distinctive features are and in what way should it be understood. There is no one right answer to this precariousness, but otherwise we can rethink national security and peer to have a better understanding of the essentials to the more complicated elements of this concept.

What is national security and which factors determine the exact meaning of this term? Professor Samuel Makinda's definition of security as 'the preservation of the norms, rules, institutions and values of society' appears to be useful. He argues that all the social institutions, principles and structures associated with society, including its people, are to be protected from 'military and non-military threats'.[2] The United Nations in their publications also underline that in many forums on the topic of security, there has been an attempt to establish a divide between national and global security. Although, in theory, a boundary exists between these two conceptual frameworks, such a boundary is not sufficient to maintain a clear-cut delimitation between them. Rather, they have a symbiotic relationship, although limited to the local security sphere, in which states lack the capacity to handle unilaterally. Equivalently, there are issues at the international sphere that will require a domestic security apparatus to deal with.[3] Therefore, it is also vital to point out reasons for more cooperation and synergy between national and global security mechanisms. Depending on which elements are considered as most significant, we should start with pointing out that national security could be perceived as the ability of a state's government (or authorities) to protect its citizens, economy and other institutions. Global security as a set of ideas, developed by the United Nations, evolved from the necessity that nature and many other activities, particularly globalisation, have placed on states. These are demands that no national security apparatus has the capacity to handle on its own and, as such, call for the cooperation of states. The global interconnection and interdependence among states that the world has experienced and continues to experience makes it necessary for states to cooperate more and work together.[4] Generally speaking, the global security concept promoted by the United Nations is focused on trying to solve and eliminate conflicts within such tools as international law, aid, confidence-building measures and global governance, where such instruments as the use of force should be reserved largely for international

1 Steve Peers. National Security and European Law. Introduction, p. 1. *Yearbook of European Law*, Vol. 16, Iss. 1, 1996. https://academic.oup.com/yel/article-abstract/16/1/363/1718740?redirectedFrom=PDF

2 Samuel M. Makinda, *Sovereignty and Global Security, Security Dialogue*, 1998, Sage Publications, Vol. 29(3) 29, pp. 281–292.

3 Segun Osisanya, National Security versus Global Security. *United Nations – UN Chronicle*. https://www.un.org/en/chronicle/article/national-security-versus-global-security

4 Ibidem.

peacekeeping, peace enforcement and the protection of citizens from violence and should be decided upon and organised by the UN.[5]

Kim R. Holmes presented an interesting point of view in this matter. He perceives national security through the lens of certain concepts that this term incorporates, among others the concept of power. It can best be defined as a nation's possession of control of its sovereignty and destiny. It implies some degree of the control of the extent to which outside forces can harm the country. Hard, or largely military, power is about control, while soft power is mainly about influence – trying to persuade others, using methods short of war, to do something. Instruments of power exist along a spectrum, from using force on one end to diplomatic means of persuasion on the other. Such instruments include the armed forces, law enforcement and intelligence agencies and various governmental agencies dedicated to bilateral and public diplomacy, foreign aid and international financial controls. Variables of power include military strength, economic capacity, the will of the government and people to use power, and the degree to which legitimacy – either in the eyes of the people or in the eyes of other nations or international organisations – affects how power is wielded. The measure of power depends not only on hard facts, but also on perceptions of will and reputation.[6]

Anyway, one of the most common ways of current thinking about national security is understanding this concept not only within the scope of military field, but also as a broader concept which includes: economic security, political security, energy security, homeland security, cybersecurity, human security and environmental security. Assuming the above-mentioned national security concept, we can determine the different key points of this issue, including threats to the national security and other crucial elements.

It is worth mentioning in this place some strategic concepts of national security, considered from the perspective of national interests. One of these concepts is derived from the National Security Strategy of the Republic of Poland, which asserts that this country creates favourable conditions to pursue its national interests and achieve strategic objectives in the domain of national security in conformity with the following values: independence and sovereignty of the state, security of its citizens, human and civil liberties and rights, human dignity, justice, national identity and heritage, democratic rule of law, solidarity, international order based on the principles of international law and environment protection. The national interests in the field of national security include:

- safeguarding the independence, territorial integrity, sovereignty and security of the state and its citizens
- shaping international order, based on solidarity and respect for international law, which guarantees the safe and secure development of a country

---

5 Kim R. Holmes, *What Is National Security? 2015 Essays*. 7 October 2014. The Heritage Foundation. https://www.heritage.org/military-strength-essays/2015-essays/what-national-security

6 Ibidem.

- strengthening national identity and guarding national heritage
- ensuring conditions for sustainable and balanced social and economic development and environment protection.

The above-listed national interests form the pillars of the national security of the Republic of Poland.[7]

Another somewhat similar understanding of national security essentials was presented by the Government of the Netherlands, which in its strategy concludes that the government, in order to protect society from disruption owing to a disaster or crisis. With such understanding, it is examining the threats, how to prevent them, and what to do if a disaster occurs. National security is at stake when one or more of the country's vital interests are threatened. Those interests are:

- territorial security: this would be jeopardised by a military occupation, but also by prolonged flooding
- economic security: a major internet or electrical breakdown would disrupt online financial transactions
- ecological security: damage to the environment from pollution or extreme heat, or drought
- physical security: deaths, injuries and chronic illnesses caused by flooding or a pandemic
- social and political stability: violations of the rule of law caused, for instance, by tensions between communities.

Furthermore, the government investigates potential threats to the country, how serious they are and how they can be dealt with. This process is roughly divided into three steps:

- Describing threats: what threats may be facing the country?
- Comparing threats: how serious would the consequences of a threat be and how likely is it to be carried out? This is based on the National Risk Assessment. A summary of the National Risk Assessment will give one an idea of the method used.
- Determining the approach: how the risk of an incident can be reduced (prevention) and how we can deal with an incident if it occurs (preparation and response).[8]

All of the above-specified ideas or concepts concerning national security lead to the conclusions that national security issue has often been taken to narrowly, where the main factors were limited to the preservation of sovereignty, territorial integrity and internal

[7] National Security Strategy of the Republic of Poland, 2020. https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

[8] Government of the Netherlands/Home/Topics/Counterterrorism and National Security/National Security. https://www.government.nl/topics/counterterrorism-and-national-security/national-security

stability, and that was a traditional way of comprehending national security matters. Although, the world has changed and new threats are arising, which are more complex and unpredictable, and we cannot catalogue them because new ones will come up within the perspective of next decades. Some of well-known phenomena will still constitute threats to the national security, among them the most dangerous ones: terrorism, espionage and organised crime as well as proliferation of weapons of mass destruction. There is still one obligation of a states, in the context of national security, which cannot be denied and it is the duty of a state to protect its citizens, even if it requires to take some extraordinary measures in the interest of national security, taking into consideration the fact that such measures could interfere or even in some cases clash with the citizens' fundamental rights. Such measures have the potential to threaten fundamental rights through means such as surveillance, military intervention etc. The essential justification is that states may interfere with individual rights in exceptional circumstances when, for instance, their independence, sovereignty, territorial integrity, constitutional order and/or public safety are threatened. Such threats are usually regarded as falling within the scope of the national security or similar terms, but the problem is that, in the absence of a definition, such terms are vague and open to different interpretations.[9] Notwithstanding the above, national security issue and its proper understanding is a fundamental interest of the intelligence and security services as well as it is crucial for performing its tasks, within observing the legal framework and in an effective way. Therefore, in the next subchapter I will review the issue of the legal definition of national security.

2. LACK OF THE LEGAL DEFINITION OF 'NATIONAL SECURITY' IN THE EUROPEAN LAW

First of all, there is no legal definition of national security in the European Union law. Furthermore, there is no consensus on what national security means in the international law, either. It might be interesting that in the United Kingdom, during the passage of the Investigatory Powers Bill through the House of Lords in 2017, rejecting an amendment to the Bill which would have clearly defined 'national security' in law, Earl Howe, for the UK Government, stated: 'It has been the policy of successive Governments not to define national security in statute. National security is one of the statutory purposes of the security and intelligence agencies. Threats to national security are, as we have heard, constantly evolving and difficult to predict, and it is vital that legislation does not constrain the security and intelligence agencies in their ability to protect the public from new and

[9] Report on national security and European case-law prepared by the Research Division of the ECtHR, para. 25, p. 4, and Council of Bars & Law Societies of Europe. (2019). *CCBE Recommendations on the Protection of Fundamental Rights in the Context of 'National Security'*, pp. 4–5. https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf

emerging threats… I think the key point is that to define national security in statute could have the unintended effect of constraining the ability of the security and intelligence agencies to respond to new and emerging threats to our national security.'[10]

The above-mentioned statement of Earl Howe touches upon two completely separate issues. The first one being what constitutes the national security of the state may seem be constant, and the second one – the manner in which national security is threatened is constantly changing.[11] The key point is not to constraint intelligence and security services in performing their activities and it makes their activities more flexible and capable of providing swift response to new threats at the time when they occur. Otherwise, opponents will say that such an approach is malfunction because if national security remains undefined in law, there is no legal basis upon which a court is able to evaluate whether the purpose for some intrusive powers might have been performed, is or is not performed, in pursuit of national security.[12] Otherwise, the opponents may argue that such an approach is fundamentally flawed due to the lack of legal basis enabling the court to assess whether or not the intrusive powers have been applied in order to safeguard national security.

Although there are many formulations and interpretations of the term of national security, there is no singular, unified definition, set forth in the EU law. Obviously, in some member states of the EU, domestic legal order provides definitional clarity, but these definitions may differ in different states and jurisdictions. As it was already stated, the bottom line for the activities carried out by the intelligence and security services is the correct interpretation of the notion of national security and its boundaries as well as its relation to the EU secondary law. It is important for a number of reasons, but basically, applying various legal instruments within the legal framework of the EU by intelligence and security services as well as making use of its competences is subject to numerous limitations under the EU primary and secondary law. It is laid down in the Treaties that the European Union must respect the national identities of the member states that are inherent in their fundamental structures, political and constitutional ones. The Treaties expressly set out the above-mentioned obligations. For the first time, the concept of national security was vaguely mentioned for the first time in the Maastricht Treaty.[13] Article F, para. 1 set out 'The Union shall respect the national identities of its Member States'. Later on, the above-mentioned provision F.1 of the Maastricht Treaty was re-

---

10 Council of Bars & Law Societies of Europe. (2019). *CCBE Recommendations on the Protection of Fundamental Rights in the Context of 'National Security'*, p. 4.

11 Ibidem, p. 5.

12 Ibidem.

13 Formally the Treaty on European Union, an international agreement approved by the heads of government of the states of the European Community (EC) in Maastricht, Netherlands, in December 1991. Ratified by all EC member states (voters in Denmark rejected the original treaty but later approved a slightly modified version), the treaty was signed on 7 February 1992 and entered into force on 1 November 1993.

placed by Article 6(3) of the Amsterdam Treaty[14] (the wording of this Article was the same as the wording of the previous one).

The provisions of the Amsterdam and Maastricht Treaty referred to above paved the way for the most important legal norm of the European Union primary law in the area of national security – Article 4(2) of the Treaty on European Union,[15] which reads as follows:

Article 4

2. *The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.*

National security is not only invoked in Article 4(2) of the Treaty on European Union, but it is also mentioned in Article 6(1) and para. 2 of Articles 8, 10 and 11 of the European Convention on Human Rights[16]:

Article 6 (Right to a fair trial)

1. *In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.*

---

14 The Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, signed in Amsterdam on 2 October 1997, entered into force on 1 May 1999.

15 The TEU is based on the Maastricht Treaty which marked a new stage of European integration by going beyond the original economic objective (a common market). It opened the way to political integration with a transition from the European Economic Community (EEC) to the European Union (EU). Signed on 13 December 2007, the Lisbon Treaty – which comprises the TEU and the TFEU – entered into force on 1 December 2009. Further referred to as 'the TEU'.

16 European Convention on Human Rights. The Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights, was opened for signature in Rome on 4 November 1950 and came into force on 3 September 1953. Further referred to as 'the ECHR'.

Article 8 (Right to respect for private and family life)

2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

Article 10 (Freedom of expression)

2. *The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

Article 11 (Freedom of assembly and association)

2. *No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. This Article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State.*

As we can notice, the notion of national security is used in two basic legal acts of the European Union (TEU) and the Council of Europe (ECHR). However, despite the fact that this notion appears in the provisions of the above-mentioned Treaty and Convention, they do not provide its definition. In Article 4(2) of the TEU, the last sentence seems to be pivotal. It stipulates stating: 'national security remains the sole responsibility of each Member State'. However, the interpretation of this phrase, in particular taking into account the jurisprudence of the CJEU, may differ significantly and be very tricky, which depends on who is performing a legal interpretation. Although the ECHR seems to be using the national security clause as a reason for limitation on the exercise of human rights guaranteed in the Convention. These exemptions regarding the presumption of national security in the ECHR lead to the conclusion that the rights which are guaranteed in the ECHR are not absolute and the States-Parties to the Convention having regard to demo-

cratic standards can take advantage of the opportunities to constrain particular rights if it is justified in the situation that has arisen. Taking into account these considerations, it is important to observe that the European Court of Human Rights (Case *Esbester v. the United Kingdom*[17]) has considered providing a definition of the term 'interests of national security', finally coming to the conclusion that it is not necessary to have a comprehensive definition of this issue. It justified its position by underlining the fact that 'many laws, which by their subject-matter require to be flexible, are inevitably couched in terms which are to a greater or lesser extent vague and whose interpretation and application are questions of practice.'

A closer look at the jurisprudence, with regard to the cases brought to the CJEU and the ECHR will be a subject of examination in the next subchapter. In this context it should be noted that in accordance with Article 4 of the Treaty on the Functioning of the European Union[18] within the scope of the area of freedom, security and justice, some competences are shared between the EU and member states, according to the principle of conferral, the EU and its member states are able to legislate and adopt legally binding acts. The EU member states exercise their own competence where the EU does not exercise, or has decided not to exercise, its own competence. Furthermore, Article 4 of the TEU sets out that in accordance with Article 5, competences not conferred upon the Union in the treaties remain with the member states. However, it is said, in compliance with Article 4(2) of the TEU, that 'national security remains the sole responsibility of each Member State.'

In any case, national security needs to be distinguished from the security of the European Union, but also from state security, public security and defence. All these notions are referred to separately in the EU treaties and underlying legislation, although they are inextricably linked. Therefore, whether or not something should be defined as falling under the national security exemption cannot only be explained by strictly legal arguments. What can be said is that, whereas activities by intelligence and security services are generally accepted as falling under the national security exemption, this is not always the case when general law enforcement authorities fulfil similar tasks.[19] It must be noted that the exemption in the treaties offers no possibility of invoking the national security of a third

---

17 *Case Esbester vs United Kingdom* (18601/91) (1994), Commission decision from 2 April 1993, www.echr.ketse.com/doc/18601.91-en-19930402/view/ https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-1537%22]}

18 The Treaty on the Functioning of the European Union (TFEU), as a result of the Lisbon Treaty, was developed from the Treaty establishing the European Community (TEC or EC Treaty), as put in place by the Treaty of Maastricht. The EC Treaty itself was based on the Treaty establishing the European Economic Community (TEEC), signed in Rome on 25 March 1957. Signed by 27 EU countries (Croatia did not join the EU until 2013) on 13 December 2007, the TFEU entered into force on 1 December 2009. Further referred to as 'the TFUE'.

19 Working Document on surveillance of electronic communications for intelligence and national security purposes. Adopted on 5 December 2014, 14/EN WP 228, p. 2.

country alone in order to avoid the applicability of EU law. However, it acknowledges that there may be areas where a national security interest of an EU member state and that of a third country are aligned. If so, this should be properly justified by the EU member state to the relevant authorities on a case-by-case basis.[20]

Coming back to the national security clause, the EU Treaties refer to many aspects, which are closely tied with the issue of national security and within the scope of which the EU has its competence to legislate and adopt legally binding acts. For instance, by virtue of Article 73 of the TFEU:

> ***Article 73***
> *It shall be open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security.*

This provision clearly confirms that in present times, almost each activity which is undertaken by intelligence and security services requires cross-border cooperation, and it is within the scope of their competences how they determine the mechanisms and forms of cooperation concerning national security. However, cross-border cooperation between the intelligence and security services of the member states of the EU does not mean that they get rid of exclusive competences regarding national security.

In the discussion about the issue of national security issue, Article 75 of the TFEU (Title V of *the area of freedom, security and justice)*[21] should also be considered in this context. This article, among others, sets out an entitlement for the EU (Council and European Parliament) to adopt measures concerning terrorism prevention. Having regard to the above-mentioned provision, the question arises in what way establishing the EU competence to prevent terrorism distinguishes the scope of above-mentioned tasks from safeguarding national security. Bearing in mind that many of the EU member states consider activities linked with fighting terrorism as falling within the scope of national security, and thereby as falling within their exclusive scope of competence. This is one of the examples of how

---

[20] Working Document on surveillance of electronic communications for intelligence and national security purposes. Adopted on 5 December 2014, 14/EN WP 228, pp. 2–3

[21] Article 75 of the TFEU: 'Where necessary to achieve the objectives set out in Article 67, as regards preventing and combating terrorism and related activities, the European Parliament and the Council, acting by means of regulations in accordance with the ordinary legislative procedure, shall define a framework for administrative measures with regard to capital movements and payments, such as the freezing of funds, financial assets or economic gains belonging to, or owned or held by, natural or legal persons, groups or non-State entities. The Council, on a proposal from the Commission, shall adopt measures to implement the framework referred to in the first paragraph. The acts referred to in this Article shall include necessary provisions on legal safeguards.'

the EU legislative activities could be undertaken on the very edge between the EU and the member states powers of its member states.[22]

There has also been the matter regarding consideration about national security issue of Article 346(1)(a) of the TFUE.[23] It should be noted that this provision does not pertain explicitly to the area of national security. Despite its derogatory nature, this provision is substantial to the appropriate interpretation of national security clause. In the light of this provision, member states can adopt measures which in a different situation could be considered an infringement of the EU regulations. Such an interpretation is acceptable in view of essential interests of a member state's security (which might be defined as national security or external military security), bearing in mind that Article 346 of the TEU is a derogation and general clause.[24]

Taking into account all considerations regarding the national security legal definition, last but not least, the Charter of Fundamental Rights of the European Union should be mentioned. The EUCFR in its preamble laid down that the European Union respects the national identities of the member states. As revealed by this statement, it is indisputable that the above-mentioned rule is commonly applied within the EU *Acquis Communautaire*, and a proof of that is applying this rule not only in the EUCFR, but also in the EU treaties and in different various legal acts of the European Union.

3. OVERVIEW OF THE CASE-LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS AND THE COURT OF JUSTICE OF THE EUROPEAN UNION

The jurisprudence of the ECHR has surely contributed in a great way to determining some of the inherent components of the concept of national security. It is reasonable to point out that the protection of the member states' security, their constitutional order as well as democracy against a threat of espionage, terrorism or separatism per se qualify as activities remaining within the scope of national security.

One of the cases which should be mentioned is the case *C.G. and others v. Bulgaria*,[25] in which the ECHR found that 'the Court is naturally mindful of the fact that in the

---

22 In this case, one has to deal with so-called principle of 'the occupied field' refers to areas in which treaties have handed law and policy-making powers (competence) to the EU. When it happens, member states lose their powers (competence) in this area, even if the EU has not yet legislated. It comes to taking over of the competences by occupying field. Being active by any member state in the area, which is a subject to regulation is not possible anymore. This exemplifies a situation where the very sensitive and crucial issue of national security could be taken out from the countries, in the aftermath of the EE legislative measures undertaken by its institutions.

23 Article 346(1)(a): '1. The provisions of the Treaties shall not preclude the application of the following rules: (a) no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security.'

24 W. Sadowski, *Art. 346*, [in:] *Treaty of the Functioning of the EU*..., p. 3 (Articles 223–358).

25 ECtHR-C.G. and others v. Bulgaria, Application No. 1365/07, 24 July 2008 (1365/07), 24 April 2008, http://www.echr.ketse.com/doc/1365.07-en-20080424/view/

particular context of measures concerning national security, the requirement of foreseeability cannot be the same as in many other fields. In particular, the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to expel an individual on national security grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance. However, even where national security is at stake, the concepts of lawfulness and the rule of law in a democratic society require that deportation measures affecting fundamental human rights be subject to some form of adversarial proceedings before an independent authority or a court competent to effectively scrutinise the reasons for them and review the relevant evidence, if need be, with appropriate procedural limitations on the use of classified information. The individual must be able to challenge the executive's assertion that national security is at stake. While the executive's assessment of what poses a threat to national security will naturally be of significant weight, the independent authority or court must be able to react in cases where the invocation of this concept has no reasonable basis in the facts or reveals an interpretation of "national security" that is unlawful or contrary to common sense and arbitrary.'

In a different case before the ECHR, *Leander v Sweden*,[26] referring to the phrase 'necessary in a democratic society in the interests of national security', the Court stated that 'however, the Court recognises that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved. In the instant case, the interest of the respondent State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life.'

In another case, *Janowiec and Others v. Russia*,[27] the ECHR has stated that 'the judgment by the national authorities in any particular case in which national security considerations are involved is one which it is not well equipped to challenge. However, even where national security is at stake, the concepts of lawfulness and the rule of law in a democratic society require that measures affecting fundamental human rights must be subject to some form of adversarial proceedings before an independent body competent to review the reasons for the decision and the relevant evidence. If there was no possibility of challenging effectively the executive's assertion that national security was at stake, the State authorities would be able to encroach arbitrarily on rights protected by the Convention.'

[26] Leander v Sweden: ECHR No. 9248/81 from 26 March 1987. https://hudoc.echr.coe.int/eng#{%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}

[27] Janowiec and Others v. Russia Nos. 55508/07 and 29520/09, from 21 October 2013. https://hudoc.echr.coe.int/eng?i=001-127684

Among the recent judgments of the ECHR, the landmark case *Big Brother Watch and Others v. the United Kingdom* should be analysed in detail.[28] The case looked at three different types of surveillance: the bulk interception of communications, intelligence sharing and the obtaining of communications data from communications service providers. The Court expressly recognised the severity of the threats currently facing many contracting states, including the scourge of global terrorism and other serious crimes, such as drug trafficking, human trafficking, the sexual exploitation of children and cybercrime. It also recognised that advancements in technology have made it easier for terrorists and criminals to evade detection on the internet. It therefore held that states should enjoy a broad discretion in choosing how best to protect national security. Consequently, a state may operate a bulk interception regime if it considers that it is necessary in the interests of national security. That being said, the Court could not ignore the fact that surveillance regimes have the potential to be abused, with serious consequences for individual privacy. In order to minimise this risk, the Court has previously identified six minimum safeguards which all interception regimes must have. The safeguards are that the national law must clearly indicate: the nature of offences which may give rise to an interception order, a definition of the categories of people liable to have their communications intercepted, a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed.[29]

Furthermore, attention should be focused on the CJEU case law, which in recent years developed due to pending cases concerning mostly data retention, including issues related to data retention for the purpose of safeguarding national security. The CJEU has ruled, in several cases, on the retention of and access to personal data in the field of electronic communications. The resulting case-law, in which the Court found, among others, that member states could not require providers of electronic communications services to retain traffic data and location data in a general and indiscriminate way, caused concerns on the part of certain states that they may have been deprived of an instrument which they consider necessary to safeguard national security and to combat crime.[30] It would be very useful to get thorough the most interesting cases, taking into account conclusions regarding interpretation of the notion of national security.

---

28 Big Brother Watch and Others v. the United Kingdom: ECHR Nos. 58170/13, 62322/14 and 24960/15 from 25 May 2021. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]}

29 Q&A on the judgment Big Brother Watch and Others v. United Kingdom. European Court of Human Rights. 25 May 2021. https://www.echr.coe.int

30 Court of Justice of the European Union Press release No. 123/20 Luxembourg, 6 October 2020 Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others.

Thus, in the case Digital Rights Ireland and Others,[31] the Court declared Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC invalid on the ground that the interference with the rights to respect for private life and to the protection of personal data, recognised by the Charter of Fundamental Rights of the European Union, which resulted from the general obligation to retain traffic data and location data laid down by that directive was not limited to what was strictly necessary.[32]

In the judgment regarding the Tele2 Sverige and Watson and Others case,[33] the Court then interpreted Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (Directive on privacy and electronic communications). As regards the access of the competent national authorities to the retained data, the Court confirmed that the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in the directive, even if that objective is to fight serious crime, but it must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data. That legislation must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data. Access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in particular situations where, for instance, vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be inferred that the data might, in a specific case, make an effective contribution to combating such activities.[34]

---

31 Judgment of 8 April 2014, Digital Rights Ireland and Others (C-293/12 and C-594/12). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293

32 Court of Justice of the European Union Press release No 123/20 Luxembourg, 6 October 2020, pp. 1–2.

33 Judgment of 21 December 2016, Tele2 Sverige and Watson and Others (C-203/15 and C-698/15). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0203

34 Court of Justice of the European Union Press release No. 145/16 Luxembourg, 21 December 2016 Judgment in Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others.

Finally, in two recent judgments of the CJEU – *Privacy International* and *LQN*[35] – it not only clarified the scope of application of the national security clause in relation to domestic data retention regulations, but it also provided guidelines concerning the admissibility of such regulations when their introduction is necessary for state security objectives.[36] The CJEU stated that as regards the objectives that may justify such interferences (with the rights enshrined in the Charter) and, in particular, the objective of safeguarding national security, at issue in the main proceedings, it should be noted, at the outset, that Article 4(2) of the TEU provides that national security remains the sole responsibility of each member state. That responsibility corresponds to the primary interest in protecting the essential functions of the state and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the state itself, such as terrorist activities. The importance of the objective of safeguarding national security, read in the light of Article 4(2) of the TEU, goes beyond that of the other objectives referred to in Article 15(1) of Directive 2002/58, *inter alia*, the objectives of combating crime in general, even serious crime, and of safeguarding public security. Threats such as those referred to in above can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives.[37]

To sum up, the Court first addressed the scope of the national security exemption in relation to a general data retention obligation. It confirmed that, in principle, national security remains the exclusive responsibility of each member state. However, this does not mean that measures taken in this area are entirely outside the scope of the EU law. Indeed, it follows from the well-established case-law that limitations on rights and freedoms must

---

35 Judgments of 6 October 2020 in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others. https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-623/17

36 M. Rojszczak. National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts. Published online by Cambridge University Press: 15 November 2021. https://www.cambridge.org/core/journals/european-constitutional-law-review/article/national-security-and-retention-of-telecommunications-data-in-light-of-recent-case-law-of-the-european courts/BCE3F7879744C2BFEC06DBD40F1F4A59

37 https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=257834

be interpreted narrowly.[38] In addition, on that basis – in accordance with the principle of the effectiveness of the EU law – it is pointed out that the national security exception should be interpreted as applying only to activities carried out directly by public authorities and not by entities fulfilling a legal obligation imposed on them.[39]

However, the CJEU sends an ambivalent and somewhat conflicting message. On the one hand, Privacy International is arguably more than a strong reiteration of the position articulated in Tele2 Sverige, prohibiting indiscriminate transmission and interception of personal data even in the context of national security. Tele2 Sverige concerned data retention regimes for the purposes of combatting serious crime – as opposed to national security. Therefore, Privacy International goes a step further by imposing the same demands as articulated in Tele2 Sverige, but in the context of national security. It is arguably a step further because, in the Court's own words, 'the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives.'[40] In order to correctly draw conclusions from the Privacy International and LQN, it is worth emphasising that it is the struggle for competence at the intersection of data retention and national security. The EU institutions, including the CJEU, are institutionally inclined to determine national security narrowly, strengthening their own role in the area. The member states, on the other hand, have an institutional interest in keeping the EU institutions out of their national security issues. At the same time, the member states cannot avoid the growing European interdependence in security matters, so the struggle will continue.[41]

4. CONCLUSIONS

What are the implications arising from above-mentioned judgments of the CJEU? Arguably, the interpretation of national security clause which was adopted by the CJEU in Privacy International and LQN judgment will generate fundamental difficulties in the context of determining the boundary between the sphere of the legislative competences of the EU and the sphere of competences exclusively belonging to member states. The key point is proper interpretation of Article 4(2) of the TEU, which sets out the national security clause. The CJEU presented in recent judgments an interpretation which surely is not favourable for intelligence and security services of the EU member states. It should be stressed out that the

38 M. Rojszczak. *National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts*. Published online by Cambridge University Press: 15 November 2021.

39 Ibidem.

40 M. Zalnieriute. A Struggle for Competence: National Security, Surveillance and the Scope of EU law at the Court of Justice of European Union. University of New South Wales Law Research Series. Forthcoming (2022). Modern Law Review, 2021, No. 85(1), UNSWLRS 34, p. 21.

41 M. Zalnieriute. A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union. University of New South Wales Law Research Series. Forthcoming (2022). Modern Law Review, 2021, No. 85(1), UNSWLRS 34, p. 27.

interpretation of Article 4 of the TEU should be performed together with the interpretation of Article 5 of the TEU, which lays down the principle of conferral. Under Article 5, the limits of the EU competences are governed by the principle of conferral. The use of the EU competences is governed by the principles of subsidiarity and proportionality. In accordance with the principle of conferral, the EU shall act only within the limits of the competences conferred upon it by the member states in the Treaties to attain the objectives set out therein. Competences not conferred upon the EU in the Treaties remain with the member states. The principle of subsidiarity should also be mentioned. In compliance with this principle, in areas which do not fall within its exclusive competence, the Union shall act only if and insofar as the objectives of the proposed action cannot be sufficiently achieved by the member states, either at the central level or at the regional and local levels, but they can rather, by reason of the scale or effects of the proposed action, be better achieved at the EU level.

Another conclusion concerning the recent CJEU judgments (Digital Rights Ireland, Tele2/Watson and Privacy International and LQN) will distort the balance between treaties competences of the EU and EU member states. The CJEU consequently in subsequent judgments interpreted the national security clause in Article 4 of the TEU very narrowly. Such an interpretation will lead to the situation in which the CJEU will extend applying the EU law to fields loosely tied to national security. Judicial decisions made by the CJEU presented in the above-mentioned judgments will result in the fact that the requirements of CJEU from recent judgements which set out what legal norms should have legal regulations (e.g. regarding domestic law within the scope of data retention) will be interpreted as quasi-legislative activities within the scope, in which the EU does not own competences, in accordance to the primary EU law or such competences are very limited.

One of the most crucial questions, arising from above-mentioned judgments is how the EU member states will react. For instance, the interpretation of the CJEU presented in the Privacy International and LQN judgments was negatively assessed by the French authorities. The government representatives argued that the uncritical adoption of the CJEU interpretation would lead to the weakening of the effectiveness of intelligence and security services – including in terms of counteracting terrorist threats. It was also argued that the CJEU had misinterpreted the scope of the national security clause and, as a result, its ruling went beyond the scope of its competences. Hence, the government, based on *ultra vires* doctrine,[42] requested that the Conseil d'État recognise the Court of Justice's decision as having no effect in the French legal model. The Conseil d'État did not support the government's position.[43]

---

[42] *Ultra vires*, which may best be translated as 'beyond powers', refers to acts that overshoot the competences.

[43] M. Rojszczak. *National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts*. Published online by Cambridge University Press: 15 November 2021, p. 19.

Regardless of circumstances, it should be stated that for intelligence and security services the CJEU is a new, and presumably unwelcome, actor that has appeared on stage. One question that arises for such agencies is how to engage in a dialogue with it, taking onto account the fact that primary partners for a dialogue with the CJEU are not national administrative agencies, but the national courts.[44]

[44] I. Cameron. European Union Law Restraints on Intelligence Activities. *International Journal of Intelligence and CounterIntelligence*, Vol. 33, 2020, Iss. 3(5), June 2020, p. 460.

Bibliography

Austria

1. Government bill concerning Federal Law Gazette I 148/2021, SNG.

Belgium

1. The Act of 30 November 1998 regulating the intelligence and security services (Organic Act).
2. The Act of 11 December 1998 regarding the classification and the security clearances, certificates and advice (Classification Act).
3. The Act of 18 July 1991 regulating the supervision of police and intelligence services and of the Threat Analysis Coordination Body (Inspection Act).
4. The Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (Data Protection Act).
5. Act of 7 December 1998 organising an integrated policy force structured at two levels.
6. Royal Decree of 14 January 1994 creating the status of Administrator General and Deputy Administrator General of the VSSE.
7. Royal Decree of 5 December 2006 on the general administration and the support cell with the VSSE.
8. Royal Decree of 28 January 2015 establishing the National Security Council.
9. Royal Decree of 2 June 2015 establishing the Strategic Committee and Coordinating Committee for intelligence and security.
10. Rules of the House of Representatives.
11. Belgian Constitution. Act of 3 May 1880 concerning parliamentary inquiries.
12. Special Act of 8 August 1980 on the reform of institutions.
13. Flemish Parliament Decree of 1 March 2002 organising parliamentary inquiries.
14. Walloon Parliament Decree of 15 September 1982.
15. Order of 16 June 2017 of the United Assembly of the Joint Community Commission (Brussels).
16. Rules of Procedure regarding the Guidance Commission adopted by the Belgian Parliament on 26 March 2015.
17. Act of 11 December 1998 establishing the appeal body regarding security clearances, certificates and advice.
18. Act of 29 October 1846 establishing the Court of Audit.
19. Royal Decree of 13 December 2006 on the status of the VSSE field agents.
20. Criminal Code.
21. Code of Criminal Procedure.
22. Royal Decree of 2 October 1937 on the status of government staff.

23. State Council Coordinated Act of 12 January 1973.
24. Royal Decree of 4 September 2014.
25. Ministerial Decree of 16 October 2018 regarding the internal organisation, transfer of powers and authorisation to sign with the VSSE, concerning order placement and execution of public contracts and concerning various expenses.
26. The Belgian Constitutional Court further to the Court of Justice Judgment of 6 October 2020 (La Quadrature du Net et al. v. Premier ministre et al., C-511/18).
27. Explanatory memorandum to the Bill of the original Organic Act, DOC 49 - 0638/001.
28. Royal Decree of 20 March 2000 implementing the Act of 11 December 1999 regarding the classification and the security clearances, certificates and advice.
29. Royal Decree of 20 March 2000 executing the Act of 11 December 1999 regarding the classification and the security clearances, certificates and advice.
30. Belgian Nationality Code of 28 June 1984.
31. Act of 2 October 2017 regulating private and special security activities.
32. Federal and regional cooperation agreement regarding the recognition of cults.
33. Royal Decree of 10 October 2014 establishing the Centre for Cybersecurity Belgium.
34. ECHR Judgment of 19 September 2017 (Regner v. the Czech Republic, 35289/11).
35. ECHR Judgment of 17 December 2013 (Nikolova et Vandova v. Bulgaria, 20688/04).
36. ECHR Judgment of 16 April 2013 (Fazliyski v. Bulgaria, 40908/05).
37. General Data Protection Regulation (GDPR).
38. Act of 11 April 1994 regarding the publicity of government.
39. Act of 3 December 2017 establishing the Data Protection Authority

Bulgaria

1. State Agency for National Security Act (SANS Act), SG 2007.
2. Rules on the implementation of the SANS Act, adopted with a Decree of the Council of Ministers No. 23 of 2008, Promulgated SG No. 17/2008.
3. Act on the Management and Functioning of the System of National Security Protection (AMFSNSP), Promulgated, SG No. 61/2015.
4. Special Intelligence Means Act (SIMA), Promulgated, SG No. 95/1997.
5. Classified Information Protection Act (CIPA), Promulgated, SG No. 45/2002.
6. Regulation of the system of measures, tools and means for the physical security of the classified information, and terms and order for their use, adopted with a Decree of the Council of Ministers No. 52 of 2003 (Promulgated, SG No. 22/2003).

Croatia

1. Act on the Security Intelligence System of the Republic of Croatia, Official Gazette, Nos. 79/06 and 105/06 – amendment.
2. Act and the Criminal Procedure Act, Official Gazette, Nos. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19.
3. Act on Civil Servants, Official Gazette, Nos. 92/05, 140/05, 142/06, 77/07, 107/07, 27/08, 34/11, 49/11, 150/11, 34/12, 38/13, 37/13, 1/15, 138/15, 102/15, 61/17, 70/19, 98/19.
4. Act on the Obligations and Rights of State Officials, Official Gazette, Nos. 101/98, 135/98, 105/99, 25/00, 73/00, 30/01, 59/01, 114/01, 153/02, 163/03, 16/04, 30/04, 121/05, 151/05, 141/06, 17/07, 34/07, 107/07, 60/08, 38/09, 150/11, 22/13, 102/14, 103/14, 03/15, 93/16, 44/17, 66/19.

5. Act on Service in the Armed Forces of the Republic of Croatia, Official Gazette, Nos. 73/13, 75/15, 50/16, 30/18, 125/19.
6. Act on the Pension Insurance Rights of Active Servicemen, Police Officers and Civil Servants with Official Powers, Official Gazette, Nos. 128/99, 16/01, 22/02, 41/08, 97/12, 118/12.
7. Information Security Act, Official Gazette, No. 79/07.
8. Act on the Implementation of the General Data Protection Regulation, Official Gazette, No. 42/18.

The Czech Republic

1. http://www.public.psp.cz/en/sqw/snem.sqw?id=1563
2. Annual Report of the Security Information Service for 2020 – http://www.bis.cz/annual-reports/

Estonia

1. Security Authorities Act.
2. Police and Border Guard Act. Website: https://www.riigiteataja.ee/en/eli/521012022003/consolide
3. Law Enforcement Act. Website: https://www.riigiteataja.ee/en/eli/503032021004/consolide
4. Code of Criminal Procedure. Website: https://www.riigiteataja.ee/en/eli/527122021006/consolide
5. Regulation of the Government of the Republic considering the division of investigative jurisdiction between the Police and Border Guard Board and the KAPO. Website: https://www.riigiteataja.ee/akt/107052019004
6. Aliens Act. Website: https://www.riigiteataja.ee/en/eli/517082021004/consolide
7. Obligation to Leave and Prohibition on Entry Act. Website: https://www.riigiteataja.ee/en/eli/517082021005/consolide
8. Aviation Act. Website: https://www.riigiteataja.ee/en/eli/531122021004/consolide
9. Identity Documents Act. Website: https://www.riigiteataja.ee/en/eli/501112021001/consolide
10. Explosives Act. Website: https://www.riigiteataja.ee/en/eli/506042021003/consolide
11. Strategic Goods Act. Website: https://www.riigiteataja.ee/en/eli/ee/512022020002/consolide
12. National Defence Act. Website: https://www.riigiteataja.ee/en/eli/526042022005/consolide
13. State Secrets and Classified Information of Foreign States Act. Website: https://www.riigiteataja.ee/en/eli/521052020005/consolide

France

1. Law No. 78-17 of 6 January 1978 pertaining to data and freedoms.
2. Law No. 2015-912 of 24 July 2015 pertaining to intelligence.
3. Law No. 2015-1556 of 30 November 2015 pertaining to the monitoring of international electronic communications monitoring.
4. Law No. 2017-1510 of 30 October 2017 pertaining to domestic security and counterterrorism.
5. Law No. 2021-998 of 30 July 2021 pertaining to terror attack prevention and intelligence.
6. Decree No. 2009-1657 of 24 December 2009 pertaining to the National Security and Defence Council and the National Security and Defence General Secretariat.

7. Decree No. 2014-445 of 30 April 2014 pertaining to the missions and organisation of the General Directorate for Internal Security (DGSI).
8. Decree No. 2014-833 of 24 July 2014 pertaining to the inspection of intelligence services.

Greece

1. The Government Official Gazettes are posted on the website of the National Printing Service (http://www.et.gr/).
2. The Code of Governing the Hellenic Parliament, Official Gazette A' 106/1987 is posted on the website of the Hellenic Parliament (https://www.hellenicparliament.gr/).

The Netherlands

1. Intelligence and Security Services Act 2017 ('Wiv').
2. Kamerstukken II, 2016/17, 34 588, No. 3.
3. http://www.aivd.nl
4. http://www.ctivd.nl/over-ctivd/jaarverslagen
5. http://www.tib-ivd.nl/documenten

Poland

1. Journal of Laws of 1997, No. 78, item 483.
2. Journal of Laws of 1990, No. 30, items 179 and 180.
3. Journal of Laws of 2002, No. 2002, items 74 and 676.
4. Journal of Laws of 2006, items 104 and 708.
5. Act of 9 June 2006 – Provisions implementing the Act on the Military Counter-Intelligence Service and the Military Intelligence Service and the Act governing the performance of the Military Counter-Intelligence Service and the Military Intelligence Service officers' duties, Journal of Laws of 2006, No. 104, item 711.
6. Journal of Laws of 2006, No. 104, item 709.
7. MP 2021, item 483.
8. M. Bożek, *Służby specjalne oraz kryteria ich klasyfikacji na gruncie polskiego ustawodawstwa*, [in:] *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014.
9. Journal of Laws of 2021, items 1893, 2345 and 2447.
10. Order No. 163 of the Prime Minister of 26 September 2018 on granting the statute of the Internal Security Agency (MP of 2018, item 927).
11. Order No. 174 of the Prime Minister of 26 June 2002 on granting the statute of the Intelligence Agency (MP of 2021, item 811).
12. Order No. 72 of the Prime Minister of 6 October 2010 on granting the statute of the Central Anticorruption Bureau (MP of 2010, No. 76, item 953).
13. Order of the Minister of Defence of 21 April 2017 on granting the statute of the Military Counterintelligence Service (MP of 2017, item 431).
14. Order of the Minister of Defence of 28 May 2008 on granting the statute of the Military Intelligence Service (MP of 2008 No. 44, item 385).
15. Official Journal of 2019, items 742, 1781 and 2399.

16. Official Journal of 2020, items 1369 and 1856.
17. Official Journal of the European Union L 210 of 6 August 2008.
18. M. Gołaszewska, *Zadania ABW w zakresie zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (ed.), Warszawa 2021.
19. Journal of Laws of 2018, item 1799.
20. Journal of Laws of 2016, item 1024.
21. MP 2021, item 483.
22. P. Burczaniuk, *System nadzoru i kontroli nad służbami specjalnymi w Polsce – stan obecny na tle analizy prawno-porównawczej wybranych państw. Postulaty* de lege ferenda, [in:] *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, P. Burczaniuk (ed.), Warszawa 2017.
23. Journal of Laws of 2022, item 902.
24. R. Klejc, *Szef ABW jako podmiot zobowiązany do udostępniania informacji publicznej w trybie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej na tle dotychczasowej praktyki orzeczniczej sądów administracyjnych*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (ed.), Warszawa 2021.
25. B. Skowronek, *Charakterystyka stosunku służbowego funkcjonariuszy ABW ze szczególnym uwzględnieniem analizy fakultatywnych i obligatoryjnych przesłanek zwolnienia ze służby na podstawie wybranych orzeczeń sądów administracyjnych*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (ed.), Warszawa 2021.
26. Act of 6 June 1997 – the Code of Criminal Proceedings, Journal of Laws of 2021, item 534.
27. Act of 6 June 1997 – the Code of Execution of Criminal Sentences, Journal of Laws of 2021, item 53.
28. R. Brzozowski, *Czynności wykonywane przez funkcjonariuszy ABW na tle zadań ABW*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (ed.), Warszawa 2021.
29. S. Hoc, P. Szustakiewicz, *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*. LEX/el.2012.
30. P. Burczaniuk, *Zadania Szefa ABW w zakresie obowiązków informacyjnych*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (ed.), Warszawa 2021.
31. Explanatory Memorandum to the Government's Draft Act on the protection of personal data (https://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2410).

Romania

1. Law No. 51/1991 on the National Security of Romania, republished, with subsequent amendments and supplements.
2. Law No. 14/1992 on the Organisation and Operation of the Romanian Intelligence Service, with subsequent amendments and supplements.
3. Law No. 80/1995 on the Status of Military Staff, with subsequent amendments and supplements.

4. Law No. 182/2002 on the Protection of Classified Information, with subsequent amendments and supplements.
5. Law No. 415/2002 on the Organisation and Operation of the Supreme Council of National Defence, with subsequent amendments and supplements.
6. Law No. 535/2004 on Preventing and Countering Terrorism, with subsequent amendments and supplements.
7. Law No. 223/2015 on Military Pensions, with subsequent amendments and supplements.
8. Parliament Decision No. 22/2020 on Approving the National Defence Strategy for 2020–2024.
9. GO No. 26/1994 on the Food Allowance Granted, in Times of Peace, to the National Defence, Public Order and National Security Personnel and to People Held in Custody, republished, with subsequent amendments and supplements.
10. GO No. 121/1998 on the Material Liability of Military Staff, with subsequent amendments and supplements.
11. https://legislatie.just.ro/

Slovakia

1. Aláč, M. (2015). *Získavanie informácií na spravodajské účely a na účely trestného konania*. ISBN: 9788089603329.
2. Kočan, Š. and Selinger, P. (2013). *Bezpečnostné služby v Slovenskej republike*. ISBN: 978-80-8054-555-0.
3. Act of the National Council of the Slovak Republic, No. 46/1993 Coll. on the Slovak Information Service.
4. Act of the National Council of the Slovak Republic, No. 198/1994 Coll. on the Military Intelligence.
5. Act No. 166/2003 Coll. on the Protection of Privacy Against the Unauthorised Use of Technical-Intelligence Measures and on the Amendment and Supplementation of Certain Acts (Act on Protection Against Interception).
6. Act No. 452/2021 Coll. on Electronic Communications.
7. Act No. 480/2002 Coll. on Asylums and the Amendment of Certain Acts.
8. Act No. 404/2011 Coll. on the Residence of Foreigners and the Amendment and Supplementation of Certain Acts.
9. Act of the National Council of the Slovak Republic, No. 40/1993 Coll. on the Citizenship of the Slovak Republic.
10. Act No. 392/2011 Coll. on Trade in Defence-Related Products and on the Amendment of Certain Acts.

Sweden

1. The Police Act (1984:387).
2. The Electronic Communications Act (2003:389).
3. The Qualified Protected Identities Act (2006:939)
4. Act on Measures to Prevent Certain Particularly Serious Crime (2007:979).
5. The Protection Act (2010:305).
6. Act on the Gathering of Electronic Communications Data as Part of the Intelligence Activities of Law Enforcement Agencies (2012:278).

7. The Ordinance Containing Instructions for the Swedish Security Service (2014:1103).
8. Act on Measures Against Money Laundering and Terrorist Financing (2017:630).
9. The Protective Security Act (2018:585).
10. Act Concerning the Swedish Security Service's Processing of Personal Data (2019:1182).
11. Act on Equipment Interference (2020:62).
12. Act Concerning Special Controls in Respect of Foreigners (1991:572).
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
14. Directive (EU) 2016/680 of the European Parliament and of the Council of 26 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data, and repealing the Council Framework Decision 2008/977/J11A.
15. http://www.sakerhetspolisen.se
16. https://www.efes.se
17. https://polisen.se

National Security Clause in the EU Law and Its Implications for Intelligence and Security Services

1. Peers, S. (1996). National Security and European Law: Introduction. *Yearbook of European Law*, Vol. 16, Iss. 1, p. 1.
2. Makinda, S.M. (1998). *Sovereignty and Global Security, Security Dialogue*, Sage Publications, Vol. 29(3), Iss. 29, pp. 281–292.
3. Osisanya, S. National Security versus Global Security. *United Nations – UN Chronicle*.
4. Holmes, K.R. (2014). *What Is National Security? 2015 Essays*. 7 October 2014. The Heritage Foundation.
5. National Security Strategy of the Republic of Poland 2020.
6. Government of the Netherlands/Home/Topics/Counterterrorism and National Security/National Security.
7. Report on national security and European case-law prepared by the Research Division of the ECtHR, para. 25, p. 4.
8. Council of Bars & Law Societies of Europe. (2019). *CCBE Recommendations on the Protection of Fundamental Rights in the Context of 'National Security'*, pp. 4–5.
9. Treaty on European Union, an international agreement approved by the heads of government of the states of the European Community (EC) in Maastricht, Netherlands, in December 1991. Ratified by all EC member states (voters in Denmark rejected the original treaty but later approved a slightly modified version), the treaty was signed on 7 February 1992 and entered into force on 1 November 1993.
10. The Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, signed in Amsterdam on 2 October 1997, entered into force on 1 May 1999.
11. The TEU is based on the Maastricht Treaty which marked a new stage of European integration by going beyond the original economic objective (a common market). It opened the way to political integration with a transition from the European Economic Community (EEC) to the

European Union (EU). Signed on 13 December 2007, the Lisbon Treaty – which comprises the TEU and the TFEU – entered into force on 1 December 2009.
12. European Convention on Human Rights. The Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights, was opened for signature in Rome on 4 November 1950 and came into force on 3 September 1953.
13. *Case Esbester vs United Kingdom* (18601/91) (1994), Commission decision from 2 April 1993.
14. The Treaty on the Functioning of the European Union (TFEU), as a result of the Lisbon Treaty, was developed from the Treaty establishing the European Community (TEC or EC Treaty), as put in place by the Treaty of Maastricht. The EC Treaty itself was based on the Treaty establishing the European Economic Community (TEEC), signed in Rome on 25 March 1957. Signed by 27 EU countries (Croatia did not join the EU until 2013) on 13 December 2007, the TFEU entered into force on 1 December 2009.
15. Working Document on surveillance of electronic communications for intelligence and national security purposes. Adopted on 5 December 2014, 14/EN WP 228.
16. W. Sadowski, *Art. 346*, [in:] *Treaty of the Functioning of the EU*.
17. ECtHR-C.G. and others v. Bulgaria, Application No. 1365/07, 24 July 2008 (1365/07), 24 April 2008.
18. Leander v Sweden: ECHR No. 9248/81, 26 March 1987.
19. Janowiec and Others v. Russia No. 55508/07 and 29520/09, 21 October 2013.
20. Big Brother Watch and Others v. the United Kingdom: ECHR Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021.
21. Q&A on the judgment Big Brother Watch and Others v. the United Kingdom. European Court of Human Rights, 25 May 2021.
22. Court of Justice of the European Union Press release No. 123/20 Luxembourg, 6 October 2020 Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others.
23. Judgment of 8 April 2014, Digital Rights Ireland and Others (C-293/12 and C-594/12)
24. Court of Justice of the European Union press release No. 123/20 Luxembourg, 6 October 2020, pp. 1–2.
25. Judgment of 21 December 2016, Tele2 Sverige and Watson and Others (C-203/15 and C-698/15.
26. Court of Justice of the European Union Press release No. 145/16 Luxembourg, 21 December 2016 Judgment in Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others.
27. Judgments of 6 October 2020 in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others.
28. M. Rojszczak. *National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts*. Published online by Cambridge University Press: 15 November 2021, p. 3.
29. M. Zalnieriute. A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union. University of New South Wales Law Research Series. Forthcoming (2022). *Modern Law Review*, 2021, No. 85(1), UNSWLRS 34, p. 21.
30. I. Cameron. European Union Law Restraints on Intelligence Activities. *International Journal of Intelligence and CounterIntelligence*, Vol. 33, 2020, Iss. 3(5), June 2020, p. 460.

About the Scientific Editor

Piotr Burczaniuk – PhD in Law, Assistant Professor in the Department of Theory and Philosophy of Law at the Faculty of Law and Administration of Cardinal Stefan Wyszyński University in Warsaw. Attorney-at-law, member of the Lublin Bar Association of Attorneys-at-Law. Lawyer – Legislator, member of the Polish Legislation Society.

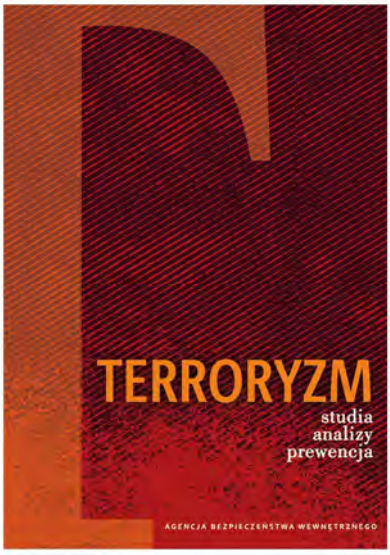
He graduated from the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw. He completed numerous post-graduate studies and courses, including National Security at the University of Warsaw, post-graduate studies in Internal Security, with particular focus on information protection at the University of Warsaw, and post-graduate studies in Business Law at the Cardinal Stefan Wyszyński University in Warsaw. He completed legislative training at the Government Legislation Centre in Warsaw and defended his PhD dissertation with honours on the issues of creating economic law in Poland in the context of European legislation.

His scientific activity is focused particularly within the field of the legal aspects of national security and functioning of the legal protection authorities. He is the author and editor of works in the field of general jurisprudence, constitutional law and economic law, including:

- editor and co-author of the monograph *Powers of Intelligence and Security Services from the Perspective of Contemporary Threats to National Security*, ed. ABW 2017
- co-author of the monograph *Analysis of Legal Solutions in the Field of the Functioning of Intelligence and Security Services in Selected Countries*, ed. ABW 2017
- author of the monograph *Creating Economic Law in Poland*, ed. Difin 2021
- co-author of the monograph *Selected Problems of Theory and Philosophy of Law*, ed. Difin 2021
- editor and co-author of the monograph *The Legal Aspects of the Functioning of the Intelligence and Security Services on the Example of the Internal Security Agency*, ed. ABW 2021.

For his achievements in scientific and research work, in 2022 he was awarded the Badge for Merit for Legislation by the Polish Prime Minister.

INTERNAL SECURITY AGENCY PUBLISHING HOUSE



The Publishing House of the Internal Security Agency, launched in 2009, issues peer-reviewed scientific monographs devoted to, inter alia, the history of Polish secret services andbroadly understood legislative matters as well as publications concerning statutory tasks of the Internal Security Agency. It is also the publisher of two scientific journals: "Internal Security Review" and "Terrorism – studies, analyses, prevention".

The biannual "Internal Security Review" is a scientific journal published since 2009 with a focus on interdisciplinary issues related to the protection of the constitutional order of the state. The topics of the articles cover a wide range of areas related to national security, e.g. legal issues, activities of institutions and organizations responsible for the protection of the constitutional order of the state as well as analyses of current and projected security status in the national and international perspectives.

The biannual "Terrorism – studies, analyses, prevention" is a scientific journal established in 2021, devoted to interdisciplinary issues related to anti-terrorist protection and building resilience to terrorist threats in the national and international perspectives. It is meant to be a platform for the exchange of scientific ideas and experience, connecting the academic world and representatives of institutions and services that cooperate with each other within the Interministerial Team for Terrorist Threats, which is the coordination centre of the anti-terrorist system of the Republic of Poland. The topics of the articles cover a wide range of areas related to terrorist threats as well as methods of reacting and building resilience to such threats, concerning both state and international organizations. Terrorist prevention issues constitute a very important part of the journal.

Authors of the articles are officers of the Internal Security Agency and other uniformed services of the Republic of Poland, academics from universities, scientific institutions and research centers as well as specialists in fields related to the history of special services and the protection of national security. The scientific editors and reviewers supervise the scientific rigor of the articles.

Since July 2021, the Publishing House of the Internal Security Agency has been included in the Polish ministerial list of publishers issuing peer-reviewed scientific monographs. Number of points – 80 (LEVEL I).

For further information concerning the Publishing House of the Internal Security Agency, including terms of cooperation, please visit: www.abw.gov.pl/pub/.

(Part of Foreword)
The basic idea of this monograph is to present institutional models of the Euro-Atlantic intelligence and security services to European readers. It continues a series of legal monographs devoted to the problems concerning intelligence and security services initiated in 2017 by Prof. Piotr Pogonowski – the then Head of the Internal Security Agency – published by the Publishing House of the Internal Security Agency. [...] The value of this publication is evidenced by the fact that it was written by a sizeable group of authors of individual chapters, i.e. 26 legal experts representing the aforementioned 19 European countries. Furthermore, substantive supervision was assumed by the University of Cardinal Stefan Wyszyński in Warsaw. All these aspects make this monograph a valuable component of the European literature on intelligence and security services.

Col. Krzysztof Wacławek
Head of the Internal Security Agency

(Part of Preface)
This publication is therefore intended to fill the aforementioned gaps, presenting organisational models of the intelligence and security services in selected European countries. I invited 26 legal experts from 19 Central and Western European countries to cooperate on this project. Each of them, based on his or her expertise in the field of the legal systems of their respective countries, wrote, individually or within a research team, one chapter devoted to each country, using a single methodological scheme. [...] I hope that this monograph will prove to be useful in the field of legal theory and would be well received by the practitioners interested in the problems concerning the intelligence and security services. I believe that the material gathered in this publication may be used for further research on the organisational models of these institutions.

Piotr Burczaniuk, PhD
Scientific Editor

ISBN 978-83-964225-0-7