Foreign Intelligence Gathering Laws

European Union • United Kingdom
France • Netherlands • Portugal • Romania • Sweden

December 2014

The Law Library of Congress, Global Legal Research Center
(202) 707-6462 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

Contents

Comparative Summary

Peter Roudik
Director of Legal Research

This report contains information on laws regulating the collection of intelligence in the European Union and selected European Union (EU) Member States. It begins with a comprehensive overview of applicable EU legislation. Because issues of national security are included in the jurisdiction of individual EU Member States and are regulated by domestic legislation, France, Netherlands, Sweden, and the United Kingdom, which are viewed as having mass surveillance operations, together with Portugal and Romania, are then surveyed to provide examples of how EU Members States control activities of their intelligence agencies and what restrictions are imposed on information collection. All EU Member States follow EU legislation on personal data protection, which is a part of the common European Union responsibility.

It appears that all countries surveyed attempt to maintain a balance between law enforcement and national security needs on the one hand and rights to privacy and personal data protection on the other. In all of the countries, intelligence functions are divided among general intelligence and security services, military and financial intelligence, and the police. While in the United Kingdom, Netherlands, and Portugal intelligence agencies work according to principles established by a comprehensive statute, in Sweden and Romania individual laws address issues specifically for individual intelligence agencies, and in France the work of these agencies is primarily based on varied executive decisions. This explains why most of the countries have no single legislative regime that applies to matters of surveillance, interception of communications, and privacy protection.

While the legislative institutions of the surveyed countries are involved in general oversight of their respective intelligence agencies, special government bodies for reviewing the legality of interception surveillance and privacy issues have also been created. These special bodies focus on how information is stored, shared among security agencies within the country and abroad, destroyed, and made available to interested individuals. Limitations on intelligence collection are established by national constitutions, criminal procedure laws, and special legislation, and are aimed at the general defense of rights and freedoms. They include restrictions in terms of scope, duration, and subject matter of surveillance activities. The use of special powers, including communications surveillance, require express permission from the Minister of Interior (Netherlands), issuance of a judicial order (Romania), or an approval warrant authorized by the Secretary of State (United Kingdom). All national laws of the surveyed countries provide for special instruments to preserve personal data. At the same time, because of gaps in legislation and the national legal systems' weaknesses, these measures are not always effective in regard to privacy protection.

European Union

Theresa Papademetriou
Senior Foreign Law Specialist

SUMMARY Electronic intelligence falls within the domain of the Member States of the European Union (EU), who have sole responsibility for safeguarding their internal security. Electronic surveillance conducted by national law enforcement authorities is inherently linked to the right to privacy and personal data protection. Such rights are enshrined in European Union treaties and secondary legislation as well as in Conventions adopted by the Council of Europe and in the International Covenant on Civil and Political Rights, which binds EU Members. The Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms guarantee the rights to privacy and personal data protection to everyone within the jurisdiction of the EU Member States. Legal issues arising from electronic surveillance that may infringe on the human rights of individuals are not subject to review by the Court of Justice of the EU. Aggrieved individuals, upon exhausting legal remedies at the national level, may bring their cases to the European Court of Human Rights in Strasbourg for a final review.

Following the Snowden revelations in the United States and press reports of mass electronic surveillance conducted by law enforcement authorities of several EU Members, the European Parliament adopted the Resolution on the US NSA Surveillance Programme, Surveillance Bodies in Various (EU) Members States and Their Impact on EU Citizens' Fundamental Rights. Moreover, the United Nations General Assembly, in a resolution adopted in 2013, urged UN Members to review their legislation on secret surveillance.

I. Introduction

Under European Union (EU) treaties, foreign electronic surveillance conducted by national law enforcement authorities of the twenty-eight EU Member States falls within the domain of the EU Members. The Treaty on European Union provides that "national security remains the sole responsibility of each Member State,"[1] and, hence, the EU arguably lacks competence to legislate in this area. Moreover, based on the Treaty on the Functioning of the EU, the Court of Justice of the EU does not have jurisdiction over cases that involve surveillance conducted by national authorities in order to safeguard the internal security of the EU Members.[2]

In conducting electronic surveillance, either foreign or domestic, EU Members are required to maintain a balance between the needs of law enforcement authorities and respect for the fundamental rights to privacy, personal data protection, and private and family life, as such rights are guaranteed in domestic legislation, EU law, and international agreements, including the

[1] Consolidated Version of the Treaty on European Union (TEU) art. 4, para. 2, 2012 O.J. (C 326) 13http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012M/TXT.

[2] Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) art. 276, 2012 O.J. (C 326) 47, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012E/TXT.

European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHRFF) and the International Covenant on Civil and Political Rights,[3] by which EU Members are bound. Under settled case law of the European Court of Human Rights, national enforcement authorities are required, when conducting electronic surveillance, to justify such activity against the privacy of individuals on the basis of a law that sets forth clearly defined grounds, including national security and public safety, and adheres to the principles of necessity and proportionality.

A number of EU Member States have been identified as engaging in large-scale surveillance. In the aftermath of the Snowden revelations in the United States, it was reported that a number of EU Members, including France,[4] Germany,[5] Sweden,[6] and the United Kingdom,[7] were allegedly involved in mass surveillance operations in cooperation with the United States. The allegations spurred a debate at the EU level with the European Parliament playing a leading role among the EU institutions by instructing the Civil Liberties Committee to conduct an inquiry. The inquiry led to the adoption of the Resolution on the US NSA Surveillance Programme, Surveillance Bodies in Various EU Members States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs.[8]

II. Electronic Surveillance: Competence Issues

Competence in the area of surveillance between the EU and its Member States is delineated in a number of articles found in the Treaty on European Union (TEU) and the Treaty on the Functioning of the EU (TFEU). Article 4, paragraph 2 of the TEU states that the Union "shall respect [the Member States'] 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."[9] In a similar vein, article 72 of the TFEU stipulates that title V of the Treaty pertaining to the Area of Freedom, Security and

[3] International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, entry into force Mar. 23, 1976, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[4] Angelique Chrisafis, *France 'Runs Vast Electronic Spying Operation Using NSA-style Methods': Intelligence Agency Has Spied on French Public's Phone Calls, Emails and Internet Activity, Says Le Monde Newspaper*, THE GUARDIAN (July 4, 2013), http://www.theguardian.com/world/2013/jul/04/france-electronic-spying-operation-nsa.

[5] *The German Prism: Berlin Wants to Spy Too*, SPIEGEL ONLINE INTERNATIONAL (June 17, 2013), http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129.html.

[6] Jordan Shilton, *Swedish Intelligence Service Spying on Russia for US National Security Agency*, GLOBAL RESEARCH (Dec. 2013), http://www.globalresearch.ca/swedish-intelligence-service-spying-on-russia-for-us-national-security-agency/5362967.

[7] *NSA Leaks: UK and US Spying Targets Revealed*, BBC News (Dec. 20, 2013), http://www.bbc.com/news/world-25468263.

[8] European Parliament Resolution 2013/2188 (INI) of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various EU Members States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN&ring=A7-2014-0139.

[9] TEU, *supra* note 1, art. 4, para. 2.

Justice, "shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security."[10] Moreover, article 73 of the TFEU allows the Member States to "organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the [competent national agencies] responsible for safeguarding national security."[11]

Whereas electronic surveillance is a state function, as the European Parliament has noted,[12] the EU also possesses some competence concerning the internal security of the EU on the grounds of article 67, paragraph 3 of the TFEU. The article states that the EU "shall endeavor to ensure a high level of security, through measures to prevent and combat crime."[13] The EU has exercised such competence by legislating and concluding international agreements, such as the Terrorist Financing Tracking Programme (TFTP) and Passenger Name Record (PNR) Agreement with the United States,[14] designed to fight terrorism and other forms of serious crime, and by establishing agencies, such as EUROPOL[15] and the Office of the EU Counter-terrorism Co-ordinator, tasked with combating terrorism and organized crime.[16] The Parliament takes the position that the EU enjoys competence in the field of security because of the overlap of the notions of "national security," "internal security," "internal security of the EU," and "international security."[17]

A corollary of the EU's lack of competence in the area of surveillance is its lack of authority to legislate on secret surveillance in order to limit it and/or impose stricter safeguards. In the event that the Commission, using its right of initiative, introduced legislation on the subject, it would not be enforceable given the lack of jurisdiction of the European Court of Justice on security matters.

III. Privacy and Personal Data Protection Issues

Electronic surveillance inevitably involves the collection and storage of personal data, access by law enforcement authorities to such data, and the possible infringement of the rights to privacy and the protection of personal data.

---

[10] TFEU, *supra* note 2, art. 72.

[11] *Id*.

[12] Resolution 2013/2188 (INI), *supra* note 8.

[13] TFEU, *supra* note 2, art. 67, para. 3.

[14] Press Release, European Commission, EU-US Agreements: Commission Reports on TFTP and PNR (Nov. 27, 2013), http://europa.eu/rapid/press-release_IP-13-1160_en.htm.

[15] *Europol's Priorities*, EUROPOL, https://www.europol.europa.eu/content/page/europol%E2%80%99s-priorities-145 (last visited Dec. 4, 2014).

[16] *EU Counter-terrorism Co-ordinator*, COUNCIL OF THE EUROPEAN UNION, http://www.consilium.europa.eu/policies/fight-against-terrorism/eu-counter-terrorism-co-ordinator?lang=en (last visited Dec. 4, 2014).

[17] Resolution 2013/2188(INI), *supra* note 8, para. Y.

Under EU law, the right to privacy and the right to protection of personal data are two distinct fundamental human rights.[18] These rights are also guaranteed in the legal systems of the EU Member States and in international agreements to which the EU parties are signatories, including the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHRFF).

The Charter of Fundamental Rights of the European Union (CFR), which acquired binding status on December 1, 2009, recognizes the right to privacy in article 7 and the right to the protection of one's personal data in article 8.[19] Furthermore, article 8 reaffirms the principle that personal data must be processed fairly and for specific purposes, based on the consent of the individual concerned or some other legitimate purposes laid down by law. It also recognizes the right of individuals to access the data collected and the right to have it rectified, in case of inaccuracy or incompleteness. Compliance with such rules is entrusted to the control of an independent authority established by the EU Member States.[20] The right to personal data may be restricted by law in order to strike a balance with the freedoms and rights of others and public safety and security, subject to the principle of proportionality, which is established in the EU and in the legal systems of the Member States.[21]

The TFEU recognizes the right of every individual to his/her personal data—that is, individuals own their data.[22] It also introduced a new and specific legal basis for the adoption of rules on data protection and granted authority to the EU legislative bodies (Parliament and Council) to adopt rules concerning the processing of personal data in the field of judicial cooperation in criminal matters, and police cooperation in the cross-border and domestic processing of personal data.[23]

The right to respect for private and family life, home, and correspondence is established in article 8 of the ECHRFF, to which all EU Members are also participating states as members of the Council of Europe.[24] The ECHRFF recognizes, however, that there are circumstances in a

[18] The right to privacy is also protected by article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHRFF), CETS No. 005 (1950), http://www.echr.coe.int/Documents/Convention_ENG.pdf, to which all EU Member States are states parties, as members of the Council of Europe. In addition, automatic processing of personal data is protected and governed by the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and Its Protocol, ETS No. 108 (1981), http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm. Recently, the Council of Europe began revising the 1981 Convention to bring it in line with contemporary technology and ensure harmonization with EU legal reforms. The Consultative Committee of the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (ETS No. 108), *Modernization of Convention 108: New Proposals* (Mar. 5, 2012), http://www.coe.int/t/dghl/standard setting/dataprotection/tpd_documents/T-PD-BUR_2012_01Rev_en.pdf.

[19] Charter of Fundamental Rights of the European Union, 2010 O.J. (C 83) 02, http://eur-lex.europa. eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF.

[20] *Id*. art. 8.

[21] *Id*. art. 52(1).

[22] TFEU, *supra* note 2, art. 16.

[23] *Id*. art. 16, para. 2.

[24] ECHRFF, *supra* note 18, art. 8.

democratic society where it may be necessary for the state to interfere with this right, but only in accordance with the law and for certain clearly defined grounds, such as national security, public safety, economic well-being, the prevention of crimes, and the protection of the rights and freedoms of others.[25] When such interference by public authorities acting in their official capacities does occur, article 13 of the ECHRFF requires a means of redress for the affected individual.[26]

A. Directive 95/46/EC on Personal Data Protection

Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data is the basic framework legislation in the EU on personal data protection.[27] The Directive provides strong protections applicable to the processing of personal data of persons living within the jurisdiction of the EU Member States. Pursuant to Directive No. 95/46/EC on personal data protection, the ownership of personal data belongs to individuals who have legal rights over the collection and processing of personal data. One of the key requirements for the processing of personal data is that the data subject must unambiguously give his/her consent, after being informed that his/her data will be processed.

Pursuant to the Directive, the data subject has the right of access, as provided for in article 12, which means that the data subject is entitled to information regarding any processing of his/her data, the purposes of processing, the categories of the data, and the recipients of the data.[28] The basic principles governing the processing of one's personal data are the following:

- Finality: Data must be collected for an explicit, specific, and legitimate purpose.
- Transparency: Individuals must be informed of the data collected and the purpose of collection.
- Legitimacy: Processing must be occur for a legitimate reason pursuant to article 7 of the Directive.
- Proportionality: The personal data collected must be adequate, relevant, and not excessive in relation to the purpose of collection.
- Accuracy and Retention of the Data: Individuals' records must be accurate and up to date. False or inaccurate data must be corrected.

In 2012, the Commission drafted two legislative pieces in order to reform EU legislation on privacy and data protection: (a) a draft regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data

[25] *Id*. art. 8.

[26] *Id*. art. 13.

[27] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[28] *Id*. art. 12.

Protection Regulation),[29] and (b) a Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities with regard to criminal offenses.[30]

B. Confidentiality of Communications

Confidentiality of communications is a principle enshrined in the legal systems of the EU Member States. At the EU level, confidentiality of communications is stipulated in Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications).[31] In particular, article 5 of the Directive requires that EU Members "prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than the users, without the consent of the users concerned, except when legally authorized to do so in accordance with article 15(1)."[32]

C. Exemptions

Interception or surveillance is permitted on the grounds of national security; defense and public security; and the prevention, investigation, detection, and prosecution of criminal offenses or of unauthorized use of an electronic communications system, as referred to in article 13(1) of Directive 95/46/EC.[33]

EU Members are also allowed to adopt legislation on data retention for a limited period and based on the same grounds provided above.[34]

D. Data Retention

Prior to its invalidation in April 2014, Directive No. 2006/24/EC (the Data Retention Directive),[35] required the providers of publicly available electronic communications services or

[29] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final (Jan. 15, 2012), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

[30] Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, COM (2012) 10 final (Jan. 25, 2012), http://eur-lex.europa.eu/LexUriServ /LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.

[31] 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) art. 5, 2002 O.J. (L 201) 37, http://eur-lex.europa.eu/LexUriServ/LexUri Serv.do?uri=OJ:L:2002:201:0037:0047:EN:PDF.

[32] *Id*. art. 5(1).

[33] *Id*. art. 15(1).

[34] *Id*.

[35] 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

public communications networks to retain traffic and location data belonging to individuals or legal entities. Such data included the calling telephone number and name and address of the subscriber or registered user, user IDs (a unique identifier assigned to each person who signs with an electronic communications service), Internet protocol addresses, the numbers dialed, and call forwarding or call transfer records. The retention period was to last for a minimum period of six months and up to two years, and the sole purpose of processing and storing the data was to prevent, investigate, detect, and prosecute serious crimes, such as organized crime and terrorism. The content of the communications of individuals was not retained.

On April 8, 2014, the Grand Chamber of the Court of Justice of the European Union (CJEU) issued a judgment declaring the Directive invalid.[36] The Directive was challenged on the grounds of infringement of the right to private life, and the right to the protection of personal data of individuals, as guaranteed in articles 7 and 8, respectively, of the Charter of Fundamental Rights of the European Union.

In examining the issue of interference with the rights to privacy and the protection of personal data, the CJEU made the following observations:

- The obligation imposed on providers of electronic communications services or public communications networks "constitutes in itself an interference with the rights guaranteed by article 7 of the Charter,"
- Access of the national authorities to data "constitutes a further interference with that fundamental right," and
- The interferences described above also violate the right to protection of personal data.[37]

The CJEU reasoned that the Directive did not establish clear and precise rules that regulate the "extent of interference with the fundamental rights of Art. 7 and 8 of the Charter."[38] Therefore, it concluded that the Directive "entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."[39]

The CJEU also held that the security and protection of personal data cannot be fully guaranteed in the absence of review of compliance by an independent authority of the rules on data protection, as required by article 8 of the Charter of Fundamental Rights.[40]

---

or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

[36] Grand Chamber, Digital Rights Ireland Ltd. (C–293/12) v. Minister for Communications, Marine and Natural Resources (Apr. 8, 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1.

[37] *Id*. paras. 34–36.

[38] *Id*. para. 65.

[39] *Id*.

[40] *Id*. para. 66.

IV. Case Law

Legal challenges to intelligence operations on the grounds of infringing the rights of the individual (such as the right to privacy freedom of expression, and a remedy) or because the intelligence operations are not conducted in accordance with the applicable law and are in violation of the standards of necessity and proportionality are not subject to review by the Court of Justice of the EU, as explicitly stated in article 276 of the TFEU:

> in exercising its powers regarding the provisions of Chapters 4 and 5 of Title V of Part Three relating to the area of freedom, security and justice, the Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.[41]

Such challenges can be brought before the European Court of Human Rights (ECHR), however. In general, the ECHR has found that the "mere existence of legislation allowing secret surveillance constitutes an interference with private life such that the necessity and legality requirements of article 8 of the European Convention on Human Rights must be met."[42] The ECHR has also found that emails, telephone communications, faxes, and Internet usage fall within the ambit of article 8 of the Convention.[43]

As far as the legality requirement, the ECHR has a strict requirement that surveillance activities must be based on a law and not conducted as matter of policy.[44]

In considering the legality of various surveillance programs followed by Members of the Council of Europe, the ECHR has concluded that the following key features are in compliance with article 8 of the Convention:

- Surveillance was performed in compliance with a law adopted by a state's legislature;
- the law exactly defined the purposes for which surveillance may be undertaken;
- The stated purposes were true and not used as a pretext; and
- Surveillance was conducted because of serious ground that the individual monitored was planning or had committed a serious criminal offense.[45]

[41] TFEU, *supra* note 1, art. 276.

[42] SARAH ST. VINCENT, CENTER FOR DEMOCRACY & TECHNOLOGY, INTERNATIONAL LAW AND SECRET SURVEILLANCE: BINDING RESTRICTIONS UPON STATE MONITORING OF TELEPHONE AND INTERNET ACTIVITY 9 (Sept. 4, 2014) (citing Weber & Saravia v. Germany (2006) & Levey v. Bulgaria).

[43] Grand Chamber, Digital Rights Ireland Ltd. (C–293/12), at 9.

[44] *Id*. at 10.

[45] *Id*. at 12.

V. Large-scale Surveillance and Compatibility with Human Rights

As stated above, at the EU level, large-scale surveillance conducted by government agencies of the EU Member States has raised concerns as to the compatibility of such activities with human rights standards.

The Parliament's Resolution on the US NSA Surveillance Programme, Surveillance Bodies in Various EU Members States and Their Impact on EU Citizens' Fundamental Rights has value as a political statement, but it lacks binding force. It urges the EU Members to discontinue the mass collection of data and to ensure that national laws and policies on electronic surveillance are in line with EU and Council of Europe standards. It also proposed to establish at the EU level a high-level group to monitor progress. In March 2014, the Parliament also requested the EU Agency for Fundamental Rights (FRA) to conduct research on the impact of large-scale surveillance on fundamental rights and to review whether individuals whose data are collected by intelligence agencies have adequate remedies against such practices. The FRA findings will be published shortly.[46]

A study conducted by the Directorate General for Internal Policies of the European Parliament, entitled *National Programs of Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law*, examines mass surveillance practices in four EU countries: France, Germany, Sweden, Netherlands, and the United Kingdom.[47] The study indicates that cooperation with foreign intelligence services appears to be a common practice. The study cites the so-called "Five Eyes" network, which comprises the US, UK, Canada, Australia, and New Zealand, that originated from a 1946 multilateral agreement for cooperation in signals intelligence, and which has extended over time in terms of activities (Echelon, and now Fornsat).[48] The US also engages in cooperative relationships with "second-tier" and "third-tier" partners such as France and Germany.[49]

The report indicates that some legal regimes operate on the basis of orders issued by special courts (for instance, in Sweden), while others were based on warrants issued by the government (the UK and Netherlands) or through an authorization role accorded to specially appointed oversight bodies (Germany, France, and Netherlands).[50]

---

[46] *National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies*, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and (last visited Dec. 5, 2014).

[47] EUROPEAN PARLIAMENT DIRECTORATE GENERAL FOR INTERNAL POLICIES, NATIONAL PROGRAMMES FOR MASS SURVEILLANCE OF PERSONAL DATA IN EU MEMBER STATES AND THEIR COMPATIBILITY WITH EU LAW (hereinafter MASS SURVEILLANCE STUDY) 24 (Oct. 2013), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf.

[48] For more information on on surveillance, including Echelon/Fornsat, see EUROPEAN PARLIAMENT, INTERCEPTION CAPABILITIES 2014, http://www.europarl.europa.eu/document/activities/cont/201309/20130916ATT71388/20130916ATT71388EN.pdf.

[49] MASS SURVEILLANCE STUDY, *supra* note 47, at 24.

[50] *Id*. at 25.

With regard to oversight, the report found that in several Member States oversight bodies encounter a number of constraints that limit their ability to scrutinize the intelligence agencies' surveillance practices. In Sweden, the two main oversight institutions—the intelligence court and the Statens inspektion för försvarsunderrättelseverksamheten (Siun, State Inspection for Defense Intelligence Activity)—are deemed to be insufficiently independent. France's main oversight body, the Commission nationale pour les interceptions de securité (CNCIS, National Commission for Security Interceptions), was found to be substantially constrained in its reach, because it has limited administrative capacity. The report also identified gaps in the UK's intelligence oversight regime, as evidenced by the statement released in July 2014 by the Intelligence Security Committee on the Government Communications Headquarters' (GCHQ's) alleged interception of communications under the PRISM program.[51]

The report also found that the surveillance programs operated by the Member States endanger the EU principle of "sincere cooperation," enshrined in article 4.3 of the Treaty on the European Union, because they compromise compliance with existing EU-level mutual assistance and cooperation legal regimes and lawful searches between EU Member States and with the US, and also compromise the internal security of the EU.

[51] *Id*. at 26.

United Kingdom

Clare Feikert-Ahalt
Senior Foreign Law Specialist

SUMMARY Foreign intelligence gathering in the United Kingdom is regulated by the Intelligence Services Act, the Human Rights Act, and the Regulation of Investigatory Powers Act. These Acts provide for a system of warrants to be obtained to conduct surveillance and intercept communications, provided the surveillance is necessary to complete the statutory functions of the relevant agency. Issuing warrants in the UK remains an executive, rather than judicial, act. UK intelligence agencies are subject to parliamentary oversight.

I. Introduction

The UK has three intelligence and security agencies, which are commonly referred to collectively as the Agencies or the Intelligence Services. These Agencies consist of the Secret Intelligence Service (SIS), also known as MI6 ("MI" standing for Military Intelligence), the UK's overseas intelligence agency; the Government Communications Headquarters (GCHQ), the UK's signals intelligence gathering agency; and the Security Service, also known as MI5, the UK's domestic intelligence agency. The Security Service has statutory responsibility to protect the national security of the UK from international threats, including those from terrorism. It is supported in this role by the SIS and GCHQ, who provide intelligence gathered from overseas.[1]

While these agencies help to collect, gather, and analyze intelligence information, they are not the only parts of the intelligence machinery in the UK. Additional intelligence is compiled by the Cabinet Office, Defence Intelligence (part of the Ministry of Defence), and the Joint Terrorism Analysis Centre.[2] The National Crime Agency addresses organized crime and economic crime and polices the UK's borders.[3] All of these agencies must act within the bounds of the law and their operations "must relate to national security, the prevention or detection of serious crime, or the UK's economic well-being."[4]

II. Legislative Framework

The work of the SIS and GCHQ is undertaken in accordance with the legislative framework of the Human Rights Act,[5] the Regulation of Investigatory Powers Act (RIPA),[6] and the

[1] INTELLIGENCE AND SECURITY COMMITTEE, REPORT INTO THE LONDON TERRORIST ATTACKS ON 7 JULY 2005, 2006, Cm. 6785.

[2] NATIONAL INTELLIGENCE MACHINERY, 2010, at 1, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf.

[3] *About the NCA*, NATIONAL CRIME AGENCY, http://www.nationalcrimeagency.gov.uk/ (last visited Dec. 3, 2014).

[4] NATIONAL INTELLIGENCE MACHINERY, *supra* note 2, at 2.

[5] Human Rights Act 1998, c. 42, http://www.legislation.gov.uk/ukpga/1998/42/contents.

[6] Regulation of Investigatory Powers Act 2000, c. 23, http://www.legislation.gov.uk/ukpga/ 2000/23/contents.

Intelligence Services Act 1994 (the ISA),[7] which placed the SIS and GCHQ on a statutory footing and under the responsibility of the Foreign Secretary.

The ISA defines the function of the SIS as follows:

> (a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and
> (b) to perform other tasks relating to the actions or intentions of such persons.[8]

The GCHQ's role is defined as follows:

> (a) to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material; and
> (b) to provide advice and assistance about—(i) languages, including terminology used for technical matters, and (ii) cryptography and other matters relating to the protection of information and other material, to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or to any other organisation which is determined for the purposes of this section in such manner as may be specified by the Prime Minister.[9]

These functions may only be exercised in the interests of national security with regard to the defense and foreign policies of the UK, in the interests of the economic well-being of the UK, and in support of the prevention or detection of serious crime.[10]

The ISA provides for a system of warrants that authorize entry on and interference with property or with wireless telegraphy upon application from any of the three Intelligence Services.[11] Due to the important role the Intelligence Services play in safeguarding the UK's national security, the ISA's requirements for an authorization are much broader than those for the Acts that cover domestic surveillance.

Each warrant must be approved by the Secretary of State.[12] The Secretary of State must believe that the conduct is proportionate and necessary to assist the Security Service, SIS, or GCHQ in conducting any of their functions under their respective Acts and that the information sought cannot be obtained by other means.[13] Warrants provided to the SIS and GCHQ for the purposes

[7] Intelligence Services Act 1994, c. 13, http://www.legislation.gov.uk/ukpga/1994/13/contents.

[8] *Id*. § 1(1).

[9] *Id*. § 3(1).

[10] *Id*. § 1(2).

[11] *Id*. § 5.

[12] The Secretary of State may also issue warrants to enable the SIS or GCHQ to conduct actions outside the UK. These are known as section 7 warrants, and their purpose is to help protect officers and agents from these agencies from prosecution in the UK. RT. HON. SIR MARK WALLER, INTELLIGENCE SERVICES COMMISSION, REPORT OF THE INTELLIGENCE SERVICES COMMISSIONER FOR 2013, H.C. 302, at 57, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/324152/Intelligence_Services_Commissioner_Accessible__2_.pdf.

[13] Intelligence Services Act 1994, c. 13, § 5, http://www.legislation.gov.uk/ukpga/1994/13/section/5.

of preventing or detecting crime may not relate to the British Islands. The Intelligence Services Act was amended by the Prevention of Terrorism Act 2005, which provides the Intelligence Services authority to obtain a warrant to conduct activities in the UK as well as overseas. The Security Service also can obtain a warrant to interfere with property or wireless telegraphy if it is acting on behalf of the SIS or GCHQ and the action proposed is to be "undertaken otherwise than in support of the prevention of detection of serious crime."[14]

III. Interception of Communications

The use of covert surveillance, use of covert human intelligence sources,[15] and interception of both communications and communications data in England and Wales is allowed, provided the relevant laws regulating this procedure are adhered to.[16]

There is no single legislative regime that applies to the interception of communications; instead the laws and procedures vary according to the body that is seeking the interception. The main piece of legislation in this area is the Regulation of Investigatory Powers Act 2000 (RIPA).[17] RIPA serves to augment the ISA, providing for distinct authorization processes for warrants that apply to the interception of communications[18] and the interception of communications data.[19]

Before the Secretary of State can authorize a warrant to intercept communications, he must believe that the conduct requested by the warrant cannot be obtained by other means, is proportionate and necessary in what it is seeking to achieve, and has as its purpose one of the following: protecting the interests of national security, preventing or detecting serious crime,[20] safeguarding the economic well-being of the UK from the acts or intentions of individuals outside the British Isles, or giving effect to an international mutual assistance agreement whose purpose is equivalent to that of preventing or detecting serious crime.[21] Before signing the

[14] *Id*. § 5(4), (5).

[15] Directed surveillance may be authorized by a designated person within each of the intelligence services provided that it is necessary to fulfill the agency's statutory functions, is undertaken for the purpose of a specific investigation, is proportionate, and cannot be achieved through other means. Regulation of Investigatory Powers Act 2000, c. 23, § 28, http://www.legislation.gov.uk/ukpga/2000/23/section/28.

[16] RIPA provides that unlawfully intercepting communications is an offense punishable by up to two years' imprisonment and/or a fine. *Id*. § 1, http://www.legislation.gov.uk/ukpga/2000/23/section/1.

[17] *Id*.

[18] "Communication" is defined broadly in section 81 of RIPA, *id*., http://www.legislation.gov.uk/ukpga/2000/23/section/81.

[19] Communications data includes subscriber data, use data, and traffic data. SECRETARY OF STATE FOR THE HOME DEPARTMENT, DRAFT COMMUNICATIONS DATA BILL, 2012, Cm. 8359, ¶ 10, http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf.

[20] Detecting crime is interpreted in RIPA as "(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and (b) the apprehension of the person by whom any crime was committed." Regulation of Investigatory Powers Act 2000, c. 23, § 81(5), http://www.legislation.gov.uk/ukpga/2000/23/section/81.

[21] *Id*. § 5.

warrant, the Secretary of State must also consider whether the warrant is operationally required and if its issuance is proportionate and necessary.[22]

RIPA provides for the lawful acquisition and disclosure of communications data in specified circumstances. Communications data does not include the content of a communication but the information that relates to the use of a communications service; thus the requirements to obtain an authorization are less stringent and the list of individuals who can request an authorization is less restrictive. An authorization to obtain communications data can only be obtained if necessary in the interests of national security or the economic well being of the UK; for the purposes of preventing or detecting crime or preventing disorder; in the interests of public safety; for assessing or collecting a tax, duty, levy or other imposition; or for protecting public health or, in an emergency, preventing death, injury, or damage to an individual's physical or mental health, or mitigating such damage.[23]

The range of officials who can authorize the interception of communications data is much broader than in other areas of surveillance, and such authorization can be granted by a senior official in the relevant public authority.[24]

IV. Oversight

The Intelligence Agencies are also subject to parliamentary oversight in the form of the Intelligence and Security Committee, which operates within the "ring of secrecy" to examine the expenditure, administration, and policy of all the Intelligence Agencies.[25] RIPA further requires that the Prime Minister appoint an Intelligence Services Commissioner to review how the Secretary of State issues warrants for both surveillance and interference with property by the Intelligence Services, as well as how the Secretary of State exercises and performs the powers and duties granted by RIPA in relation to the Intelligence Services, although the power to review warrants by this Commissioner is retrospective.[26]

[22] *Id*.

[23] *Id*. § 22(2), http://www.legislation.gov.uk/ukpga/2000/23/section/22.

[24] *Id*. § 22; 2 CURRENT LAW STATUTES 2000 (Christine Beesley et al. eds., 2000).

[25] The role of the ISC has recently been amended and clarified by the Justice and Security Act 2013, c. 18, http://www.legislation.gov.uk/ukpga/2013/18/contents/enacted.

[26] Regulation of Investigatory Powers Act 2000, c. 23, § 59(1)–(2), http://www.legislation.gov.uk/ukpga/2000/23/section/59.

France

Nicolas Boring
Foreign Law Specialist

SUMMARY While a number of intelligence agencies operate in France, large-scale communications interception is carried out primarily by the Directorate General on Exterior Security under the Ministry of Defense, and the metadata collected is shared within the French intelligence network. All of the existing intelligence agencies were created by executive action and are regulated primarily by decrees, executive decisions, circulars, and instructions that are classified.

The interception of communications is governed by the Code of Domestic Security, which recognizes privacy guarantees but also provides for the interception of communications in exceptional circumstances where national security and other safety-related concerns are at issue. The Code provides that the Prime Minister may authorize interception on the proposal of specified ministers. Such authorizations are time limited. The information collected must be destroyed when no longer needed for a recognized purpose. Intelligence agencies may also obtain certain technical information directly from telephone and Internet service providers for the limited purpose of preventing acts of terrorism. Notwithstanding this limited legislative framework, the Directorate General on Exterior Security is reportedly collecting all telephone and electronic communications metadata in France. Oversight of interception surveillance is provided by the National Commission for Security Interceptions, but the Commission's recommendations do not appear to be binding. Parliamentary requests for classified information are routinely rejected and the French Parliament has no right to hear or question members of the intelligence services.

I. Introduction

France has six intelligence agencies. Three fall under the authority of the Ministry of Defense: the Direction générale de la sécurité extérieure (DGSE, Directorate General on Exterior Security), the Direction du renseignement militaire (DRM, Directorate on Military Intelligence), and the Direction de la protection et de la sécurité de la défense (DPSD, Directorate on Defense Protection and Security). Two agencies fall under the authority of the Ministry of Finance: the Cellule de traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN, Service Against the Laundering of Capital and the Financing of Terrorism) and the Direction nationale du renseignement et des enquêtes douanières (DNRED, National Directorate on Customs Intelligence and Investigations). Finally, the Ministry of the Interior has an intelligence service as well, the Direction centrale du renseignement intérieur (DCRI, Central Directorate on Domestic Intelligence).[1]

[1] COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE [COMMISSION ON CONSTITUTIONAL LAWS, LEGISLATION, AND GENERAL ADMINISTRATION OF THE REPUBLIC], ASSEMBLÉE NATIONALE [NATIONAL ASSEMBLY], RAPPORT D'INFORMATION [INFORMATION REPORT], No. 1022, at 10–11 (May 14, 2013).

It appears that large-scale communications interception is mainly done by the DGSE, which has been reported to systematically collect all telephone and electronic communications metadata in France.[2] The DGSE appears to share the collected metadata with the other French intelligence agencies.[3]

II. Legislative Framework

French intelligence agencies operate within an ill-defined legal framework. A 2013 parliamentary report noted that much of France's intelligence agencies still operate in a very blurry "para-legal" or "extra-legal" environment, despite some recent efforts by the legislative branch to provide a better framework.[4]

The six main intelligence agencies mentioned above were all created by decisions of the executive branch rather than by legislation. The DGSE, DPSD, DRM, DCRI, and TRACFIN were all created by decrees, and the DNRED was created by an *arrêté* (executive decision).[5] Only in 2011 did the French Parliament provide some legislative basis for the creation of these agencies, by adopting a law stating that "specialized intelligence services . . . are appointed by executive decision [*arrêté*] of the Prime Minister."[6] Furthermore, the regulation of French intelligence agencies rests on many decrees, executive decisions, circulars, and instructions that are classified.[7]

The regulations mentioned above (decrees, executive decisions, etc.) do not have the same legal authority as duly enacted legislation. There appear to be serious shortcomings when it comes to such legislation that does exist, however. Until 2011, for example, French intelligence operatives were subject to the relevant provisions of the Criminal Code if they were caught under the cover of a false or borrowed identity. The abovementioned 2011 law, which implicitly acquiesced in the creation of the six French intelligence agencies, was the first law to provide some legal cover for the use of false or borrowed identities by intelligence operatives.[8] Furthermore, while there is some legislation on the interception of communications (see Part III,

---

[2] Jacques Follorou & Franck Johannes, *Révélations sur le Big Brother français* [*Revelations on the French Big Brother*], LE MONDE (July 4, 2013), http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html.

[3] *Id.*

[4] RAPPORT D'INFORMATION, *supra* note 1, at 13.

[5] *Id.* at 15–16.

[6] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure [Law No. 2011-267 of March 14, 2011, of Orientation and Programing for the Performance of Interior Security] art. 27 (Mar. 14, 2011), http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id. This provision was incorporated into the French Code de la défense (Defense Code) as article L2371-1, http://www.legifrance.gouv.fr/affichCode.do;jsessionid=6D0EC48E6013B6B33D2E5AD1A7AC622E.tpdjo10v_3?idSectionTA=LEGISCTA000023710864&cidTexte=LEGITEXT000006071307&dateTexte=20141204.

[7] RAPPORT D'INFORMATION, *supra* note 1, at 17.

[8] Loi n° 2011-267 du 14 mars 2011, art. 27; CODE DE LA DEFENSE art. L2371-1.

below), certain aspects of intelligence gathering are not protected by any laws.[9] It appears, for example, that no legislation authorizes intelligence agencies to use certain means such as "bugging" a private location, surreptitiously taking pictures of a person, or tracking the geographic location of a telephone or vehicle. These activities often run against privacy laws, yet are sometimes necessary for national security and/or antiterrorism purposes, forcing intelligence agencies to sometimes operate outside the law.[10] A number of legislators are reportedly working on solving this problem, with plans to introduce legislation that would define more precisely how intelligence agencies may operate.[11]

III. Interception of Communications

The interception of communications is governed by articles L241-1 to L245-3 of the Code de la sécurité intérieure (Code of Domestic Security).[12] This Code states that "the secrecy of correspondence emitted via electronic communications is guaranteed by law,"[13] but also provides that the interception of electronic communications may be authorized under "exceptional" circumstances for the purpose of gathering intelligence regarding national security; the safety of "essential elements of the scientific and economic potential of France"; the prevention of terrorism; the prevention of organized crime; and the prevention of the reorganization of banned groups such as armed militias, terrorist organizations, or hate groups.[14] It appears that the term "electronic communication" includes telephone communications as well as fax and email.[15]

The authorization to intercept electronic communications may only be given by written order of the Prime Minister, or by one of two persons specifically chosen by him, upon the written and reasoned proposal of either the Minister of Defense, Minister of the Interior, Minister in Charge of Customs, or one of two persons specifically chosen by each of them.[16] This authorization is valid for a maximum of four months, but may be renewed by the same procedure under which it was initially granted.[17] Only information relevant to one of the purposes enumerated above may be transcribed from the intercepted communications, and any recording must be destroyed after ten days.[18] Transcriptions must be destroyed as soon as they are no longer needed for the

[9] RAPPORT D'INFORMATION, *supra* note 1, at 31.

[10] *Id.*

[11] *Renseignements: une loi en 2015* [*Intelligence: A Law in 2015*], LE FIGARO (Oct. 2, 2014), http://www.lefigaro.fr/flash-actu/2014/10/02/97001-20141002FILWWW00287-renseignements-une-loi-en-2015.php.

[12] CODE DE LA SÉCURITÉ INTÉRIEURE [CODE OF DOMESTIC SECURITY] arts. L241-1 to L245-3, http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000025503132&dateTexte=20141204.

[13] *Id.* art. L241-1.

[14] *Id.* art. L241-2.

[15] RAPPORT D'INFORMATION, *supra* note 1, at 18–22.

[16] CODE DE LA SÉCURITÉ INTÉRIEURE art. L242-1.

[17] *Id.* art. L242-2.

[18] *Id*. arts. L242-5 & L242-6.

purposes enumerated above.[19] Furthermore, the Prime Minister sets, by decree, the maximum number of communications interceptions that may be simultaneously conducted at any given time.[20] This number was set at 1,840 as of 2009.[21]

For the limited purpose of preventing acts of terrorism,[22] intelligence agencies may also obtain directly from telephone and Internet service providers the type of technical information that may be found on a telecommunications bill: the service subscriber's identity, the location of the subscriber's terminal equipment, the calls made and/or received, or the date and duration of these communications.[23]

While the abovementioned legislation provides a legal framework for specific intercepts, the large-scale interception and storage of communications data does not appear to be governed by any legislation.[24] Despite serious uncertainties about whether this practice is legal or not, the DGSE has been reported to systematically collect all telephone and electronic communications metadata in France.[25]

IV. Oversight

The main body responsible for the oversight of interception surveillance is the Commission nationale pour les interceptions de securité (CNCIS, National Commission for Security Interceptions).[26] When the Prime Minister (or one of his/her delegates) authorizes a communication interception, the CNCIS is to review this authorization.[27] If the CNCIS deems that an authorization was not justified under the law, it sends a recommendation to the Prime Minister calling for the interruption of the interception in question.[28] Such negative recommendations seem to be rare: out of 6,396 interception authorizations granted in 2011, only fifty-five received a negative recommendation by the CNCIS.[29] The CNCIS's recommendations do not appear to be legally binding.

---

[19] *Id*. art. L242-7.

[20] *Id.* art. L242-2.

[21] RAPPORT D'INFORMATION, *supra* note 1, at 21.

[22] *Id.*

[23] CODE DES POSTES ET DES COMMUNICATIONS ELECTRONIQUES [CODE OF POSTAL SERVICES AND ELECTRONIC COMMUNICATIONS] art. L34-1-1, http://www.legifrance.gouv.fr/affichCode.do;jsessionid=47C556F895D429A18C4DDAFD5997AA7D.tpdjo10v_3?cidTexte=LEGITEXT000006070987&dateTexte=20090613.

[24] DIRECTORATE-GENERAL FOR INTERNAL POLICIES, EUROPEAN PARLIAMENT, NATIONAL PROGRAMMES FOR MASS SURVEILLANCE OF PERSONAL DATA IN EU MEMBER STATES AND THEIR COMPATIBILITY WITH EU LAW 66 (Oct. 2013), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf.

[25] *Id.*; Follorou & Johannes, *supra* note 2.

[26] CODE DE LA SÉCURITÉ INTÉRIEURE art. L243-1.

[27] *Id.* art. L243-8.

[28] *Id.*

[29] RAPPORT D'INFORMATION, *supra* note 1, at 21.

Parliamentary oversight appears to be weak, as requests for classified documents from parliamentary committees tend to be rejected, and members of the French Parliament have no right to hear or question members of the intelligence services.[30]

[30] NATIONAL PROGRAMMES FOR MASS SURVEILLANCE, *supra* note 24, at 66.

Netherlands

Wendy Zeldin
Senior Legal Research Analyst

SUMMARY Foreign intelligence gathering in the Netherlands is regulated chiefly by the Intelligence and Security Services Act 2002. The Act governs both the General Intelligence and Security Service and the Military Intelligence and Security Service, and requires that these Services obtain ministerial permission to exercise most of their powers, such as the power to institute surveillance and wiretaps and use intelligence agents.

I. Introduction

The General Intelligence and Security Service of the Netherlands (Algemene de inlichtingen- en veiligheidsdienst, AIVD) under the Ministry of Internal Affairs and Relations with the Realm is responsible for, among other tasks, investigating individuals and organizations, gathering international intelligence, and compiling risk and threat analyses.[1] According to its website, the AIVD seeks to identify risks and threats to Dutch national security by "conducting in-depth investigations to gather intelligence material," which it then "enriches" and shares with various other agencies, in particular the police Regional Intelligence Divisions (RIDs).[2] The AIVD can ask RID personnel to gather intelligence material.[3] In addition to the police regional intelligence units, there is a National Criminal Intelligence Unit that is part of the International Police Intelligence Department (IPOL) under the National Police Services Agency.[4] IPOL is the intelligence service of the Dutch police; it "receives, processes and analyses information, adds knowledge, and makes it available again."[5]

Other intelligence services are the Military Intelligence and Security Service (Militarie Inlichtengen- en Veiligheidsdients, MIVD),[6] the Fiscal Intelligence and Investigation Service-Financial Control Service,[7] the National Signals Intelligence Organization,[8] the Inspectorate

[1] *Tasks and Areas of Interest*, AIVD, https://www.aivd.nl/english/aivd/tasks-and-areas/ (last visited Dec. 4, 2014).

[2] *The AIVD's Role in National Security*, AIVD, https://www.aivd.nl/english/aivd/the-aivd-role/ (last visited Dec. 4, 2014).

[3] *Id*.

[4] POLICE AND SAFETY REGIONS DEP'T, MINISTRY OF THE INTERIOR AND KINGDOM RELATIONS, POLICING IN THE NETHERLANDS 22 (Jan. 2009), http://www.interpol.int/content/download/11814/82014/version/1/file/POLICE%20BROCHURE.pdf.

[5] *Id*. at 31.

[6] *Militarie Inlichtengen- en Veiligheidsdients*, MINISTERIE VAN DEFENSIE, http://www.defensie.nl/organisatie/bestuursstaf/inhoud/eenheden/mivd (last visited Dec. 4, 2014).

[7] *Fiscale Inlichtingen- en Opsporingsdienst - Economische Controledienst (FIOD)*, SOCIALE KAART, https://meeugv.socialekaartnederland.nl/organisaties/fiscale-inlichtingen-en-opsporingsdienst-economische-controledienst-utrecht (last visited Dec. 4, 2014).

SZW,[9] and the National Coordinator for Security and Counterterrorism (for analysis of threats and coordination of counterterrorism activities).[10]

Reportedly the Joint Sigint Cyber Unit (JSCU) was to begin operations in 2014 as a joint effort launched by the AIVD and MIVD. The new unit is to replace the National Signals Intelligence Organization, which had also combined staff from the AIVD and MIVD.[11]

The AIVD shares intelligence analyses with the secret EU Intelligence Analysis Centre (INTCEN), and INTCEN shares its analyses with the AIVD.[12]

II. Legislative Framework

The Intelligence and Security Services Act 2002 governs the activities and powers of the AIVD and also the MIVD.[13] The Act includes provisions on transparency and accountability, measures that "are a direct product of the European Convention on Human Rights."[14]

The AIVD has the authority, among other powers, to observe and follow people, use intelligence agents, and monitor and tap telecommunications. It may use "special powers" (also referred to as "special intelligence resources") only if "strictly necessary" to carry out the duties entrusted to

---

[8] *Q&A's Nationale Sigint Organisatie*, RIJKSOVERHEID (Mar. 17, 2008), http://www.rijksoverheid.nl/nieuws/2008/03/17/q-a-s-nationale-sigint-organisatie.html; *see* Ana van Es, *Jagen op terroristen vanuit de polder*, DE VOLKSKRANT (June 23, 2012), http://www.volkskrant.nl/binnenland/jagen-op-terroristen-vanuit-de-polder~a3275554/.

[9] The Inspectorate SZW, instituted on January 1, 2012, combines "the organisations and activities of the former Labour Inspectorate, the Work and Income Inspectorate and the Social and Intelligence Investigation Service of the Ministry of Social Affairs and Employment." *Special Investigation Departments*, RESEARCH AND DOCUMENTATION CENTER, MINISTRY OF SECURITY AND JUSTICE, https://english.wodc.nl/publicaties/bronnengids/politie_opsporing/bijzondere_opsporingsdiensten/ (last visited Dec. 4, 2014).

[10] Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV); *see* NATIONAL COORDINATOR FOR SECURITY AND COUNTERTERRORISM, ANNUAL PLAN NCTV 2014, at 3–5 (Jan. 27, 2014), http://english.nctv.nl/publications-products/brochures/ (scroll down page for hyperlink).

[11] Didier Bigo et al., *Netherlands' Surveillance: Justice, Freedom and Security in the EU*, OPENDEMOCRACY (May 14, 2014), https://www.opendemocracy.net/can-europe-make-it/didier-bigo-sergio-carrera-nicholas-hernanz-julien-jeandesboz-joanna-parkin-fra-4. According to this news report, "the JSCU is expected to centralize all Signals and Cyber surveillance in the Netherlands and will have a staff of 350. . . . The signals location in Burum and the analysis location in Eibergen, currently operated by the NSO, will stay active." *Id*.

[12] Matthijs R. Koot, *Dutch Govt Response to Parliamentary Questions About EU IntCen*, MATTHIJS R. KOOT'S NOTEBOOK (Jan. 10, 2014), https://blog.cyberwar.nl/2014/01/dutch-govt-response-to-parliamentary-questions-about-eu-intcen/. This blog post is a translation of responses by Dutch Cabinet members to parliamentary questions about INTCEN.

[13] *The Intelligence and Security Services Act 2002*, AIVD, https://www.aivd.nl/english/aivd/the-intelligence-and/#Documents (last visited Dec. 4, 2014; scroll to bottom of page for link to English text of Act of 7 February 2002 [in force on May 29, 2002], Providing for Rules Relating to the Intelligence and Security Services and Amendment of Several Acts (Intelligence and Security Services Act 2002), as amended by the Act of 2 November 2006 (Bulletin of Acts, Orders and Decrees 2006, 574). For the Dutch text of the Act, see http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_14-09-2014.

[14] *The Intelligence and Security Services Act 2002*, *supra* note 13.

it by law.[15] The special powers include surveillance,[16] conducting searches,[17] using intelligence agents,[18] opening mail "and other consignments" without sender or addressee consent,[19] and monitoring and tapping telecommunications.[20] Special powers cannot be used, however, for security screenings or "safeguarding vital sectors," nor may any act "likely to seriously infringe personal privacy . . . be taken without the express prior permission of the Minister of the Interior."[21] The exercise of a special power is generally allowed only if the relevant minister, or the relevant head of a service on the minister's behalf, has given permission for it.[22]

One of the tasks of the AIVD is to conduct investigations regarding other countries on subjects designated by the Prime Minister, in accordance with the relevant ministers.[23] The AIVD is authorized to conduct investigations that involve other countries "regarding matters with military relevance that have been designated by the Prime Minister, Minister of General Affairs in accordance with the relevant Ministers."[24] The AIVD and the MIVD may process the personal data of persons when this is necessary in the context of investigations concerning other countries;[25] tap, receive, record, and monitor conversations, telecommunication or date transfer by means of an automated network with ministerial permission (with certain exceptions);[26]and receive and record non-cable-bound telecommunications originating from or intended for other countries.[27] Both Services are authorized to notify "the appropriate intelligence and security services of other countries, and the appropriate international security, signals intelligence and intelligence bodies" regarding information processed by or on behalf of the Service.[28]

---

[15] *Id*.

[16] *Id*.; Intelligence and Security Services Act 2002, art. 20.

[17] *The Intelligence and Security Services Act 2002*, *supra* note 13; Intelligence and Security Services Act 2002, art. 22.

[18] *The Intelligence and Security Services Act 2002*, *supra* note 13; Intelligence and Security Services Act 2002, art. 21.

[19] *The Intelligence and Security Services Act 2002*, *supra* note 13; Intelligence and Security Services Act 2002, art. 23.

[20] *The Intelligence and Security Services Act 2002*, *supra* note 13; Intelligence and Security Services Act 2002, arts. 24–27. For AIVD's digital intelligence activities, see GENERAL INTELLIGENCE AND SECURITY SERVICE, ANNUAL REPORT 2013, at 18 (Apr. 23, 2014), https://www.aivd.nl/english/general/search/@3096/annual-report-2013/.

[21] *The Intelligence and Security Services Act 2002*, *supra* note 13.

[22] Intelligence and Security Services Act 2002, art. 19 ¶ 1.

[23] *Id*. art. 6 ¶ 2(d).

[24] *Id*. art. 7 ¶ 2(e).

[25] *Id*. arts. 13 ¶¶ 1(c) & 2(c).

[26] *Id*. art. 25 ¶¶ 3 & 8.

[27] *Id*. art. 26 ¶ 1.

[28] *Id*. art. 36 ¶ 1(c).

Both the AIVD and MIVD must submit an annual report before May 1 every year.[29] The Intelligence and Security Services Act 2002 also requires the AIVD to "notify anyone against whom it has used powers which infringe their constitutional right to privacy at home (Article 12) or secrecy of communications (Article 13)."[30] The AIVD must review whether such notification is possible five years after the use of the power in question has terminated, but it will not notify the persons in question if doing so would harm relations with other countries or reveal the sources or methods of the AIVD.[31]

III. Oversight

An independent regulatory commission, comprised of three members appointed by the Crown at the Parliament's recommendation, carries out retrospective monitoring of the AIVD in compliance with the Intelligence and Security Services Act 2002 and also the Security Screening Act.[32] "Subject to a legal obligation to confidentiality," the commission "is entitled to inspect any information it wishes."[33] The commission also publishes an annual report.[34]

[29] *The Intelligence and Security Services Act 2002*, *supra* note 13; Intelligence and Security Services Act 2002, art. 8.

[30] *The Intelligence and Security Services Act 2002*, *supra* note 13.

[31] *Id*.

[32] *Id.*

[33] *Id*.

[34] *Id*.

Portugal

Eduardo Soares
Senior Foreign Law Specialist

SUMMARY Constitutional principles guarantee the protection of personal data in Portugal, including its collection and use, as well as the privacy of a person's home and communications. An information system composed of intelligence services and supervisory bodies is in charge of producing intelligence for the purpose of defending national interests. European Union Directives have been transposed into the country's domestic legal system to regulate the protection of personal data, and privacy in the telecommunications and electronic communications sectors.

I. Constitutional Principles

The protection of personal data used in connection with information technology is a fundamental right guaranteed by the Portuguese Constitution of 1976.[1] The law must establish effective guarantees against the acquisition and abusive use, or use that is contrary to human dignity, of information concerning individuals and families.[2] The home and the privacy of correspondence and other private means of communication are inviolable.[3] Any interference by public authorities with correspondence, telecommunications, or other means of communication is prohibited, except in cases provided by law on matters of criminal procedure.[4]

II. Information System of the Portuguese Republic

In Portugal, intelligence activities are coordinated by the Information System of the Portuguese Republic (Sistema de Informações da República Portuguesa, SIRP). Law No. 30 of September 5, 1984, establishes the general basis of SIRP.[5] The purposes of SIRP are reflected exclusively in the powers and prerogatives of the information services provided for in Law No. 30.[6] These information services are responsible for ensuring, in compliance with the Constitution and the law, the production of information necessary for the preservation of internal and external security, as well as the independence and national interests, unity, and integrity of the state.[7]

---

[1] CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA [C.R.P.] (Constitutional Revision VII (2005)) art. 35, *available at* Assembleia da República [Assembly of the Republic], http://www.parlamento.pt/Legislacao/ Paginas/ ConstituicaoRepublicaPortuguesa.aspx.

[2] *Id.* art. 26(2).

[3] *Id.* art. 34(1).

[4] *Id.* art. 34(4).

[5] Lei No. 30/84, de 5 de Setembro, as amended by Organic Law No. 4 of August 13, 2014, art. 1, http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=764&tabela=leis.

[6] *Id.* art. 2(1).

[7] *Id.* art. 2(2).

Among the bodies created to achieve the purposes of Law No. 30 are the Strategic Information Service of Defense (Serviço de Informações Estratégicas de Defesa, SIED)[8] and the Security Information Service (Serviço de Informações de Segurança, SIS).[9]

SIED is the agency in charge of producing information that may assist in safeguarding the national independence, national interests, and external security of the country.[10] SIS is the agency in charge of producing information to assist in safeguarding internal security and the prevention of sabotage; terrorism; espionage; and the performance of acts that, by their nature, may alter or destroy the state as constitutionally established.[11]

Law No. 30 determines that activities involving research, processing, and dissemination of information that poses a threat or offense to the rights, freedoms, and guarantees embedded in the Constitution and the law cannot be developed.[12] For this purpose, the information services are subject to all the restrictions established by law in defense of rights and freedoms.[13] Each information service can only develop research activities and process information related to their specific mission, without prejudice to the obligation to mutually communicate data and information that may be relevant to the achievement of the purposes of SIRP.[14]

Civil or military employees or agents of the information services provided for in Law No. 30 cannot exercise powers, perform actions, or develop activities under the specific jurisdiction of the courts and bodies with police functions.[15] The information services may have data centers consistent with the nature of the service, which must process and save on a magnetic file the data and information collected in the course of their business.[16] Each data center works autonomously and cannot be connected with other data centers.[17]

III. European Union Directives and Domestic Laws

In 1995, the European Union issued Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[18] During

[8] *Id.* art. 7(e).

[9] *Id.* art. 7(f).

[10] *Id.* art. 20. *See also* Law No. 9 of February 19, 2007, art. 26, http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=910&tabela=leis&ficha=1&pagina=1&.

[11] *Id.* art. 21. *See also* Law No. 9, art. 33.

[12] *Id.* art. 3(1).

[13] *Id.* art. 3(2).

[14] *Id.* art. 3(3).

[15] *Id.* art. 4(1).

[16] *Id.* art. 23(1). *See also* Law No. 9, arts. 41–43.

[17] *Id.* art. 23(2).

[18] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. For a discussion of this and other EU legislation, see EU survey, *supra*.

Portugal's Constitutional Review of 1997, article 35 of the Constitution was amended to enable an adequate transposition of Directive No. 95/46/EC into Portugal's Constitutional Charter.[19] Subsequently, Law No. 67 of October 26, 1998,[20] was enacted as the new law on protection of personal data, which transposed Directive No. 95/46/EC into Portugal's domestic legislation.

Law No. 41 of August 18, 2004,[21] transposed Directive 2002/58/EC[22] on Privacy and Electronic Communications into Portugal's domestic legislation and applies to the processing of personal data in the context of networks and electronic communication services available to the public, specifying and supplementing the provisions of Law No. 67/98.[23]

The processing of personal data referring to philosophical or political beliefs, political party or union membership, religious faith, private life, and racial or ethnic origin, as well as the processing of data concerning a person's health or sex life, including genetic data, is prohibited under article 7(1) of Law No. 67/98.[24] However, article 7(2) of Law 67/98 determines that the processing of the data mentioned in article 7(1) is allowed if permission is provided by law or authorized, in specific situations, by the National Commission of Data Protection (Comissão Nacional de Protecção de Dados, CNPD).[25] Article 5(1) of Law No. 67/98 lists the requirements for the collection and treatment of personal data.[26]

On July 17, 2008, Law No. 32 was issued to regulate the storage and transmission of traffic and location data relative to natural persons and legal entities, as well as the related data necessary to identify the subscriber or registered user, for purposes of investigation, detection, and prosecution of serious crimes by the competent authorities.[27] Law No. 32 transposed Directive

[19] QUARTA REVISÃO CONSTITUCIONAL, Lei No. 1/97, de 20 de Setembro, art. 18, *available at* Procuradoria-Geral Distrital de Lisboa [Lisboa Attorney General's Office], http://www.pgdlisboa.pt/ pgdl/leis/lei_mostra_articulado.php?nid=11&tabela=leis&ficha=1&pagina=1.

[20] Lei No. 67/98, de 26 de Outubro, Lei da Protecção de Dados Pessoais [Personal Data Protection Law], http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=156&tabela=leis&ficha=1&pagina=1.

[21] Lei No. 41/2004, de 18 de Agosto, http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=707&tabela=leis&ficha=1&pagina=1.

[22] 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), 2002 O.J. (L 201) 37, http://eur-lex.europa.eu/LexUriServ/LexUri Serv.do?uri=CELEX:32002L0058:en:HTML.

[23] Lei No. 41/2004, art. 1(2).

[24] Lei No. 67/98, art. 7(1).

[25] *Id.* art. 7(2). Article 22(1) of Law No. 67/98 determines that the CNPD is the national authority charged with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for the human rights and the fundamental freedoms and guarantees provided by the Constitution and the law.

[26] *Id.* art. 5(1).

[27] Lei No. 32/2008, de 17 de Julho, art. 1(1), http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=1264&tabela=leis&ficha=1&pagina=1&.

2006/24/EC[28] into Portugal's domestic legal system. According to Law No. 32, the retention of data revealing the content of communications is prohibited, without prejudice to the provisions of Law No. 41/2004 and criminal procedure law on the interception and recording of communications.[29]

The storage and transmission of data must be made exclusively in connection with the investigation, detection, and prosecution of serious crimes by the competent authorities.[30] The transmission of data to the competent authorities can only be authorized by a written order issued by a judge, in accordance with article 9 of Law No. 32/2008.[31] The files for the retention of data under Law No. 32/2008 must be separated from any other files used for other purposes.[32] The data subject cannot oppose the storage and transmission of data.[33]

[28] 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, 2006 O.J. (L 105) 54, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024.

[29] Lei No. 32/2008, art. 1(2).

[30] *Id.* art. 3(1).

[31] *Id.* art. 3(2).

[32] *Id.* art. 3(3).

[33] *Id.* art. 3(4).

Romania

Nerses Isajanyan
Foreign Law Consultant

SUMMARY Intelligence gathering in Romania is divided among several government agencies as provided in national security legislation. Constitutional principles guarantee the protection of privacy and personal data. Surveillance and intelligence gathering is conducted in accordance with national criminal procedural legislation, and all agencies involved in intelligence collection are subject to the same procedures. Control over intelligence activities by government agencies is conducted by the Parliament and through the judicial review of warrants for data collection issued by the prosecutorial offices; the latter form of control, however, appears to be inefficient because of weakness in the judiciary.

I. Introduction

The Romanian intelligence community consists of six cabinet-level services and ministerial substructures charged with intelligence collection:

- Domestic Intelligence Service (Serviciul Român de Informaţii, SRI)
- Foreign Intelligence Service (Serviciul de Informaţii Externe, SIE)
- Guard and Protection Service (Serviciul de Protecţie şi Pază, SPP, in charge of protecting Romanian and foreign VIPs)
- Defense Ministry's Directorate of Defense Intelligence
- Interior Ministry's General Directorate of Intelligence and Internal Protection (police)
- Justice Ministry's General Directorate for Protection and Anti-Corruption[1]

Each agency works in a specific field within the scope of its jurisdiction as assigned by the Law on National Security of Romania.[2] The SIE was created under a specific law that defined its duties and created a multilayered oversight structure aimed at immunizing the Service from political manipulations along party lines.[3] The Service operates independently of the government and is not subordinate to the incumbent executive.[4] The Law states that the means

[1] HANS BORN & MARINA CAPARINI, DEMOCRATIC CONTROL OF INTELLIGENCE SERVICES: CONTAINING ROGUE ELEPHANTS 48 (Ashgate Pub. Ltd. 2013).

[2] Law No. 51/1991 on National Security of Romania, MONITORUL OFFICIAL [MO] [OFFICIAL GAZETTE], Aug. 7, 1991, *available in English at* https://www.sri.ro/fisiere/legislation/Law_national-security.pdf.

[3] Law No. 1/1998 on the Organization and Functioning of the Foreign Intelligence Service, MO, Jan. 6, 1998, http://www.sie.ro/En/Legi/1.pdf.

[4] COUNCIL OF EUROPE, CIA ABOVE THE LAW? SECRET DETENTIONS AND UNLAWFUL INTER-STATE TRANSFERS OF DETAINEES IN EUROPE 201 (2008).

of intelligence gathering must not violate citizens' basic rights and freedoms, private life, or honor and reputation, nor can it impose on them any illegal restraints.[5]

To ensure the unified coordination of all activities pertaining to defense and state security, including intelligence operations, the National Defense Supreme Council, an autonomous administrative body managed by the Office of the President of Romania, was created by law in 1990.[6] Additionally, the Council coordinates and monitors activities of the SRI, SEI, and SPP.[7]

II. Legislative Oversight

The SIE and the SRI are subject to parliamentary control through special parliamentary committees individually dedicated to each agency.[8] These committees consist of nine members each, seven representing the lower chamber of the Parliament and two representing the Senate.[9] Each party represented in Parliament has members on these committees.[10] Both committees overseeing the SRI and SIE are empowered to verify constitutional and legal compliance of the Services' activities and investigate allegations of illegal intelligence collection.[11]

The committees are allowed to request information possessed by the SRI and SIE. Both Services are required to respond to such requests within a reasonable period of time, unless doing so jeopardizes ongoing operations, the identities of agents, or intelligence sources and methods.[12] The committees are authorized to investigate the directors of the agencies and their staff members and have the right to conduct unannounced visits to the Services, which must grant the committees full access to personnel, data, and facilities.[13] Reportedly the committees have uncovered corruption and links to organized crime within the agencies, and violations of civil rights and liberties committed by intelligence services personnel.[14] On the basis of media accusations, parliamentary committees initiated a series of SRI and SIE investigations and inquiries, which resulted in the removal of personnel.[15]

---

[5] Law No. 1/1998 on the Organization and Functioning of the Foreign Intelligence Service art. 10(3).

[6] Law No. 39/1990 on the Setting Up, Organization and Functioning of the Supreme Council of National Defense, MO, Dec. 13, 1990.

[7] THOMAS BRUNEAU & STEVEN BORAZ, REFORMING INTELLIGENCE: OBSTACLES TO DEMOCRATIC CONTROL AND EFFECTIVENESS 255 (Univ. Texas Press 2009).

[8] COUNCIL OF EUROPE, *supra* note 4, at 201.

[9] Rule No. 44/1998 on the Setting Up, Organization and Functioning of the Special Parliamentary Commission for Overseeing the Foreign Intelligence Service, http://sie.ro/En/Legi/44.pdf.

[10] BRUNEAU & BORAZ, *supra* note 7, at 227.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.* at 233.

III. Judicial Control over Surveillance Procedures

Judicial oversight is generally limited to the consideration and issuance of warrants for surveillance that restrict an individual's civil rights and liberties.[16] The National Security Law authorized the SRI and SIE to undertake intelligence surveillance and established preemptive control by judicial authorities.[17] Article 13 of the Law states that requests for warrants must be approved by the Prosecutor General's office and must contain details regarding the following:

- Motivating threat to national security
- Specific activities for which the warrant is being issued (e.g., surveillance, wiretapping, search, seizure)
- Names of persons whose communications are to be intercepted, or of those who hold the information, documents, or objects that must be obtained
- Location where the warranted activities will be carried out, if and when it is possible to provide this information
- Duration for which the requested warrant is valid (up to six months initially)
- Office charged with the execution of the warrant[18]

Warrants are valid for six months, although they can be extended an indefinite number of times for three-month periods when cause is shown.[19] In 2005 warrant approval was reassigned from prosecutors to judges, although prosecutors were permitted to approve short-term (twenty-four- to forty-eight-hour) warrants during weekends when judges are off duty.[20]

The weakness and vulnerability to political influence of the legal and justice system is still a significant obstacle to effective democratic oversight.[21] Statistics revealed that 14,267 wiretapping warrants were requested between 1989 and 2002 by the intelligence agencies, and the Prosecutor General did not deny a single one.[22] Of the warrants issued, only about 2% led to an indictment, while the Services claimed the remaining 98% were "used for prevention of a crime."[23]

[16] BORN & CAPARINI, *supra* note 1, at 59.

[17] Law No. 51/1991, arts. 8, 13.

[18] *Id*. art. 13.

[19] *Id*.

[20] BORN & CAPARINI, *supra* note 1, at 59.

[21] *Id.* at 64.

[22] BRUNEAU & BORAZ, *supra* note 7, at 228.

[23] *Id*.

The National Security Law states that "any citizen who considers himself injured in an unjustified manner through the activities that constitute the object of the warrant . . . may lodge a complaint with the public prosecutor specially appointed, hierarchically superior to the public prosecutor who has issued the warrant."[24] The Law provides that citizens who believe that their rights or liberties have been violated by the government in the course of its information gathering have the right to "inform any of the standing comittees [sic] for the defence and ensuring of the public order, of the two chambers of the Parliament."[25]

[24] Law No. 51/1991, art. 13.

[25] *Id.* art. 16.

Sweden

Elin Hofverberg
Foreign Law Consultant

SUMMARY Signal surveillance is regulated by Swedish law. Only the National Defense Radio Establishment may carry out surveillance and only on cross-border communication. Information may be requested by the government, the military, and the police. Sweden's surveillance legislation has received widespread criticism, including from the European Parliament, on the grounds that it fails adequately to protect privacy and may violate the European Convention on Human Rights. Specific privacy protection regulations that pertain to surveillance information are in place.

I. Signal Surveillance Legislation

Intelligence collection of data through signal surveillance is carried out by Försvarets Radioanstalt (FRA) (the National Defense Radio Establishment)[1] and is governed by the Act on Signal Surveillance for Defense Intelligence Activities, commonly referred to as the FRA legislation.[2] Surveillance is also limited by the more general Act on Defense Intelligence Activity.[3]

A. Requirements

Intelligence data collection through signal intelligence can only be requested by the government, government offices, the Swedish Armed Forces, the Swedish Security Service (Police), and the National Operative Department of the Police.[4] Such collection requires prior authorization from the Defense Intelligence Court[5] and can only be carried to determine

> 1. outer military threats against the country,
> 2. conditions for Swedish involvement in peace promotion and humanitarian international missions or threats against security for Swedish interests during such missions,
> 3. strategic relationships regarding international terrorism and other significant transborder crime that can threaten important national interests,
> 4. development and spread of mass destruction weapons, military material and products covered in the Law (SFS 2000:1064) on control of products with dual uses and technical assistance,

[1] *In English*, FRA, http://www.fra.se/snabblankar/english.10.html (last visited Dec. 2, 2014).

[2] LAG OM SIGNALSPANING I FÖRSVARSUNDERRÄTTELSEVERKSAMHET [ACT ON SIGNAL SURVEILLANCE FOR DEFENSE INTELLIGENCE ACTIVITIES] (Svensk författningssamling [SFS] 2008:717), http://www.notisum.se/rnp/sls/lag/20080717.htm.

[3] LAG OM FÖRSVARSUNDERRÄTTELSEVERKSAMHET [ACT ON DEFENSE INTELLIGENCE ACTIVITIES] (SFS 2000:130), https://lagen.nu/2000:130.

[4] 4 § ACT ON SIGNAL SURVEILLANCE.

[5] *Id*. 4 § para. 3.

> 5. serious outer threats against society's infrastructure,
> 6. conflicts abroad with consequences to international security,
> 7. foreign intelligence activity against Swedish interests, or
> 8. foreign governments powers conduct or intentions of considerable importance to Swedish foreign, security or defense policy.
>
> If necessary for security defense intelligence operations signals in electronic form may also be collected to
> 1. follow changes in the signal environment abroad, technical development and the signal protection as well as
> 2. continuously develop the technology and methods needed to carry out its activity in accordance with this law (2009:967).[6]

The court may only grant an application for surveillance if it conforms to the purposes of the surveillance legislation and the Act on Defense Intelligence Activity, the need cannot be met in a less invasive manner, and the value of the surveillance clearly outweighs the violations against integrity (human rights).[7] In addition, the application cannot be limited to one specific, physical individual.[8] The Swedish Defense may cooperate with foreign governments in the collection of the abovementioned information.[9]

B. Limitations

There are limitations on signal surveillance both in terms of scope, duration, and subject. The main limitation is that signal surveillance must only cover cross-border communications.[10] Thus, communications that take place solely within the borders of Sweden cannot be legally collected through signal surveillance. However, these limits do not apply to "senders and receivers on foreign state ships, foreign state aircraft or military vehicles."[11] Domestic surveillance is instead covered by the Swedish law implementing the European Union Data Retention Directive.[12] Moreover, surveillance cannot be targeted against one specific individual alone[13] and may only be approved for a period of six months at a time.[14]

Once collected, stored information must be destroyed by the FRA under certain circumstances, e.g., if information on an individual lacks importance to the investigation[15] or the "information

[6] *Id*. 1 § paras. 2 & 3 (translation by author).

[7] *Id*. 5 §.

[8] *Id*.

[9] *Id*. 9 §; 3 § LAG OM FÖRSVARSUNDERRÄTTELSEVERKSAMHET (SFS 2000:130).

[10] 2a § ACT ON SIGNAL SURVEILLANCE.

[11] *Id*. 2a § para. 2.

[12] The domestic Act, LAGEN OM ELEKTRONISK KOMMUNIKATION (SFS 2003:389), is still in force following the EU Court's invalidation of the Data Retention Directive as a violation of human rights earlier this year. For a discussion of the EU Directive, see EU survey, *supra*.

[13] 4 § para 3 ACT ON SIGNAL SURVEILLANCE.

[14] *Id*. 5a § item 5.

[15] *Id*. 7 §.

was communicated during religious confession or private care of the soul, unless there are exceptional reasons to collect the information."[16]

II. Privacy

Specific privacy legislation deals with the treatment of personal data collected by the FRA.[17] Individuals have the right to inquire whether they are included in the material collected by the FRA.[18] Such information can be requested once a year and should be provided within four months.[19] Information may be withheld if secrecy requires it.[20]

Stored data can only be shared with foreign or multinational entities if the information is not protected by secrecy *and* if sharing it is required for the FRA to fulfill its international commitments.[21] However, the government has the right to issue regulations that allow secret information to be transferred if considered necessary for the operations of the FRA.[22] The FRA must employ security measures to safeguard personal information.[23]

Only decisions on information correction requests and the communication of information to third parties may be appealed.[24] Under certain circumstances, such as when information collection constitutes a violation of personal integrity, the state can be held liable for damages to an individual whose information was illegally obtained.[25]

Sweden has been criticized by the European Parliament for its legislation on signal surveillance, especially as it pertains to privacy protections and its oversight, on the ground that it may violate the European Convention on Human Rights.[26]

---

[16] *Id*. (translation by author).

[17] LAG OM BEHANDLING AV PERSONUPPGIFTER I FÖRSVARSMAKTENS FÖRSVARSUNDERRÄTTELSEVERKSAMHET OCH MILITÄRA SÄKERHETSTJÄNST (SFS 2007:258); LAG OM BEHANDLING AV PERSONUPPGIFTER I FÖRSVARETS RADIOANSTALTS FÖRSVARSUNDERRÄTTELSE- OCH UTVECKLINGSVERKSAMHET(SFS 2007:259).

[18] Ch. 2:1 § LAG OM BEHANDLING AV PERSONUPPGIFTER I FÖRSVARETS RADIOANSTALTS FÖRSVARSUNDERRÄTTELSE- OCH UTVECKLINGSVERKSAMHET.

[19] *Id*.

[20] *Id*. ch. 2: 3 §.

[21] *Id*. ch. 1:17 §.

[22] *Id*.

[23] *Id*. ch. 3:2 §.

[24] *Id*. ch. 3:3 §.

[25] Ch. 2:5 § LAG OM BEHANDLING AV PERSONUPPGIFTER I FÖRSVARETS RADIOANSTALTS FÖRSVARSUNDERRÄTTELSE- OCH UTVECKLINGSVERKSAMHET.

[26] *EU Scrutinizes Sweden's Surveillance Capacities*, SVERIGES RADIO (Nov. 8, 2013), http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=5698572; EUROPEAN PARLIAMENT, DRAFT REPORT, 2013/2188(INI) (Jan. 8, 2014), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/moraes_1014703_/moraes_1014703_en.pdf.

III. Oversight Authorities

Sweden has two different oversight authorities for signal intelligence gathering. The oversight authority that oversees FRA's compliance with the Signal Surveillance Act is Statens inspektion för försvarsunderrättelseverksamheten (Siun),[27] whereas the Swedish Data Inspection Board is responsible for the oversight of privacy issues, specifically how information is stored and shared between agencies.[28] In this capacity the Data Inspection Board has the right to access personal information that has been stored, obtain information about the storage and protection of the collection, and access facilities containing the information.[29] It is also responsible for trying to ensure the correction of possible violations.[30] The oversight authority may initiate court proceedings before the district administrative court to have illegal information erased.[31] However, information may not be erased if doing so is deemed unreasonable.[32]

[27] 2 § Förordning med instruktion för Statens inspektion för försvarsunderrättelseverksamheten (2009:969) [Regulation with Instruction for the State Inspection of Defense Intelligence Activity], http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Forordning-2009969-med-inst_sfs-2009-969/.

[28] Förordning med instruktion för Datainspektionen [Regulation with Instruction for the Datainspektionen] (SFS 2007:975), http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Forordning-2007975-med-inst_sfs-2007-975/.

[29] Ch. 5:2 § LAG OM BEHANDLING AV PERSONUPPGIFTER I FÖRSVARETS RADIOANSTALTS FÖRSVARSUNDERRÄTTELSE- OCH UTVECKLINGSVERKSAMHET.

[30] *Id*. ch. 5:3 §.

[31] *Id*. ch. 5:4 §.

[32] *Id*. ch. 5: 4 § para. 2.