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

PORTUGAL

Version of 30 September 2014

Centro de Estudos para a Intervenção Social (CESIS)
Josefina Leitão
(with the collaboration of José Filipe Sousa)

Summary

[1]. The Information System in Portugal is structured by the legal framework of the Intelligence System of the Portuguese Republic[1] (SIRP), which is complemented by the Act on the Organisation of the Intelligence Services[2]. Also of relevance is the Internal Security Act[3], that sets the powers of the several authorities regarding criminal investigation, and therefore the possibility of taking on surveillance measures.

[2]. The Portuguese Constitution[4] is also a crucial part of the legal framework since it is the main repository for the protection of the individual's rights and freedom.

[3]. As regards the specific problem of mass surveillance, the present legal framework remains insufficient. The SIRP Framework Law was recently reformed[5].This reform enhanced the democratic control of the Parliament (regarding the election of the Secretary General of the SIRP and the appointment of the Directors of the Intelligence Services) and the guarantees of transparency, impartiality and independence of the bodies overseeing the Intelligence Services, as well as of the agents working for them.

[4]. The framework is thus defined under the umbrella of the SIRP – System of Information of the Portuguese Republic, which brings together:

- The Service of Strategic Intelligence and Defense (*Serviço de Informações Estratégicas e de Defesa,* SIED) which is the service responsible for the production of information that contributes to the safeguard of national independence, the national interests and the external security of the Portuguese State.
- The Service of Security Intelligence *(Serviço de Informações de Segurança,* SIS*)* which is responsible for the production of information that contributes to the safeguard of the internal security, the prevention of sabotage, terrorism, espionage and other practices that could aim to change or destroy the constitutional establishment and the Rule of Law.

---

[1] Portugal, Framework Law on the Intelligence System of the Portuguese Republic (*Lei Quadro do Sistema de Informações da República Portuguesa),* Law 30/84, 5 September 1984, available at http://dre.pt/pdf1sdip/1984/09/20600/27342738.pdf. This Legal framework was subject to changes and republished by the Organic Law 4/2004, of 6 November, available at http://dre.pt/pdf1sdip/2004/11/261A00/65986606 . All Hyperlinks accessed on 5 August 2014.

[2] Portugal, Act on the organisation of the Intelligence Services (*Lei que estabelece a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS))* Law 9/2007, 19 February of 2007, available at http://dre.pt/pdf1sdip/2007/02/03500/12381252.pdf . Hyperlink accessed on 5 August 2014.

[3] Portugal, Internal Security Act (*Lei da Segurança Interna)* Law 53/2008, 29 August 2008, available at http://dre.pt/pdf1sdip/2008/08/16700/0613506141.pdf . Hyperlink accessed on 6 August 2014.

[4] Portugal, Constitutional Law No.1/2005, VII Constitutional revision (*Lei Constitucional n.º 1/2005, VII Revisão constitucional*), 12 August 2005, available at: https://dre.pt/pdf1sdip/2005/08/155A00/46424686.pdf. H English version available at http://www.en.parlamento.pt/Legislation/CRP/Constitution7th.pdf. Hyperlinks were accessed on 5 of August 2014.

[5] Portugal, Organic Law 4/2014, Fifth Amendment to the Framework Law on the Intelligence System of the Portuguese Republic *(Quinta Alteração à Lei Quadro do Sistema de Informações da República Portuguesa)* , 13 August 2014, available at https://dre.pt/pdf1sdip/2014/08/15500/0419404206.pdf . Hyperlink accessed on 5 September 2014.

[5]. These two services have common departments dealing mostly with the management and administrative support, under what is defined by article 17 and following of the Act on the organisation of the Intelligence Services: Human Resources, Finance and General Support, IT and Security.

[6]. Both these services are overseen by a Secretary General, depending directly from the Prime-Minister who has the same statute of a Secretary of State, under the article 2 of the Act on the Organisation of the Intelligence Services.

[7]. The Portuguese system must be understood within the context of the building up of the democracy after the Revolution of the 25th April 1974. After the abuses committed under the dictatorship regarding surveillance, trials, imprisonment and torture by the State Police, the creation and consolidation of the Intelligence Services took more than 10 years. This was mainly due to the distrust on the existence of "Secret Police". This context explains the existence of a very strict legal framework regarding surveillance which applies to the Portuguese Intelligence Services.

[8]. The intelligence services have legal limitations regarding their activities, and cannot perform criminal investigations or intervene in the penal procedure, as stated by articles 3 and 4 of the SIRP legal framework, and article 6, no 2 and 3 of the Act on the Organisation of the Intelligence Services. This fact also finds legal evidence in article 34, no 4 of the Constitution, which does not allow any intrusion on the mail, telephone or other communications other than as a result of a criminal investigation. This means that, since the intelligence services cannot perform criminal investigation, as stated by the legal framework, they consequently cannot perform surveillance actions, such as surveillance of communications, e-mail, or telephone.

[9]. Both the SIED and the SIS have the power **-** under their specific attributions - to systematically promote research and analysis and the processing of intelligence, as well as the archive and dissemination of the information gathered. Working under the direct orders of the Prime-Minister, and under the direction of the Secretary General of the SIRP, they prepare documents, studies and communicate information, namely to other law enforcement services about crimes committed for further criminal investigation. The Secretary General of the SIRP is nominated by the Prime-Minister and has the same statute of a Secretary of State, under articles 17 and 19 of the SIRP framework law, and article 2 of the Act on the Organisation of the Intelligence Services. The specific competences of the Prime Minister are, under article 4 of the Act on the Organisation of the Intelligence Services: to approve the annual work plan and to give orders or guidelines through official dispatches, and to approve, together with the Finance Minister, the budget for the intelligence services activities. These activities are classified and not publicly available, under article 5 of the Act on the Organisation of the Intelligence Services.

[10]. Each of the services has a data centre for the processing of information, which is responsible for the processing and storing of the data collected. No third party or other organisation outside the SIRP can have direct access to the information stored by its services, under article 43 of Act on the Organisation of the Intelligence Services. Furthermore, the circumstances in which the services stated by the SIRP Framework Law can access the information are defined by the Prime-Minister, and the means of access by the staff of the information services are defined by the Secretary General of the SIRP.

[11]. Article 9 of the Act on the Organisation of the Intelligence Services sets the right of access of the intelligence services, through its directors, deputy directors and heads of department, to information and records relevant to the pursuit of its powers, contained in files held by the public institutions. Under article 10 of the same law, the public institutions have the duty of cooperation with the intelligence services.

[12]. Regarding the private sector, the same duty of cooperation is possible to private entities when they develop relevant activities in the context of a contract between them and the State, regarding the subjects that are under the competences of the Secretary General of the SIRP, the SIED and the SIS. The article 10 n. 2 of the Act on the organisation of the Intelligence Services does not specify the type of contracts nor the details of its operation.

[13]. The access to data held by telecom providers is done under the Act on privacy and electronic communications[6] and the Act[7] that Regulates the Conservation and Transmission of Communications and Location Data (Data Retention Act). In both cases the access of the authorities to the data must be preceded by judicial authorisation. In the case of the Data Retention Act, the intelligence Services do not access the data directly, as the law only refers to the Police forces and Immigration Services (SEF), as the criminal investigation is, as said before, outside the intelligence services jurisdiction. If the data collected by the police forces are relevant within their jurisdiction, and within the duty of cooperation of the article 10 of the Act on the Organisation of the Intelligence Services, the relevant information may be shared but the internal procedures are not disclosed in the law.

[14]. The SIRP framework sets a comprehensive mechanism of control and oversight of the activities of the intelligence services:

- Council for the Oversight of the SIRP *(Conselho de Fiscalização do SIRP)* - The Supervisory Board of SIRP, as the inspection body of this system, is responsible to monitor and supervise the activities of the Secretary-General and the intelligence services, ensuring compliance with the Constitution and the law, in particular the system of fundamental rights, freedoms and guarantees of the citizens. It is composed of three citizens of recognized integrity and in full capability of their civil and political rights, whose profile gives the guarantee that they will respect, during the mandate and after its term, the duties of independence, impartiality and discretion. Its members are elected by the Parliament by secret ballot, by a two-thirds majority of members present in the plenary, as long as it represents more than the absolute majority of MPs in active duty. Before the election, the candidates are subject to a public hearing in the Parliaments Commission for Constitutional matters, where they have to present a statement of interest, under article 8-A of the framework, in order to check the guarantees of impartiality

[6] Portugal, Act on privacy and electronic communications[6], *(Lei que regula a protecção de dados pessoais no sector das comunicações)* Law 41/2004, 18 August of 2004, that transposes the Directive 2002/58/CE (Directive on privacy and electronic communications), available at http://dre.pt/pdf1sdip/2004/08/194A00/52415245.pdf . Hyperlink accessed on 8 of August 2014.

[7]Portugal, Act that regulates the conservation and transmission of communications and location data *(Lei que regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas)* Law 32/2008, 17 July of 2008, that transposes EU Directive 2006/24/CE, of the Parliament and the Council, of 15 of March (Data Detention Directive), available at http://dre.pt/pdf1sdip/2008/07/13700/0445404458.pdf . Hyperlink accessed on 7 of August 2014.

regarding the professional, political, or non-governmental activities of the candidate.

- Superior Intelligence Council *(Conselho Superior de Informações)* – It is the interministerial consultative and coordination body for the information, chaired by the Prime Minister, and composed by the Ministers of State and the Presidency of the Council of Ministers, Defence, Internal Affairs, Justice, Foreign Affairs and Finance, the Presidents of the Regional Governments of the Azores and Madeira, the General Chief of the Armed Forces, the Secretary General of SIRP and two members of Parliament, elected by a majority of two thirds of the members present, provided that it exceeds the absolute majority of MPs in office. The Prime Minister can still determine the presence of other relevant entities depending on the subject to discuss. Its competences are defined in article 18, number 4 of the SIRP framework law: to assist and advise the Prime-Minister in the coordination of the intelligence services; to give an opinion about every matter that the Prime-Minister brings to the council regarding the intelligence subjects; to propose the orientation of the activities of the Intelligence Services.
- SIRP´s Data Oversight Commission *(Comissão de Fiscalização de Dados do SIRP)* - The Commission works within the Attorney General Office (*Procuradoria Geral da República,* PGR*)* and is composed by three prosecutors. It is the exclusive body that oversees the activity of the data centres, through periodical verifications, and the enforcement of the law, in respect for the compliance of the Fundamental Rights, Liberties and Guarantees of the citizens.
- The legal framework sets the geographical scope of the surveillance only for the SIS, which is the equivalent to the territory of Portugal as a sovereign state[8].

[15]. The conditions for access to information and to conduct surveillance are connected to the purpose of serious crimes, like terrorism, violent crimes, highly organised crime, kidnapping, hostages' situation, crimes against cultural identity and personal integrity, against national security, counterfeiting and crimes under international law that endanger the maritime or air navigation.

[16]. The Penal Procedural Code[9], in its article 187, regulates the access and interception of communications and sets the specific cases where that interception can take place. National security is one of the situations included in this catalogue. The law on Cybercrime[10], is applicable under its article 11, extending the scope of the law beyond the investigation of cybercrime, whenever it is necessary to intercept communications.

[17]. The general regime of privacy and data protection is defined by article 35 of the Constitution by the Data Protection Act[11]. Under the Data Protection Act, the Portuguese Data Protection Commission (*Comissão Nacional de Proteção de Dados*,

---

[8] Article 34 of the Law 9/2007 described above.

[9] Portugal, Penal Procedure Code (*Código de Processo Penal*) last version available at http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis. Hyperlink accessed on 7 of August 2014.

[10] Portugal, Law on Cybercrime (*Lei do Cibercrime)* Law 109/2009 of 15 September, that transposes Framework Decision 2005/222/JAI of the Council, 24 of February of 2005, available at http://dre.pt/pdf1sdip/2009/09/17900/0631906325.pdf. Hyperlink accessed on 7 August of 2014.

[11] Portugal, Data Protection Act (*Lei de Protecção de Dados)*- Law 67/98, of 26 October 1998 , that transposes EU Directive 95/46/CE, of 24 October 1995, available at http://dre.pt/pdf1sdip/1998/10/247A00/55365546.pdf . Hyperlink accessed 6 of August 2014.

CNPD) has the responsibility of guaranteeing compliance with the Law and the Constitution, both by the public and the private sector. But the power of inspection of the intelligence services is outside the jurisdiction of the CNPD, as a consequence of the final part of article 4, no 7 of the Data Protection Act.

[18]. According to the provision of article 26 no 1 of the SIRP Framework Law, the SIRP Data Oversight Commission is the exclusive competent body with direct control over the functioning of the SIS and SIED's data centres, as stated above. Complaints regarding the violation of the law and the Constitution, or the right to challenge surveillance can be addressed to the Council for the Oversight of the SIRP.

[19]. The general principles and rights that are set both by the Constitution and the Data Protection Act are relevant to the processing of any kind of data, namely the right of information, right of access, right to object, and the rights to rectification/deletion/blockage. Furthermore, article 8 of the Data Protection Act sets the conditions for the data processing in case of suspicion of illegal activities, criminal and administrative offences, demanding that there is a legal provision that legitimates such data processing.

[20]. The violation by the State of an individual's fundamental rights gives citizens the possibility to address both the CNPD (within the limit of its powers), the Council for the Oversight of the SIRP (article 27 of the SIRP Framework Law) or to address the subject within the discussion of the case in an Administrative or Judicial Court.

[21]. The Ombudsman, in accordance with the Constitution in its article 23, and under the definition of the Ombudsman Statute[12], *is a State body elected by the Parliament whose main duties shall be to defend and to promote the rights, freedoms, guarantees and legitimate interests of the citizens, ensuring, through informal means, that public authorities act fairly and in compliance with the law.* Therefore, the Ombudsman can, under the article 20 of the Statute, issue recommendations, opinions, promote public interventions and point out shortcomings of the legislation of any aspect that is linked with the scope of the Ombudsman activity, under the article 2 of the Statute. Thus,the intelligence services are public services that can be under that scope of activity and the Ombusdman can act if there is evidence of the violation of the peoples rights, freedoms and guarantees.

[12] Portugal, Statute of de Ombudsman (Estatuto do Provedor de Justiça) **Law no. 9/91, of April 9**, amended by Law no. 30/96, of August 14, Law no. 52-A/2005, of October 10, and Law no. 17/2013, of February 18, available at http://www.provedor-jus.pt/?idc=20&idi=15393,. Hyperlink accessed 24 of September, 2014.

Annex 1 – Legal Framework relating to mass surveillance

A. Details on legal basis providing for mass surveillance

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
Act of the Parliament Law 32/2008Data Retention Directive Penal Procedure Code	Suspects of committing serious crimes	Serious crimes, like terrorism, violent crimes, highly organised crime, kidnapping, hostages' situation, crimes against the cultural identity and personal integrity, against national security, counterfeiting and crimes under international law that endanger the	National security. The Institute for the National Defence defines National security as "the Nation´s condition which can be translated by the guarantee of permanent peace and freedom, its sovereignty, independence and unity, the integrity of its territory, and the safeguard of	A judicial warrant is always needed to proceed with the surveillance. It can only be issued during the investigation, and has the duration of three months, renewable (article 187 of the Penal Procedure Code).	Suspect of illegal activities. Decision of investigation. Judicial authorisation/warrant	Portuguese Territory	There is no specific legal reference that allows mass surveillance in a different country. The law applies to the territory of Portugal.

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
		maritime or air navigation.	people, property and spiritual values, and the development of the tasks of the State, the freedom of political action by the State bodies, and the regularity of the democratic institutions." National independence. Prevention of sabotage. Fight against Terrorism and espionage.		Collecting data; Analysing data; Report to the Council of Supervision Storing data; Destruction of non-relevant data. Information to competent criminal authorities.		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
Act on the Organisation of the Intelligence Services;	The intelligence services cannot perform mass surveillance, neither can they perform surveillance of any kind of communications	Only if, in the course of the jurisdiction of the intelligence services, they find out that a subject is suspect of committing crimes. In this case, the information is provided to the Police Forces who are responsible for the criminal investigation	No surveillance can be taken upon this legislation.	N/A	N/A	Portuguese Territory	The law applies to the territory of Portugal.
Internal Security Act;	Does not state such categories as they are defined in other pieces of legislation mentioned above.	N/A	N/A	N/A	*Polícia Judiciária* is the Police responsible for the execution of every surveillance of communications – article 27º of the Internal Security Act	Portuguese Territory	The law applies to the territory of Portugal.

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
Framework Law on the Intelligence System of the Portuguese Republic;	The intelligence services cannot perform mass surveillance, neither can they perform surveillance of any kind of communications	Only if, in the course of the jurisdiction of the intelligence services, they find out that a subject is suspect of committing crimes. In this case, the information is provided to the Police Forces who are responsible for criminal investigation	No surveillance can be taken upon this legislation.	N/A	N/A	Portuguese Territory	The law applies to the territory of Portugal.
Law on privacy and electronic communications Law 41/2004 of 18th of August.	Article 1, number 4 indicates that regarding criminal offences, defence, public Security and State Security,	N/A	N/A	N/A	N/A	Portuguese Territory	The law applies to the territory of Portugal.

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
	the exceptions to the law are defined in specific legislations (the one mentioned above)						

B. Details on the law providing privacy and data protection safeguards against mass surveillance

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	**List specific privacy and data protection safeguards put in place by this law(s)**	**Indicate whether rules on protection of privacy and data protection apply:** **only to nationals or also to EU citizens and/or third country nationals**	**Indicate whether rules on protection of privacy and data protection apply:** **only inside the country, or also outside (including differentiation if EU or outside EU)**
Include a reference to specific provision and describe their content	*e.g. right to be informed, right to rectification/deletion/blockage, right to challenge, etc.*	*Please, provide details*	*Please, provide details*
Constitution of the Portuguese Republic article 35	Right of access, information, rectification.	Applies to every Portuguese citizen, EU and third country nationals	Portuguese territory
Law on privacy and electronic communications Law 41/2004 of 18th of August	Right of access, information, rectification.	Applies to every Portuguese citizen, EU and third country nationals	Portuguese territory
Organic Law 4/2004 of 6th of November Legal Framework of the Information System of the	Right of rectification and deletion Limitation of Purpose	Applies to every Portuguese citizen, EU and third country nationals	Portuguese territory

Portuguese Republic (SIRP); article 27th			
Act on the organisation of the Intelligence Services	No Specific Safeguards	No Specific Safeguards	No Specific Safeguards
Internal Security Act	No Specific Safeguards	No Specific Safeguards	No Specific Safeguards
Data Protection Act Law 67/98, of 26 October.	Right of access, information, rectification, deletion and blockage. Purpose limitation Quality of the Data.	Applies to every Portuguese citizen, EU and third country nationals	Portuguese territory

Annex 2 – Oversight bodies and mechanisms

Name of the body/mechanism	**Type of the body/mechanism**	**Legal basis**	**Type of oversight**	**Staff**	**Powers**
in English as well as in national language	*e.g. parliamentary, executive/government, judicial, etc.*	*name of the relevant law, incl. specific provision*	*ex ante / ex post / both/ during the surveillance/etc. as well as whether such oversight is ongoing/regularly repeated*	*including the method of appointment of the head of such body **AND** indicate a total number of staff (total number of supporting staff as well as a total number of governing/managing staff) of such body*	*e.g. issuing legally binding or non-binding decisions, recommendations, reporting obligation to the parliament, etc.*
Council for the Oversight Of SIRP CFSIRP – Conselho de Fiscalização do SIRP	Parliamentary	Law 4/2014, of 13 August, Article 8	Regular oversight: Report analysis every 2 months about the ongoing processes. Reports are not public. Questions to the Government. Inspections and Visits. Opinions about legislative reforms. Opinions on specific topics about the subject of oversight ,	Three citizens of recognized integrity and in full capability of their civil and political rights, elected by the Parliament. Permanent staff of 1.	N/A

			The opinions are published at the Council website[13]. The Council's evaluation regarding the last three and half years is positive, despite the indication that the budget restrictions imply that activities are developed according to those restraints. Moreover, in 2012-2013, the complaints lodged and the further investigations found out that no incorrect or unlawful data processing took place by the intelligence services. In 2011 there is the reference to a public case of undue access to a reporter´s phone register. All the opinions stress the importance		

[13] Portugal, Annual Opinions of the Council for the Oversight of the SIRP, available at http://www.cfsirp.pt/Geral/Documentos/, Hyperlink accessed on 6 September 2014,

			of control and ethics management of all the System and the people that work for SIPR, regarding the compliance with their duty of non-disclosure and respect for the State and Professional Secrecy.		
CFD - SIRP - Comissão de Fiscalização de Dados - Data Oversight Commission	Judicial – Attorney General Office	Law 4/2004, of 6 November, article 8th. Article 26º	Periodical verifications of the programmes, data and intel	3 prosecutors. Staff from the Attorney General. Information on total Staff not available	Verifications. In case of violations or lack of compliance, the CFD must report to the Supervision Body.
Data Protection Commission Comissão Nacional de Proteção de Dados, CNPD	Independent Body within the Parliament	Constitution of the Portuguese Republic, article 35. Law 67/98 article 21 and following.	Verification upon complaint or self-initiative.	7 Members of the Commission. About 30 people on the Staff.	Recommendations. Legally binding Decisions. Non-binding opinions

Annex 3 – Remedies[14]

Framework Law on the Intelligence System of the Portuguese Republic				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*	No	Yes	Claims lodged with the Council for the Oversight of the SIRP within their competences, that are defined in the SIRP Framework Law, may require information and evidence to analyse if the data processing complies with the law regarding the respect for the rights and liberties	Violation of the Limitation of Purpose. Violation of privacy. Violation of duties by the Intelligence Services Staff.

[14] In case of different remedial procedures please replicate the table for each legal regime.

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection

			of the people. If the Council finds that the processing is unlawful, the data can be eliminated under article 27 of the SIRP framework law. Furthermore, under article 9 k) of the Framework Law, the Council of Oversight can propose the undergoing of inquiries, investigation, or sanctions, if the situation is serious and justifies further actions to the Government. The sanctions range from disciplinary to criminal procedures, in the case of a violation of special duties by the staff of the intelligence services, as defined by articles 28, 29 and 30 of the Framework Law. The complaints regarding the data centres can also be lodged with the SIRPS´ Data Oversight Commission, that under articles 26 and 27, can order the elimination of incorrect or unlawful data, reporting the situation to the Council for the Oversight of the SIRP.	

Analysis*	No	Yes	Claims lodged with the Council for the Oversight of the SIRP within their competences, which are defined on the SIRP Framework Law, may require information and evidence to analyse if the data processing complies with the law regarding the respect for the rights and liberties of the people. If the Council finds that the processing is unlawful, the data can be erased under the article 27th of the SIRP framework law. Furthermore, under the article 9 k) of the Framework Law, the Council of Oversight can propose the Government the undergoing of inquiries, investigation, or sanctions, if the situation is serious and justifies further actions. The sanctions can go from disciplinary to criminal procedures, in case of violation of special duties by the staff of the intelligence services, as defined by the articles 28, 29 and 30 of the Framework Law. The complaints regarding the data centres can also be lodged with the SIRPS´ Data Oversight Commission, that under the articles 26 and 27, can order the	Violation of the Limitation of Purpose. Incorrect data processed. Conservation Period Over, and the need to be extended. Violation of privacy.

			elimination of incorrect or unlawful data, reporting the situation to the Council for the Oversight of the SIRP.	
Storing*	No	Yes	Claims lodged with the Council for the Oversight of the SIRP within their competences, which are defined on the SIRP Framework Law, may require information and evidence to analyse if the data processing complies with the law regarding the respect for the rights and liberties of the people. If the Council finds that the processing is unlawful, the data can be erased under the article 27th of the SIRP framework law. Furthermore, under the article 9 k) of the Framework Law, the Council of Oversight can propose the Government the undergoing of inquiries, investigation, or sanctions, if the situation is serious and justifies further actions. The sanctions can go from disciplinary to criminal procedures, in case of violation of special duties by the staff of the intelligence services, as defined by the articles 28, 29 and 30 of the Framework Law.	Conservation Period Over. Violation of privacy.

			The complaints regarding the data centres can also be lodged with the SIRPS´ Data Oversight Commission, which under the articles 26 and 27, can order the elimination of incorrect or unlawful data, reporting the situation to the Council for the Oversight of the SIRP.	
Destruction *	Yes	Yes	Claims lodged with the Council for the Oversight of the SIRP within their competences, which are defined on the SIRP Framework Law, may require information and evidence to analyse if the data processing complies with the law regarding the respect for the rights and liberties of the people. If the Council finds that the processing is unlawful, the data can be erased under the article 27th of the SIRP framework law. Furthermore, under the article 9 k) of the Framework Law, the Council of Oversight can propose the Government the undergoing of inquiries, investigation, or sanctions, if the situation is serious and justifies further actions. The sanctions can go from disciplinary to criminal procedures, in case of violation of	Violation of privacy.

			special duties by the staff of the intelligence services, as defined by the articles 28, 29 and 30 of the Framework Law. The complaints regarding the data centres can also be lodged with the SIRPS´ Data Oversight Commission, that under the articles 26 and 27, can order the elimination of incorrect or unlawful data, reporting the situation to the Council for the Oversight of the SIRP.	
After the whole surveillance process has ended	Yes	Yes	The competences of the Council for the Oversight of SIRP, under the Framework Law, involves periodical visits to the Intelligence Services, every three months, minimum. (Article 9 d) of the Framework Law). The Council can request information regarding the functioning and the activities pursued by the intelligence services at all times. .	Violation of privacy.
Data Protection Act – Law 67/98 (general remedies)				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**

	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*	Yes	Yes	Limits to the processing of data concerning criminal investigation, only admissible by public authorities, whose legislation must be preceded by the Opinion of the CNPD, under the article 8 of the Data Protection Act. articles 22 and 23 of the Data Protection Act define the Duties and Responsibilities of the CNPD, that can order the interruption, cease or blocking of the data processing. The remedy available to citizens is the Complaint to the CNPD, that proceeds with the investigation under article 23 k) of the Data Protection Act. If the data	Unlawful processing Lack of information Lack of notification Lack of consent Violation of the right to information and right to object to the data processing. Violation of the duties to comply with the supervisor orders. Data Protection Act, particularly articles, 8, 10, 11, 12, 27, 28 36, 28 43 and 46.
Analysis*	Yes	Yes		
Storing*	Yes	Yes		

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection

			processing is unlawful, or if the controller fails to comply with its obligations (e.g. the obligation of information or notification under the article 27 and 28 of the Data Protection Act), CNPD applies the fines for administrative offences under article 38 of the Data Protection Act. If in the course of the investigation, there is ground for criminal liability, the CNPD reports to the Public Prosecution Service, under article 22, number 5, of the Data Protection Act.	
Destruction *	Yes	Yes	Disrespect for the order of destruction of the data or even the interruption, or the blockage is considered a crime of qualified noncompliance under article 46 of the Data Protection Act.	
After the whole surveillance process has ended	Yes	Yes	CNPD can still monitor and supervise the controller or processor activities and data processing to check if they are complying with the previous orders.	

General Administrative Actions, including the Liability of the State for unlawful actions or decisions				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*	No	Yes	The reference to the general State Liability must be done bearing in mind that at some point the subjects are informed that there was a data processing about them, and that the administrative decision was unlawful or illegal.	Unlawful decisions by the Administration Administrative Procedure Code (CPA)[15]
Analysis*	Yes	Yes		
Storing*	Yes	Yes		
Destruction *	Yes	Yes		
After the whole surveillance process has ended	Yes	Yes		

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection

[15] Portugal, Administrative Procedure Code Law , Law decree 442/91, of 15 November, last version available at http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?ficha=101&artigo_id=&nid=480&pagina=2&tabela=leis&nversao=&so_miolo=, Hyperlink accessed on 6 of September 2014

			Bearing in mind that context, citizens can use the general instruments available to them in their relationship with the administration, through the Administrative Procedure Code (CPA), or they can go to court, through the Administrative Courts Procedure Code (CPTA). Through the applicability of the Administrative Procedure Code, the tenant can address the administrative body responsible for the decision through a protest (article 158º/2-A CPA) or he/she can address a superior body through a hierarchical appeal (article 158º/2-b CPA). Regarding the judicial action, if the decision is considered illegal, the tenant can go to the administrative court, filing a restraining order to suspend the applicability of that decision (Article 112 CPTA) and filling the administrative law suit, which is called the common	Administrative Courts Procedure Code (CPTA)[16] Act on the Civil Liability of the State[17]

[16] Portugal, Administrative Courts Procedure Code (CPTA), Law 15/2002, of 22 of February last version available at http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=439&tabela=leis , Hyperlink accessed on 6 September 2014

[17] Portugal, Act on the Civil Liability of the State, Law 67/2007, of 31 December, available at http://dre.pt/pdf1sdip/2007/12/25100/0911709120.pdf, with the changes made by the Law 31/2008 of 17 July, available at http://dre.pt/pdf1sdip/2008/07/13700/0445404454.pdf. All Hyperlinks accessed on 6 September 2014.

			administrative action (Article 37 of the CPTA), in order to pursue compensation for the damages suffered as result of the unlawful decision of the administration. This is possible under article 7 and following of the Act of the Civil Liability of the State.	

Annex 4 – Surveillance-related case law at national level

Please provide a maximum of three of the most important national cases relating to surveillance. Use the table template below and put each case in a separate table.

Case title	– "Caso Nuno Simas" – Text of the decision is not available to the Public. The case has not yet reached a final decision in Court. [18]
Decision date	February 2014
Reference details (type and title of court/body; in original language and English [official translation, if available])	Comissão Nacional de Protecção de Dados – Portuguese Data Protection Commission TCIC – Tribunal Central de Instrução Criminal – Central Court of Criminal Investigation
Key facts of the case (max. 500 chars)	In August 2010, weekly newspaper "Expresso "published a newsbreak where it stated that the phone records of a reporter from another newspaper, "Público" had been accessed by the SIED. This happened after the publication of some pieces by the journalist that indicated that he had sources inside the intelligence services. The data was accessed through the wife of a SIED agent who worked at "Optimus", a cell phone operator. This news had consequences, both administrative and criminal. CNPD investigated and fined Optimus in over €4,5M. This case would eventually end up also in the criminal court, with five people being indicted of several crimes. The case is still under trial. Furthermore, there was also a connection between, the director of the SIED (at the time that the facts took place) and a private company, "Ongoing", to whom he worked and allegedly leaked information from the time he was working for SIED, violating his duties as an employee of the Intelligence Services

[18] Portugal, News available online, at http://expresso.sapo.pt/optimus-multada-em-45-milhoes-no-caso-secretas=f857285, ,http://en.rsf.org/portugal-intelligence-agency-spied-on-29-08-2011,40863.html, http://www.publico.pt/sociedade/noticia/tribunal-leva-a-julgamento-cinco-arguidos-no-caso-secretas-1631869, all hyperlinks accessed on 6 of September 2014.

Main reasoning/argumentation (max. 500 chars)	Regarding the administrative offence, Optimus was fined by CNPD in February 2014, as data controller, for not putting in place adequate security measures and adequate conditions for the data processing and for not respecting the conservation period. The case is still ongoing Regarding the criminal action: In April 2014, five people were indicted for several crimes: undue access to personal data, corruption, and abuse of power, violation of the Secret of State, and violation of professional secrecy.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	This case brought a key issue around the importance of complying with the best practices of security and levels of access and the importance of respecting the conservation period in a sensitive subject such as personal communications services. On the criminal aspect, the concept of the Secret of State, the duties of the people who work at the Intelligence Services and their relationship with the private sector are also issues that will be very much discussed. Also relevant will be the definition of the liability of the agent and his wife, who accessed the registers and detailed billing of the journalist.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	There are no final Decisions or consequences to report, as it is still an undergoing case. The former director of SIED, was charged with undue access to personal data, corruption, and abuse of power. The president and CEO of Ongoing and another former director of SIED, were charged with violation of the State Secret, corruption and abuse of power. Two other persons, an operative of the SIED and an employee at Optimus were charged with undue access and violation of professional secrecy. The Council for the Oversight of SIRP also reacted to this subject through an official release which can be consulted in the annual Opinion of 2011, having communicated the deficiencies identified to the Government, which ordered two internal investigations.[19]

[19] Portugal, Annual Opinion of 2011 of the Council for the Oversight of the SIRP, available at http://www.cfsirp.pt/images/documentos/Parecer%202011.pdf, Hyperlink accessed on 6 September 2014

Annex 5 – Key stakeholders at national level

Please list all the key stakeholders in your country working in the area of surveillance and divide them according to their type (i.e. public authorities, civil society organisations, academia, government, courts, parliament, other). Please provide name, website and contact details.

Name of stakeholder (in English as well as your national language)	**Type of stakeholder** *(i.e. public authorities, civil society organisations, academia, government, courts, parliament, other)*	**Contact details**	**Website**
Prime Minister Primeiro Ministro, PM	Government	Presidência do Conselho de Ministros (PCM) Rua Prof. Gomes Teixeira n.º 2 1399-022 LISBOA **Tel.:** (+351) 213 927 600 **Fax:** (+351) 213 927 918	www.portugal.gov.pt/pt.aspx
SIRP SG	Government	Presidência do Conselho de Ministros (PCM) Rua Prof. Gomes Teixeira n.º 2 1399-022 LISBOA **Tel.:** (+351) 213 927 600 **Fax:** (+351) 213 927 918	www.sirp.pt
SIS	Public authority	Forte da Ameixoeira	www.sis.pt

		Calçada do Forte da Ameixoeira 1750-111 Lisboa (+351) 217 523 300	
SIED	Public authority	Estrada do Forte do Alto do Duque 1400-157 Lisboa PORTUGAL Tel: (+351) 210 920 700 Fax: (+351) 210 920 765	www.sied.pt
CNPD	Public authority	Rua de São Bento 148, 3º 1200-821 Lisboa Tel: (+351) 213928400 Fax: (+351) 213976832 e-mail: geral@cnpd.pt	www.cnpd.pt
Parliament	Parliament	Palácio de São Bento Rua de São Bento, 1249-068 Lisboa Tel.: (+351) 213 919 000 Fax: (+351) 213 917 440	www.parlamento.pt
Attorney General	Public authority	Rua da Escola Politécnica, 140 - 1269-269 Lisboa - Portugal	www.pgr.pt

		Tel: (+351) 21 392 19 00 Fax: (+351) 21 397 52 55 e-mail: mailpgr@pgr.pt	
Ombudsman	Public authority	Rua Pau de Bandeira, 9 1249-088 LISBOA PORTUGAL Tel.: (+351) 213926600/19/21/22 Fax.: (+351) 213961243 e-mail: provedor@provedor-jus.pt	www.provedor-jus.pt
Council for the Oversight of SIRP	Public Authority	Av. D. Carlos I, 130 1200-651 Lisboa Tel : (+351) 21 391 70 57 Fax (+351) 21 391 70 03 geral@cfsirp.pt	www.cfsirp.pt
Superior Intelligence Council	Consultative Body presided by the Prime Minister	Presidência do Conselho de Ministros (PCM) Rua Prof. Gomes Teixeira n.º 2 1399-022 LISBOA **Tel.:** (+351) 213 927 600 **Fax:** (+351) 213 927 918	www.portugal.gov.pt/pt.aspx
SIRP´s Data Oversight Commission	Public authority constituted by Public Prosecutors and	Rua da Escola Politécnica, 140 - 1269-269 Lisboa - Portugal	www.pgr.pt

	located at the Attorney General Office.	Tel: (+351) 21 392 19 00 Fax: (+351) 21 397 52 55 e-mail: mailpgr@pgr.pt	

Annex 6 – Indicative bibliography

1. **Government/ministries/public authorities in charge of surveillance**

Portugal, SIRP Framework Law – Official Records of the discussion in the Parliament (*Proposta de Lei 135/IX - Altera a Lei-Quadro do Sistema de Informações da República Portuguesa*), available at www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=20546. Hyperlinks accessed on 8 of August 2014.

Portugal, Act on the Organisation of the Intelligence Services - Records of the discussion in the Parliament *(Proposta de Lei 83/X. stabelece a Orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS) e revoga o Decreto-Lei n.º 225/85, de 4 de Julho, e o Decreto-Lei n.º 254/95, de 30 de Setembro)*, 14 July 2006, available at www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=33237

Portugal, Council for the Oversight of Portuguese Republic's Information System (Conselho de Fiscalização do Sistema de Informações daRepública Portuguesa), Annual Opinion 2011 (*Parecer relativo ao ano de 2011*), Official Gazette, II Serie-E, No 38, 2 July 2012, available at: http://cfsirp.pt/images/documentos/Parecer%202011.pdf, hyperlink accessed on 24 September 2014

Portugal, Council for the Oversight of Portuguese Republic's Information System (Conselho de Fiscalização do Sistema de Informações daRepública Portuguesa), Annual Opinion 2012 (*Parecer relativo ao ano de 2012*), Lisboa, Assembly of the Republic, 2013, available at http://cfsirp.pt/images/documentos/Parecer%20CFSIRP%20referente%20a%20%202012.pdf

Portugal, Council for the Oversight of Portuguese Republic's Information System (Conselho de Fiscalização do Sistema de Informações daRepública Portuguesa), Annual Opinion 2013 (*Parecer relativo ao ano de 2013*), Lisboa, Assembly of the Republic, 2014, available at http://cfsirp.pt/images/documentos/Parecer_CFSIRP_2013.pdf,

Portugal, Law 53/2008, approves the Law of Internal Security (*Lei n.º 53/2008, que aprova a Lei de Segurança Interna)*, 29 August 2008, available at: https://dre.pt/application/dir/pdf1sdip/2008/08/16700/0613506141.pdf.

Portugal, Constitutional Law 1/2005, VII Constitutional revision (*Lei Constitucional n.º 1/2005, VII Revisão constitucional*), 12 August 2005, available at: https://dre.pt/pdf1sdip/2005/08/155A00/46424686.pdf. English version available at www.en.parlamento.pt/Legislation/CRP/Constitution7th.pdf.

Portugal, Organic Law 4/2014, Fifth Amendment to the Framework Law on the Intelligence System of the Portuguese Republic *(Lei Orgânica n.º 4/2014, Quinta Alteração à Lei Quadro do Sistema de Informações da República Portuguesa)* , 13 August 2014, available at; https://dre.pt/pdf1sdip/2014/08/15500/0419404206.pdf.

Portugal, Law 41/2004, transposing Directive 2002/58/EU on processing of personal data and privacy protection on electronic communications sector (*Lei n.º 41/2004 que transpõe para a ordem jurídica nacional a Directiva n.º2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas*), 18 August 2004, available at: https://dre.pt/application/dir/pdf1sdip/2004/08/194A00/52415245.pdf.

Portugal, Law 32/2008, transposing Directive 2006/24/EU on the retention of data generated or processed in the context of provision of publicly available electronic communications services or of public communications networks *(Lei n.º 32/2008 que transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações*), 17 July 2008, available at: https://dre.pt/application/dir/pdf1sdip/2008/07/13700/0445404458.pdf.

Portugal, Organic Law, which proceeds to the 20th amendment of the Penal Procedure Code (*Lei Orgânica n.º 2/2014 que procede à 20ª alteração do Código de Processo Penal*), 6 August 2014, available at: https://dre.pt/application/dir/pdf1sdip/2014/08/15000/0407404078.pdf.

Portugal, Law 109/2009, Law on Cybercrime (*Lei n.º 109/2009, Lei do Cibercrime*), 15 September 2009, available at: www.dre.pt/pdf1s/2009/09/17900/0631906325.pdf.

Portugal, Decree-Law 18/2008, which approves the Administrative Procedure Code (*Decreto-Lei nº 18/2008 que aprova o Código do Procedimento Administrativo*), 29 January 2008, available at: www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=480&tabela=leis

Portugal, Lei 63/2011 which approves the Administrative Courts Procedure Code (*Lei n.º 63/2011que aprova o Código de Processo nos Tribunais Administrativos*), 14 December 2011, available at: www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=439&tabela=leis.

Portugal, Law 67/2007, which approves the State and other Public Entities' Extra-contractual Civil Liability (*Lei n.º 67/2007 que aprova o Regime da Responsabilidade Civil Extracontratual do Estado e Demais Entidades Públicas*), 31 December 2007, available at: http://dre.pt/pdf1sdip/2007/12/25100/0911709120.pdf.

Portugal, Law 31/2008, which proceeds to the 1st amendment of Law on the State and other Public Entities' Extra-contractual Civil Liability (*Lei n.º 31/2008 que procede à 1ª alteração ao Regime da Responsabilidade Civil Extracontratual do Estado e Demais Entidades Públicas*), 17 July 2008, available at: https://dre.pt/application/dir/pdf1sdip/2008/07/13700/0445404454.pdf.

2. **National human rights institutions, ombudsperson institutions, national data protection authorities and other national non-judicial bodies/authorities monitoring or supervising implementation of human rights with a particular interest in surveillance**

Portugal, Opinion of the CNPD about the bill for the Act on the Organisation of the Intelligence Services, Opinion 26/2006 *(Parecer nº26/2006)*, 19 July 2006, available at www.cnpd.pt/bin/decisoes/par/40_26_2006.pdf. Hyperlinks accessed on 24September, 2014.

Portugal, Law 17/2013 re-published as the 3rd amendment to Law 9/91 of 9 April on the Statute on the Ombudsperson's Duties (*Lei n.º 17/2013 que procede à 3.ª alteração e à republicação da Lei 9/91, de 9 de Abril relativa ao Estatuto do Provedor de Justiça*), 18 February 2013, available at: http://dre.pt/pdf1sdip/2013/02/03400/0097900986.pdf.

3. **Non-governmental organisations (NGOs)**

N/A

4. **Academic and research institutes, think tanks, investigative media report.**

Reis, S. and Silva, M., (2007), 'O sistema de informações da República Portuguesa', *Revista da Ordem dos Advogados*, Ano 67, Vol. III, available at: www.oa.pt/Conteudos/Artigos/detalhe_artigo.aspx?idc=30777&idsc=65580&ida=65520. Hyperlinks accessed on the 7 August 2014.

Pereira, R., (2004), 'Os Desafios do Terrorismo: a Resposta Penal e o Sistema das Informações', in: Moreira, A. (coord.) (2004) *Informações e Segurança – Estudos em Honra do General Pedro Cardoso*, Lisboa, Prefácio Edições.

Carvalho, J. (2006), 'Segurança Nacional e Informações', *Segurança & Defesa*, n.º 1, p. 92, available at: www.segurancaedefesa.com/