REGIONAL CONSULTATION ON
NATIONAL SECURITY AND THE RIGHT TO INFORMATION

National Questionnaire
European Consultation, Copenhagen, Denmark, 20-21 September 2012

Country analysed:

SPAIN

Expert analyst:

Name of person completing this form:

SUSANA SANCHEZ FERRO

Institutional or organizational affiliation:

UNIVERSIDAD AUTONOMA DE MADRID (SPAIN)-AUTONOMA UNIVERSITY OF MADRID (SPAIN)

1. **A National Security Exception to the Right to Information**

   a. Does the term "national security" or a similar term (*e.g.*, "state security"; "vital national interest") appear in the law as a basis for restricting the public's access to information? *[Principle 2]*

      Please check one: ☒ Yes ☐ No

      If your answer refers to a similar term, please state that term here:

      There are several rules or laws that along with the term national security use that of national defence to exclude access to information. Article 105 of the Spanish Constitution and article 37.5 of the Law regulating the functioning of the Public Administration (Ley 30/1992, of 26th November, de Régimen Jurídico de las Administraciones Públicas y el Procedimiento Administrativo Común) regulating citizen's access to public archives and registries do so, as well as article 2 of the Official Secrets Act (Law 9/1968 of 5th April, modified by Law 48/1978 of 7th October, de Secretos Oficiales) regulating the information that can be classified.

      If you checked "Yes":

      i. How is "national security" (or the similar term) defined for purposes of justifying non-disclosure of information? *[Principle 2, 3a]*

      Neither article 105 of the Constitution, nor the Official Secrets Act or the Law regulating the functioning of the Public Administration defines what constitutes national security or national defence. The definition of national defence is contained in the National Defence Act of 2005 (Organic Law 5/2005 of 17th November, Ley Orgánica de la Defensa Nacional). Article 2 of the law states that the purpose of the defence policy is the protection of the whole Spanish society, of its Constitution, of the superior values, principles and institutions contained in the Constitution, of the social and democratic State, of the full exercise of rights and liberties, and of the preservation, independence and territorial integrity of Spain. Likewise its purpose is to contribute to the preservation of the international peace and

security, in the context of the agreements made by the Spain. Article 8 of the Spanish Constitution when defining the role of the armed forces says that they have to defend the Spanish sovereingty and independence, its territorial integrity and the constitutional order. It is interesting to mention that the old organic law regulating the basic criteria of the national defense (Organic law 6/1980, of 1st July, Ley Orgánica por el que se regulan los Criterios Básicos de la Defensa Nacional y la Organización Militar), already repealed by the 2005 law, in its article 3 expressly said that the national defence should be organised and executed as to proportionate an effective national security. So national security would be the result of a good national defence. This reference has disappeared in the actual legislation. When the old law (Organic Law 6/1980) was discussed in parliament an amendment to include in the law a reference saying that the defence was aimed to protect the nation only against external attacks was rejected by parliament (Official Journal of Congress, 1st Legislature, A series, number 72.I.1, of 10th October of 1979: Boletín Oficial de las Cortes Generales, Congreso de los Diputados, 1ª Legislatura, Serie A, núm. 72.I.1, de 10 de octubre de 1979, page 356/5). From the wording of article 2 of Law 5/2005 one can derive that the law does not only contemplate external attacks.

ii. Does the definition of "national security" include international relations?

Please check one: ☒ Yes ☐ No

iii. Does the definition of "national security" include protection against domestic security threats (*e.g.*, law enforcement)?

Please check one: ☒ Yes ☐ No

b. Are there any categories of information (*e.g.*, intelligence operational files) that are exempt from disclosure on the basis of national security? *[Principle 9]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. Please list the categories of information that are exempt:

We must explain here that article 37, section 5 of the Law 30/1992, regulating citizen's access to public archives and registries says only that there is no right of access to records containing information about National Security or National Defence and article 37, section 6 of the same Law says that the access to archives subject to the Official Secrets Act will be ruled by the Official Secrets Act. On the other hand, article 13.2 of the Law 27/2006, of 18th July, regulating the right of access, public participation and access to jurisdiction in environmental matters states that there will be no access to this kind of information if the disclosure of the information could affect negatively the international relations, the national defence or the public security. Therefore the list of categories exempted from disclosure that exist is not directly contained in the laws regulating

public access to information. The sole list of categories exempted from disclosure existing in our country is the list of categories of classified information. This list is not included in the Official Secrets Act and, as we will see, has been done by the Government and in some cases some categories are contained in some other laws. See answer to question 5.a.i of this questionnaire where we give the list of categories of classified information.

ii. Is exemption of these categories absolute?

Please check one: ☒ Yes ☐ No

If you checked "No", please explain when the exemption does and does not apply?

c. Are there any public offices or officials (*e.g.*, military branches, intelligence agencies, police) that are exempt from disclosure obligations? *[Principle 6]*

Please check one: ☐ Yes ☒ No

If you checked "Yes":

i. Please list the offices or officials that are exempt:

ii. Is the exemption of these offices or officials absolute?

Please check one: ☐ Yes ☐ No

If you checked "No", please explain when the exemption does and does not apply?

d. Do disclosure obligations apply to non-state actors that are serving as agents or contractors for the government? *[Principle 1a]*

Please check one: ☐ Yes ☒ No

e. Beyond any obligation to disclose information upon request, do public authorities have an affirmative obligation to publish information? *[Principle 1b]*

Please check one: ☐ Yes ☒ No

If you checked "Yes", what information do the security sector, defence, and intelligence agencies have an affirmative obligation to publish? How often is this information affirmatively published by these agencies in practice?

2. Requirements for Denying a Request for Information

a. Upon receipt of a request for information, is a public authority always required to confirm or deny whether it holds the requested information? *[Principle 21]*

Please check one: ☒ Yes ☐ No

If you checked "No", under what circumstances may a public authority refuse to confirm or deny whether it holds the requested information?

b. In denying a request for information, is a public authority required to provide written reasons for the denial? *[Principle 22, 4c]*

Please check one: ☒ Yes ☐ No

c. What requirements are there for a public authority to describe information responsive to a request that it withholds (*e.g.*, Is there a duty to specify the number of pages withheld, or to identify the category of information)? *[Principle 25]*

The public authority is only obliged to give a very brief general explanation of the reasons for withholding the information. It would be enough to say that the information is classified or that it affects national defence or national security. As there is no Freedom of Information Act, the articles applicable here are article 37.4 and article 54 of Law 30/1992, regulating the functioning of the Public Administration (there is no duty to specify the number of pages withheld or to identify the category of information).

d. Is a declaration or certification by the public authority, denying a request for information, that disclosure would cause harm to national security conclusive? *[Principle 4d]*

Please check one: ☐ Yes ☒ No

e. What information or documentation must support an assessment that disclosure would cause harm to national security? Is this information provided to the public? *[Principle 4c]*

There is no obligation to support the assessment with any documentation or additional information. Article 11 of the Decree developing the Official Secrets Act (Decree 242/1969) requires the authority classifying the information to specify the area affected by the information according to article 2 of the Official Secrets Act. Article 2 of the Official Secrets Act states that the Government and the Committee of the Chiefs of Staff of the Armed Forces within their area of competence can classify those acts, issues, documents, data or objects the knowledge of which by unauthorized persons could cause harm or threaten (put at risk) national security or national defence. As we said, the public authority is only obliged to give a very brief general explanation of the reasons to withhold the information. In the case of two researches that wanted to access some documents of the Foreign Affairs Ministry the Technic Secretary General of the Archive in charge of answering the request sent a letter to the researchers reproducing the agreement of the Government declaring secret a set of categories of information (see the list of categories classified by the Government in the comments at the end of the document and, in Spanish, the answer reproduced by the press in

http://ep00.epimg.net/descargables/2012/06/03/81b3c3748773b522e38eb34079877132.pdf).

f. Where there is doubt about whether disclosure would harm national security, does the law favour disclosure? *[Principle 4b]*

Please check one: ☐ Yes ☒ No

g. Is a public authority required to segregate and disclose non-exempt information within a document if those portions of the document are reasonably segregable? *[Principle 24]*

Please check one: ☐ Yes ☒ No

h. What time limits exist for a public authority to respond to a request for information? Are these time limits enforced in practice? *[Principle 27]*

Here there is no speficic legislation dealing with access to information. The time to respond is the general one to respond to any request directed to the Public Administration, three months (article 42.3 Law 30/1992) save in the case of petitions to access to environmental information. In this last case the time to respond is one month save that the volume or complexity of the information is such that impedes the compliance with the time limit. In this case the time limit can be extended to two months but the authority must notify before one month to the applicant the extension of the limit and the reasons to extend it (article 10.2.c Law 27/2006, of 18th July, regulating the Right of Access, Public Participation and Access to Jurisdiction in Environmental Matters).

3. Classification Procedures

a. Are classification rules publicly available? *[Principle 13]*

Please check one: ☒ Yes ☐ No Cite: In the Official Secrets Act (Law 9/1969, modified by Law 48/1978)

b. What criteria are used to determine whether information may be classified? *[Principle 12]*

The sole criterion is whether the knowledge of the information by an unauthorised person could cause harm or threaten (put at risk) national security or national defence (article 2 of the Official Secrets Act).

c. Is the classification status of information conclusive in determining whether a request for that information will be denied? *[Principle 20]*

Please check one: ☒ Yes ☐ No

d. Does the law consider the public's interest in the disclosure of information when deciding whether to classify information? *[Principle 5]*

Please check one: ☐ Yes ☒ No

If you checked "Yes", please explain, in the terms provided by the law, what consideration is given to the public's interest:

e. Does the law specify levels of classification (*e.g.*, "Top Secret", "Secret", "Confidential")? *[Principle 12c]*

Please check one: ☒ Yes ☐ No

If you checked "Yes", please list and define the classification levels:

The Law (article 3 of the Official Secrets Act) provides for the existence of two classification levels: "secreto" equivalent to top secret, and "reservado" equivalent to secret (please, see comments at the end of the document) but it does not define in a concise manner how to differentiate those categories. The Act in article 3 only says that the information will be classified in one or another category in accordance with the degree of protection needed by the information (please, see comments at the end of the document).

f. Who has the authority to classify information? May this authority be delegated? *[Principle 14a]*

According to article 4 of the Official Secrets Act, the Government and the Joint Committee of Chiefs of Staff (Armed Forces) have the authority to classify information (please, see comments at the end of the document). But the Joint Committee of Chiefs of Staff have only advisory functions (article 12 National Defence Organic Law -Law 5/2005, of 17th November-). The law says in article 4 that both organs are allowed to classify information in the sphere of their competences: the Joint Committee of Chiefs of Staff and its substitute in the new National Defence Law do not have decision-making powers, so we understand they really do not have the capacity to classify information. According to article 5 of the Official Secrets Act this authority cannot be delegated (please see comments at the end of the document).

g. Do classification authorities have a duty to classify information? *[Principle 11b]*

Please check one: ☐ Yes ☒ No

If you checked "Yes", when is that duty triggered?

h. Is there a duty for public authorities to state reasons for classifying information? *[Principle 11b]*

Please check one: ☒ Yes ☐ No

i. Are there any penalties for improperly classifying information?

Please check one: ☐ Yes ☒ No

If you checked "Yes", what are the penalties?

j. When documents are classified, must the documents bear classification markings? *[Principle 12]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. What information is contained in the classification marking?

Article 10.1 of the Official Secrets Act refers the question to the Decree 242/1969, developing it. Article 11 section a) of this Decree developing the Official Secrets Act (Decree 242/1969) requires to specify in the document the authority who classifies the information, the declaration of classification, the place, date, the short form or whole signature of the authority classifying the document and the sphere affected by the information according to article 2 of the Official Secrets Act. Article 2 of the Official Secrets Act states that the Government and the Committee of the Chiefs of Staff of the Armed Forces within their area of competence can classify those acts, issues, documents, data or objects the knowledge of which by unauthorized persons could cause harm or threaten (put at risk) national security or national defence. Article 11 c) of the Decree states that whenever it is possible to classify parts of the document with a lower degree, every part will be classified according to its content but the whole document will bear the mark of the highest category of classification. On the other hand, article 3 section III of the Decree says that whenever possible, the authority in charge of classifying the information will determine the duration of the classification, mentioning if it could be finished or lowered the classification level to the following category of classification.

ii. Is a separate classification marking needed for each section of a document?

Please check one: ☒ Yes ☐ No

k. Is the identity of the person responsible for a classification decision indicated on the document, or otherwise easily traced, to ensure accountability? *[Principle 14b, 22b]*

Please check one: ☒ Yes ☐ No

l. Does classified information lose its classified status if it becomes widely available in the public domain?

Please check one: ☐ Yes ☒ No

If you checked "Yes", please explain how the declassification of information based on its availability in the public domain is triggered in practice:

m. Can information be classified if it originated in the public domain?

Please check one: ☒ Yes ☐ No

If you checked "Yes", please explain under what circumstances:

There is no prohibition in the law to do so. It would be difficult because the authorities classifying information must follow article 2 of the Official Secrets Act that states that the classification of information can only be done if the knowledge of acts, issues, documents, data or object by unauthorized persons could cause harm or threaten (put at risk) national security or national defence.

4. Declassification Procedures

a. When information is classified, does the classifier specify a time (date or event) that triggers the declassification of the information? *[Principle 18b]*

Please check one: ☒ Yes ☐ No

b. What is the maximum duration of classification? Can this time period be extended? *[Principle 18c]*

There is no maximum duration established by the law (see comments at the end of the document for questions 4 a) and b).

c. May information ever be classified indefinitely (in law or in practice)? *[Principle 18c]*

Please check one: ☒ Yes ☐ No

d. Are decisions to classify information reviewed periodically to ensure that the original reason for the classification is still valid? *[Principle 14a]*

Please check one: ☒ Yes ☐ No

If you checked "Yes", how often are classification reviews performed?

The Decree 242/1969 only says that to avoid excessive accumulation of classified material the authority in charge of classifying the information will establish a procedure to determine, periodically, the convenience of reclassifying (in a lower category) or declassifying the classified material (article 3 section IV of the Decree). Norm NS/04 of the National Security Delegated Authority, who is the director of the National Intelligence Centre, provides that the Control Organs of the Administration and the users of the classified information will carry out a continuous review of the classified information to proceed to destroy that useless or obsolete. There is no systematic review of classification done with a precise method. There are no procedures for en bloc (bulk and/or sampling) declassification.

e. What is the procedure for requesting the declassification of documents?

Article 7 of the Official Secrets Act only establishes that the authority that has the power to classify the information is the only one with the power to decide to declassify it. There is no specific procedure established by the law to request the declassification of documents. As it is so and as the Government (and the Joint Chiefs of Staff but,

as we already said, we do not think that they should be recognised the power to classify) is the only one with the power to classify documents following the Official Secrets Act the request should be directed to the Government following the ordinary administrative or judicial channels.

f. Can declassification requests be made by the public? *[Principle 19d]*

Please check one: ☒ Yes ☐ No

g. Does the law consider the public's interest in the disclosure of information when deciding whether to declassify information? *[Principle 19a]*

Please check one: ☐ Yes ☒ No

If you checked "Yes", please explain, in the terms provided by the law, what consideration is given to the public's interest:

5. Categories of Information that are Classifiable

a. Does the law list specific categories of information that may be classified on national security grounds?

Please check one: ☒ Yes ☐ No Cite:

If you checked "Yes":

i. What categories of information are included in this list? *[Principle 9]*

(Please, see comments at the end of the document)

The Secret Funds Act (Law 11/1995, of 11th May) in article 1 declares secret those funds established in the Annual Finance Law intended to cover the expenses deemed necessary for the national defence and security.

The law on Measures for the Control of Chemical Substances liable to be diverted for the Production of Chemical Weapons also declares secret the information handled in accordance with the law (Law 49/1999, of 20th November).

By agreement of the Government of 1986 the following categories of information are classified information:

1. Several Defence Documents
   a. The National Defence Directive
   b. The National Defence General Plan
   c. The Joint Strategic Plan
   d. Plans and programs resulting from the Joint Strategic Plan
2. Information, analyses, and evaluation of actual or potential threats to the peace and security of Spain.
3. The content of the conversations aimed at the adoption of international agreements about defence or military matters or those

that can affect the national security and national defence of Spain.
4. Cryptology
5. Troops deployment, systems of communication, control and command structure of the military permanent net.
6. The deliberations of the Chief of Staff Committee (and other Defence organs).
7. The activities, structure, organization, sources and methods of the intelligence services. Their personnel, facilities, databases, and the information and data that would reveal those [this exemption was first adopted by the Government in a more restricted form and was expanded and is now contained in article 5.1 of the National Intelligence Centre Act (Law 11/2002, of 6th of May)].
8. Efficiency of the task forces and moral of the military units.
9. Position of the personnel with an special status
10. Security plans for Public Institutions and Armed Forces centres or organs, and war weapons production centres as well as protection plans for their personnel.
11. Military research and scientific developments carry out by military industries or defence related industries.
12. Production, acquisition, supplies and transport of weaponry.
13. Individual reports and sanctions to members of the Armed Forces
14. Personnel, equipment and means of the military units.
15. Information classified by international agreements ratified by Spain and incorporated into the Spanish legal system, as well as that classified by allied international organizations or allied powers will receive the same protection as that received from them by the Spanish information.

By agreement of the Government of 1996 the following categories of information are classified:

1. Structure, organization, methods sources and operation technichs used against terrorism by the State security forces and all information that can reveal their sources.
2. Data files of the Prisons Administration.

By agreement of the Government of 2010 (following a proposal of the Spanish Foreign Affairs Ministry) the following categories of information are classified whenever their non-authorised disclosure could harm or seriously put at risk (or just put at risk if the classification is confidential) the national security and defence of Spain, of their allies and friends, the political, social, economic and commercial interests and the diplomatic relations with other countries:

1. Spanish basic standpoints and strategies in political, security, economic and commercial negotiations related to the essential interests of the country in the bilateral context as well as in the context of the European Union, The North Atlantic Treaty Organization, Iberoamerican Conference, and other Organizations and International Conferences.

2. Information about Spanish standpoints in internal or international conflicts of political, social, economic or commercial nature that can compromise Spanish interests or its opportunity to negotiate with other states
3. Information concerning the activity of terrorist groups and movements link to them, of organized crime and the traffic of drugs, persons and weapons, with ramifications or an impact in Spain or in the Countries with which Spain has signed agreements on these issues or with which Spain has a friendship relation.
4. Information concerning the deployment of Spanish and allied Armed Forces and Security Forces units in Spain as well as in international missions.
5. Negotiations and good practices on kidnapping and the release of Spanish or foreign citizens as well as information concerning extradition and transport of convicted persons.
6. Mediation contacts and good practices carry out by Spain with other countries and opposition groups and leaders to facilitate peace processes and the promotion and defence of human rights.
7. Human rights protection, especially those linked with especially sensitive humanitarian cases and the negotiations with other countries in this regard.
8. Asylum and refugee questions.
9.Spanish and Foreigners Chiefs of Mission approval procedures
10.I Information related to questions affecting the sovereignty, independence and territorial integrity of Spain or friend countries and the Spanish standpoints on interstate or intrastate conflicts.
11. Information related with the implementation of bilateral or multilateral international agreements signed by Spain on security and defence issues, including those related with overflights, stays and stopovers of planes and ships.
12. Issues related with the most serious crimes of international relevance under the jurisdiction of the International Criminal Court or other international courts as well as the Spanish courts.
13. Information concerning the preparation of the trips of His Majesty the King and Her Majesty the Queen, and the Prime Minister, and when circumstances so required, of the Ministers and other Authorities of the State.
14. Keys for encryption and cryptographic material
15. Interviews with foreign dignitaries and diplomats with implications for the interests of the country or the international relations.
16. Support to tenders of Spanish firms abroad and in especially serious disputes affecting them.
17. Spanish candidacy to posts in international organizations.

ii. Is this list exhaustive?

Please check one: ☐ Yes ☒ No

b. Does the law prohibit any categories of information from being classified?

Please check one: ☐ Yes ☒ No Cite:

Please, see comments at the end of the questionnaire

If you checked "Yes", please identify which categories: *[Principle 10]*

In particular, does the law prohibit classification of:

i. human rights violations

Please check one: ☐ Yes ☒ No

ii. government corruption

Please check one: ☐ Yes ☒ No

iii. the existence of a government entity

Please check one: ☐ Yes ☒ No

iv. the budget or expenditures of a government entity

Please check one: ☐ Yes ☒ No

v. the existence of a law (or portion of a law)

Please check one: ☒ Yes ☐ No

vi. emergency response plans

Please check one: ☐ Yes ☒ No

If you checked "Yes" to any of the above, please provide additional detail:

The existence of a law cannot be secret. The Rule of Law, and in particular article 9.3 of the Spanish Constitution guarantees the publicity of all regulations.

6. Review of a Denied Request for Information

a. Is there an opportunity for a speedy, low-cost review of a denied request for information by an independent authority? *[Principle 28a, 3e]*

Please check one: ☐ Yes ☒ No

b. Is there an opportunity for judicial review of a denied request for information? *[Principle 28a, 3e]*

Please check one: ☒ Yes ☐ No

7. Judicial Proceedings

a. Do courts have the authority to examine classified information that the government seeks to keep secret on national security grounds? *[Principle 29b]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. May a judge order the release of information if s/he determines that the information does not need to be kept secret, despite a public authority's assertion that national security justifies withholding the information? *[Principle 29d]*

Please check one: ☒ Yes ☐ No

ii. Do judges normally defer to the public authority's assessment that disclosure would harm national security? *[Principle 29c]*

Please check one: ☐ Yes ☒ No

b. Are judicial decisions required, according to the law, to be made available to the public (subject to redactions to protect privacy interests)? *[Principle 31b]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. May national security justify withholding part of a court decision?

Please check one: ☐ Yes ☒ No

ii. May national security justify withholding an entire court decision?

Please check one: ☐ Yes ☒ No

c. Are court hearings and trials presumptively open to the public? *[Principle 31c]*

Please check one: ☒ Yes ☐ No

d. Can a court case ever be kept entirely secret, such that it is not even recorded on the court's public docket? *[Principle 31b]*

Please check one: ☐ Yes ☒ No

e. Must all evidence that forms the basis of a criminal conviction be made available to the public? *[Principle 31c]*

Please check one: ☐ Yes ☒ No

What, if any, exceptions exist on the basis of national security?

The hearings and trials are presumptively open to the public: Article 120 of the Spanish Constitution: Judicial proceedings shall be public, with the exceptions provided for by the laws on procedure; Article 24 section 2 of the Spanish Constitution: all persons have the right to a public trial.
The evidence that forms the basis of the criminal conviction is presented and discussed during what we called the oral trial. The press and public may be excluded from all or part of the trial in the interest of morals, public order, the protection of rights or the owed respect for the person offended or his/her family (article 295 of the Militar Procedural Code, article 680 of the Code of Criminal Procedure and article 232 of the Organic Law regulating the Judicial Power -Law 6/1985 of 1st of July-.). The courts have extended the notion of public order to include also national security reasons,

interpreting the law in accordance with article 6.1 of the European Convention on Human Rights and article 14.1 of the International Covenant on Civil and Political Rights (article 10 section 2 of the Spanish Constitution says that regulations relative to basic rights and liberties which are recognized by the Constitution shall be interpreted in conformity with the Universal Declaration of Human Rights and the international treaties and agreements on those matters ratified by Spain). The judge will have to weight the right to a public judgment of article 24 of the Spanish Constitution with other values that must be protected (in this case, national security).
We have some examples of how this exception to the publicity of the trial has been used. One was in the context of a case against a Colonel that was convicted because he microfilmed intelligence documents before being removed from his position. He took the documents with him (and afterwards the press published some of the documents). In its Decision number 15/1998, of 30th of March, hearing an appeal by this Colonel, the Supreme Court (Military Section) said that the closing of the trial to the public was justified in the case because very important issues for Spain and its allies were at stake and in the debate at the trial the witnesses or the accused could reveal information that would have a very negative impact on the highest interests of the State. The decision to close the trial was also considered to be valid as it also was aimed at protecting the physical integrity and lifes of certain members of the intelligence services that would have gone under a serious risk if there had been any data revealed at the trial that could have helped to identify them. The Supreme Court (Criminal Section) in its Decision 1094/2010 of 10th of December, also justifies the closing of another trial to the public. The Court was hearing an appeal of a former National Intelligence Centre agent that took away from the Centre some classified documents with the intention to reveal the secret information to the Russians. The decision to close the trial was considered to be justified: there was going to be a debate about documents of the National Intelligence Centre that had been already declassified by the government in part but the discussion between accusation and defence could imply the revelation of classified information, including information about the methods of the National Intelligence Centre, and there were going to be National Intelligence Agents testifying as witnesses.

f. Must all evidence that forms the basis of a criminal conviction be shown to the accused, including in cases involving national security? *[Principle 32]*

Please check one: ☒ Yes ☐ No

If you checked "No":

i. What limitations exist on the disclosure of information to the accused on the basis of national security?

ii. What information, if any, must be provided to the accused in lieu of the classified evidence?

iii. Are there other safeguards to protect the accused's right to a fair trial? (*e.g.*, Can the accused hire special counsel who have access to all of the classified evidence, pursuant to security clearance?)

g. May the government refuse to disclose information to the opposing party in any of the following court proceedings, on the basis of national security?

i. A *habeas corpus* claim

Please check one: ☒ Yes ☐ No

ii. A claim of grave human rights violations (*e.g.*, torture) brought against a public authority *[Principle 33a]*

Please check one: ☒ Yes ☐ No

iii. A tort claim brought against a public authority *[Principle 33a]*

Please check one: ☒ Yes ☐ No

If you checked "Yes" for any of the above, please indicate what safeguards, if any, are in place to protect the fairness of the proceeding.

What we are going to explain is not only valid for the proceedings mentioned in question 7 section g of the questionnaire, but for all type of judicial proceedings, including criminal proceedings. We are about to explain what solution has been given by the Spanish Courts to the problem of the need to use classified information as evidence in a judicial proceeding when there is a refusal by the Government to declassify such information.

In Spain there is no procedure to disclose secret information just to the opposing party, either the information is kept secret and the party and the judge of the proceeding do not have access to the evidence - and so the judge will have to decide with the open material of the case if he has to dismiss the case or not- or the information is finally declassified "by order of the Supreme Court" and then it is incorporated to the case and it becomes public.

The Official Secrets Act provides in article 7 that only the classifiers of the information (the Government) can declassify classified information. In article13 the Official Secrets Act provides that classified information cannot be communicated, disseminated, published or used outside the limits established by the Act. Article 8 says that only those authorized to access classified information will be able to do it, in the conditions and with the limits established by the law. The Act contemplates that the Congress and the Senate will have access to classified information, always in the way established by

their House rules (art. 10.2), but does not say anything about access by the judges. In the Act, the prevalence of national security over the Judicial Power seems to be absolute.

Notwithstanding that, the Spanish Supreme Court (Decisions of 4th of April of 1997) determined that it, but only it, has the power to review the classification of the information done by the Government and decide over the incorporation of the material evidence to any case. The Supreme Court has five different sections and section three (sala de lo Contencioso-Administrativo) in charge of reviewing the acts of Government will be the one reviewing the classification of the information (based on articles 2.a and 12.1 of the Law that regulates the jurisdiction on administrative matters: Law 29/1998, of 13th July reguladora de la Jurisdicción Contencioso-Administrativa). It will do it in camera and only after the following procedure has taken place:
1) The Judge or the party in the proceeding that considers that some evidence is adequate and relevant to the case has to ask the Government through the established channels (article 187 of the Code of Criminal Procedure) to declassify the information [as established in the Judgment of the Conflicts of Jurisdiction Court of 14th December 1995, solving conflict number 10/1995-T, between the Ministry of Defense and Judge Garzón, who was judge of section number 5 of the Audiencia Nacional and who wanted to incorporate some classified information to the enquiry of a case about illegal state terrorism (BOE núm 306, de 23 de diciembre de 1995 (III. Otras Disposiciones), pp. 36833-36836 (RJ 1995/10064)].
2) Once the judge or the party has asked the Government to declassify the information, if the Government refuses to do so, the interested party at the proceedings can appeal the Government's decision to the Supreme Court and it will review this decision and decide whether the information has to be incorporated to the case and made public or must be kept secret [Judgments of 4th of April 1997 (appeal cases num. 726/1996; 602/1996 and 634/1996), known as the cases of the CESID documents -the CESID was the old Spanish Intelligence Service-].
3) Once the Supreme Court has decided, the proceedings in front of the Court a quo will continue with or without those evidences, depending whether the Supreme Court "has decided" to declassify the information or not. [The Madrid's Court -Decision 61/2010, of 11th February- judging a case of treason of a National Intelligence Agent that sought and got classified information and took it outside the National Intelligence Service with the intention to favour another State -Russia- by revealing the information to it, did not take into consideration a piece of information that had not been declassified by the Government nor shared with the accusation and the defence]

The Supreme Court considers the act of classification as an act pertaining to those of political nature linked with the policy direction power of the Government because it is related to the highest and most sensitive spheres of power, as it is linked with the survival of the constitutional order, defined as a complex of political and legal values

that have to be protected against those who want to attack them by violent means and through attacks to the external and internal security. It considers that it has the power to declare whether the documents that were asked to be declassified affect national security or not.
The Supreme Court argues that it can carry out a review on the merits, although limited. The Supreme Court says that its function in these cases is not only to determine the political nature of the act, but that it can control the merits of the act when the law has defined through attainable concepts to the judges the limits or previous requirements to which these acts of political direction are subject. In that case, says the Court, articles 9.1 and 24 of the Spanish Constitution (article 9.1 provides that all citizens and political powers are subject to the Constitution and the legal system and article 24 regulating the right to a fair trial) oblige the Court to accept the exam of the possible abuses or failures to comply with the law in which the Government could have incurred when taking the decision to classify the information. The key element is the definition of the requirements of the act by attainable concepts, even if these concepts are those known as undetermined juridical concepts. The question, says the Court, is to reduce the immunities of power (see also Judgment of the Supreme Court of 28th June 1994, sec. 1). The concept seen as attainable is national security. Even if the Supreme Court determines that the documents belong to those affecting national security, it has asserted that it can decide also if there are elements that either suppress the affection to national security of the documents or reduce it –balancing the interests at stake– giving preference to the due process clause and the rights invoked by the appellants (article 24 of the Spanish Constitution, right to the evidence relevant to the case). So the Supreme Court applies a balancing test to the case, understanding that national security is an undetermined concept that can be analyzed and balance with other rights and interests. Our Supreme Court considers itself legitimized to control the documents in camera, without the presence of the parts of the process a quo, even when there is no similar procedure regulated in our legal system.
The Court analyzes document by document and decides when national security has to give way to the right to the relevant evidence, because of the special importance of that evidence in the case.

h. Can a judge dismiss a case, without reviewing the case on its merits, because reviewing the case would involve state secrets? *[Principle 29a]*

Please check one: ☐ Yes ☒ No Cite: Judgments of the Supreme Court of 4th of April 1997.

8. Autonomous Oversight Bodies

a. Is there an autonomous oversight body with authority to review classification decisions by security sector, defence, and intelligence agencies? *[Principle 34a]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. Identify the body. What are its mandates and powers? *[Principle 34a, 35]*

Parliament

Article 10 section 2 of the Official Secrets Act determines that Parliament will have access to classified information in the way established by the Parliament Standing Orders and in secret sessions.

Article 109 of the Spanish Constitution gives Parliament Committees, in general, a right to request, through their respective Speaker, any kind of information and help they may need from the Government and Government Departments and from any authorities of the State. This right is not given to the individual MPs. Congress has been the only one to rule on access to secret information (there is no Senate regulation).

Article 44 of the Standing Orders of Congress reads as follow: Congress Committees may request, through the Speaker i) Such information and documentation as they may require from the Government and administrative bodies, subject to the provisions of Section 7, paragraph 2; ii) The attendance of members of the Government to report on matters relating to their respective Department; iii) The attendance of authorities and civil servants competent by reason of the subject-matter of the debate in order that they report to the committee; iv) The attendance of persons competent in the subject-matter for the purposes of reporting to and advising the committee. The Standing Orders do not say anything about access to classified information by Congress Committees. This omission was solved by the President of the House through a Resolution, Resolution of 18th December 1986 on access by Congress to Classified Information [Resolución de la Presidencia sobre acceso por el Congreso de los Diputados a materias clasificadas, de 18 de diciembre de 1986 (Parliament Official Journal: B.O.C.G., serie E, de 19 de diciembre de 1986, núm.14)]. This Resolution was amended by another President of Congress Resolution of 2nd June 1992 [Resolución de la Presidencia del Congreso de los Diputados sobre acceso por el Congreso de los Diputados a secretos oficiales, de 2 de junio de 1992 (Parliament Official Journal: B.O.C.G., serie E, de 3 de junio de 1992, núm. 208)] and by President of Congress Resolution of 11th May 2004 [Resolución de la Presidencia del Congreso de los Diputados sobre acceso por el Congreso de los Diputados a secretos oficiales (Parliament Official Journal: B.O.C.G. Congreso de los Diputados, Serie D, número 14, of 12th May of 2004)].

According to section 2 of the 2004 Resolution, Congress Committees and one or more political groups amounting to at least one-quarter of the Members of the House (the House has 350 members) can request to be informed about classified information via the House President.

Sections 3 and 4 of the Congress Resolution on access to classified information reads as follow:

Section 3: When the information were classified as Secret, the Government will share the information with on MP for every political group of the House. The MPs will be elected to this end by the House by a majority of three-fifth (they form what is known as the Official Secrets Committee).

Section 4: When the information were classified as Confidential, the Government will share the information with the Chairmen of the

political groups or their representatives at the former Committee when the request had come from it.
The Government, exceptionally, and justifying it, could ask the House's Bureau to share information about a matter declared secret with the President of Congress alone, or with the President of the Committee alone if the request came from the Committee. The Bureau would then have to decide on this question (section 5).
Likewise, the Government, exceptionally, and justifying it, could ask the House's Bureau to share the information, in secret session, with the Committee that requested it, or with any Committee with powers in the subject if the information was requested by the Parliamentary Groups. In these cases only the members of the Committee will be allowed to take part in the session (section 6).
If the recipients of the information understand that the information would be incomplete without the direct knowledge of the document, the authority that provides the information will show the MPs allowed to access to the information the original or a copy of the documents (section 7). Those MPs can examine the documents in the presence of the authority that provides the information and take notes but cannot get copies or reproduce them. The MPs will examine the document in the House, unless the House President thinks that to improve access to the particular information it would be better to see the document or documents in the place where they are held (see, to this regard, articles 7 and 8 of the 2004 Resolution) (section 8).

The National Intelligence Centre's use of its Budget and its use of secret funds is also oversight by Parliament. The Secret Funds Act of 11th May 1995 (Act 11/1995) says that this oversight will be carried out by the President of the Congress and the Congressmen that have access to official secrets in accordance with the rules of the House (art.7 section 1 of the Secret Funds Act). The Rules of The House that regulate this as we have already seen are the ones established by President of Congress Resolution on access to official secrets of 11th of May of 2004. This Congress Committee may make an annual report and send it to the Prime Minister and the President of the Exchequer Court, but it is not compulsory (article 7 section 3 of the Secret Funds Act).
Secret funds can be used only to certain aims (art. 1). The money must be used only to cover expenses necessary to protect national security (art. 1, 11/1995 Act). The Secret Funds Act determines who has the power to authorize expenditures of these funds (the Ministers of Defense, Internal Affairs, Foreign Affairs and Justice) and the special means by which these expenditures have to be justified by the National Intelligence Centre. The Parliamentary Oversight Committee must send a report to Congress whenever the Ministers ask for an increase in the amount of secret funds. The Departments that handle secret funds must report to the Committee on the use given to the money every six months (arts. 2 and 7 section 2 of the Secret Funds Act) and on the internal rules that these Departments approve in order to make sure that the credits are handled by the authorities of their Department in accordance with the legal ends established by the 1995

Act (art. 6 Secret Funds Act).

On the other hand, the National Intelligence Centre Act of 2002 [Law 11/2002 of 6th May, reguladora del Centro Nacional de Inteligencia, Official Journal -BOE- number 109, of 7th of May of 2002, pages 16440 to 16444] provided for the first time that a Parliamentary Committee would control the National Intelligence Centre (CNI) activities, not only the use of the budget, but also every aspect of the activities of the Intelligence Agency (art.11 section 1 of the National Intelligence Centre Act 2002). Congress President chairs the Committee and the other members of the Committee are those MPs with access to classified information (following Congress Resolution of 2004, one MP for every political group of the House elected by a three-fifth majority). The Government is obliged by law to send information to the Committee about the aims of intelligence fixed annually. The Committee will also receive the report that annually drafts the Director of the CNI evaluating the activities of the Centre and the degree of accomplishment of the aims fixed by the Government (article 11 section 2 of the CNI Act). Of course, the sessions of the Committee are secret (article 11 section 1 CNI Act).

The Ombudsman
The Spanish Ombudsman is appointed by Parliament and his task is to protect the fundamental rights of Spanish citizens. To accomplish its task, the Ombudsman has the power to supervise any activity of the Spanish Administration, including that of the Intelligence Service [article 54 of the Spanish Constitution and articles. 1, 2 and 9 of the Ombudsman Act of 6 April 1981 (Act 3/1981, amended by Organic Law 2/1992 of 5th March)]. Article 22 of the Ombudsman Act provides that the Ombudsman can request public authorities to send him any document that he considers necessary for the development of its tasks, even those classified according to the Official Secrets Act. The Ombudsman will establish mechanism to protect the secret documents.

ii. What, if any, limitations are there on this body's ability to review classified information? *[Principle 7, 34b, 34c, 35]*

Parliament Oversight:
Article 16 of the Rules of the House will be of application to the MPs with access to classified information (Section 9 of President of Congress Resolution of 11th of May of 2004 on access by Congress to classified information) . Article 16 reads that Members of Congress shall conform in their conduct to the Standing Orders and observe parliamentary order, courtesy and discipline, as well as refrain from disclosing any proceedings which, as provided herein, may in exceptional circumstances be of a secret nature.
The sanction for breaching this obligation is disciplinary. A Member may be deprived, by resolution of the Bureau, of some or all of the rights granted to him under Sections 6 to 9 of these Standing Orders if he/she fails to keep the duty of secrecy established in Section 16 hereof (Article 99.1 Standing Orders of Congress). The penalty may

also extend to a proportional part of the allowance contemplated in Section 28 hereof (Article 99, sec. 2 Standing Orders of Congress). Articles 6 to 9 include the right to vote, the right to sit at least in one committee, to request information or to be paid a financial allowance . If the cause behind the penalty may, in the opinion of the Bureau, constitute a criminal offence, the Speaker shall convey the incriminating facts to the judicial authority having jurisdiction (Article 101.3 Standing Orders of Congress).
Also article 7 section 3 of the Secret Funds Act states that Members of the Committee that oversees secret funds can not reveal what they learn inside the Committee. Article 16th of the Standing Orders of Congress will apply to them as well.
The other problem is if the revelation by the MP of information that he or she has received in secret session is a criminal offence (as they are obliged to keep secret about the information received -article 16 of the House Standing Orders-).
Articles 598 to 603 of the Spanish Criminal Code dealing with crimes related with classified information seem to apply to MPs that have access to official secrets. Article 598 provides that he who seeks and obtains, reveals, falsifies or renders useless information classified as secret or confidential, related to national security, will be sanction with one to four years imprisonment. When the person has got the information because of his or her position, the sanction will be applied in its superior half (article 599). But we could argue that the application of this article to MPs would depend on the information revealed by them. The Supreme Court in its Decision 1074/2004, of 18th October (confirmed by the Constitutional Court in its judgment 126/2011, of 18th of July) and in its Resolution num. 921/2006 of 26th of September (see comments) said that the activities that clearly exceed the aims to which the declaration of secrecy was made and cover criminal offences cannot automatically be covered by secrecy and by the effects that the law recognizes to classified information. What if the classified information revealed by an MP did not cover a criminal offence but did not affect national security (which is the condition that the Official Secrets Act requires to classify information in article 2)? The Courts have not said anything on this but probably it would not be considered to be a crime of revealation of classified information if we followed what the Supreme Court said in the Judgments mentioned in the comments (at the end of the document).

On other issue, the National Intelligence Act provides that the Committee that oversights the Centre will not have access to any classified information coming from a foreign secret service (art. 11 section 2 CNI Act). This is an important exception in a global world like ours in which the intelligence services are more and more connected. The CNI Act also excludes access by the Committee from the information relating the methods and sources of the intelligence service. Under our Constitution, citizens are the source of legitimacy of all powers (art. 1.2 of the Spanish Constitution) and the MPs are their representatives. They must know what the executive does and judge by themselves whether these activities merit the secrecy with

which there are surrounded. Why must we trust our security services and Government and not our MPs in respect to their ability to keep secret the sources and methods of the CNI and the information coming from other foreign intelligence agencies?

The Ombudsman oversight
The Government can decide thorugh a written agreement that the secret documents must not be sent to the Ombudsman. When the Ombudsman thinks that this fact can affect seriously the development of his investigations, he will notify the Congress-Senate Committee of relations with the Ombudsman, so then, Parliament can act.
Article 26 of the Decree on the Organization and functioning of the Ombudsman, approved by the Congress and the Senate (Official Journal -BOE- number 92, of 18th April of 1983) provides that only the Ombudsman and his deputy will have access to official secrets. No reference will be made in the Ombudsman annual report to the content of the secret documents neither in the answer to the person who had complaint to the Ombudsman or request its action. The Ombudsman will consider whether to give information about the classified documents to Congress and Senate or not.

In general, I think the Spanish Legislation does not provide the oversight bodies with enough "technological and human resources to enable them to indentify, access and analyse information that is relevant to the effective performance of their functions, including information of highly technical character" as only some MPs or the Ombudsman and his deputy have access to all the secret information but they cannot be accompanied by any advisor or technical expert on secret information when they analyse the information.
In this regard, for example, Congress has elected the spokesmen of every political group of the House to be part of the committee that controls the National Intelligence Centre. On the one hand, this is good, as it reflects that Parliament gives the utmost importance to this matter, but on the other hand, these MPs are involved in everyday business of Parliament and have not much time to focus on the CNI.

b. Can the public make requests for access to information held by the autonomous oversight body? *[Principle 36a]*

Please check one: ☐ Yes ☒ No

9. <u>Whistleblower Protections</u>

a. May public personnel who have authorized access to classified national security information be subject to criminal penalties if they disclose that information to the public? *[Principle 46]*

Please check one: ☒ Yes ☐ No <u>Cite</u>:

Articles 584, 598, 599, 601 and 602 of the Spanish Criminal Code (Organic Law 10/1995 of 23th of November) and articles 50, 52, 53, 54 and 56 of the Code of Military Justice (Organic Law 13/1985 of

9th of December).

If you checked "Yes":

i. What is the maximum penalty for this crime?

4 years if there was no purpose to favour a foreign country with the disclosure (10 years for members of the armed forces), 12 years if the aim of the disclosure was to favour a foreign country (25 years for members of the armed forces).

ii. What must the government prove in order to obtain a conviction?

That the information was classified and the disclosure threatens or harms national security or national defence. See comments at the end about question 7 were we explain how in some judicial decisions the courts have ruled that a testimony given to a court about criminal activities by the intelligence services could not be considered to amount to a revelation of classified information and national security would not be affected by those testimonies. The same applies to the following question -9.a.iii-.

iii. Does the law take the public's interest in the disclosure of the information into consideration when deciding whether to penalize the disclosure? *[Principle 46b]*

Please check one: ☐ Yes ☒ No

If you checked "Yes":

1) Who bears the burden of proof in regard to whether the disclosure was in the public interest?

2) What factors must be present to meet this burden?

iv. Is a showing of either actual or probable harm to national security, resulting from the disclosure, required in order for a penalty to be imposed? *[Principle 46c]*

Please check one: ☐ Yes, actual ☒ Yes, probable ☐ No, neither

If you checked "No", is it a defence or mitigating circumstance that the disclosure did not harm national security?

Please check one: ☐ Yes ☐ No

v. Is it a defence or mitigating circumstance that the personnel making the disclosure had used, or tried to use, internal reporting procedures before making a disclosure to the public? *[Principle 46c]*

Please check one: ☐ Yes ☒ No

If you checked "Yes", what constitutes adequate exhaustion of the internal procedures?

vi. Is it a defence or mitigating circumstance that the personnel had a good faith belief that using the internal reporting procedure would be ineffectual, or would result in retaliation?

Please check one: ☐ Yes ☒ No

vii. Are there other defences or mitigating circumstances?

b. Have any public personnel been charged with a crime for disclosing classified national security information in the past two decades? *[Principle 46]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. Approximately how many prosecutions have there been?

None for disclosing classified information, even if in one case, that of Colonel Perote, he took away documents from the National Intelligence Centre and the documents were afterwards published by the press, but he was condemned for the taking away of the documents from the Centre; he was convicted to seven years imprisonment (Militar Central Court Decision of 9th of July of 1997, Supreme Court Decision 15/1998 of 30th of March of 1998). There was another prosecution of an agent of the National Intelligence Centre who took away classified information from the National Intelligence Centre to sell it to the Russians, but he finally did not disclose the information. He was condemned to nine years imprisonment (Supreme Court Decision 1094/2010 of 10th of December of 2010, Criminal Section).

ii. Approximately how many convictions have there been, and what punishments were imposed, if any?

If you checked "No", have any personnel been investigated or otherwise threatened with government sanction as a result of disclosing classified national security information in the past two decades?

Please check one: ☐ Yes ☐ No

If you checked "Yes", please explain what happened:

c. Do laws protect "whistleblowers" who disclose certain categories of classified information pertaining to government wrongdoing?

Please check one: ☐ Yes ☒ No Cite:

In Spain there are no internal reporting procedures established by law, neither is there any legal clause protecting the disclosure of certain categories of classified information

If you checked "Yes":

i. What categories of information are covered by the whistleblower protection laws? *[Principle 39]*

Do the protected categories vary depending on whether the information is disclosed publicly, internally, or to a designated independent body?

Please check one: ☐ Yes ☐ No

If you checked "Yes", please identify the type of disclosure that is protected for each listed category.

ii. Do these whistleblower protections apply to whistleblowers in the security sector, defence, and intelligence agencies?

Please check one: ☐ Yes ☐ No

iii. How do the protections afforded to whistleblowers in the security sector, defence, or intelligence agencies differ from whistleblowers in other government sectors, if at all?

d. Are public personnel prosecutable if they disclose classified national security information, in making a complaint *internally*, to someone within their own ministry, department, or unit, even if not a direct supervisor? *[Principle 39-41]*

Please check one: ☒ Yes ☐ No

e. Is there an *independent* body, expressly designated to receive complaints involving classified information from public personnel? *[Principle 42]*

Please check one: ☐ Yes ☒ No

If you checked "Yes":

i. Are public personnel prosecutable if they disclose classified national security information to the designated independent body? *[Principle 34d]*

ii. Must such personnel complain internally before approaching the independent body?

f. Are public personnel encouraged to make internal disclosures when they encounter information about government wrongdoing?

Please check one: ☐ Yes ☒ No

If you checked "Yes":

i. How are internal disclosures encouraged? *[Principle 47]*

ii. Do public personnel have a duty to disclose information of governmental wrongdoing to an internal or designated independent body? *[Principle 39]*

iii. What criminal, civil, and/or administrative penalties, if any, are there for retaliation (*e.g.*, firing, demotion, harassment) against personnel who provide information concerning governmental wrongdoing to an internal or designated independent body? *[Principle 44]*

g. Are there criminal penalties for the unauthorized *possession* of classified information by a person who had authorized access to that information? *[Principle 50a]*

Please check one: ☒ Yes ☐ No

If you checked "Yes", do whistleblower protections apply to unauthorized possession of information?

Please check one: ☐ Yes ☒ No

10. Media Protections

a. May a person who does *not* have authorized access to classified national security information (such as a journalist) be subject to criminal penalties for disclosing this information to the public? *[Principle 50b]*

Please check one: ☒ Yes ☐ No Cite: Articles 598 and 600 section 2 of the Criminal Code (the latter in relation with article 9 Official Secrets Act).

If you checked "Yes":

i. What is the maximum penalty for this crime?

The maximum penalty for this crime is four years imprisonment if it was the journalist who directly sought and got the classified information.

ii. What must the government prove in order to obtain a conviction?

That the information was classified and the activity carried out by the journalist threatens or harms national security or national defence.

In the case of article 598 of the Criminal Code the government must prove that it was the journalist who sought the information and got it without the intervention of a third person who gave him the information. In the case of article 600 section 2 of the Criminal Code the government will have to prove that the journalist by chance obtained the classified information (someone else gave him the information or he got it by chance) and knowing that it was classified (that is important) he did not return it to the empowered authority, as article 9 of the Official Secrets Act oblige to do (obviously, without disclosing it).

iii. Does the law take the public's interest in the disclosure of information into consideration in deciding whether to impose a penalty?

Please check one: ☐ Yes ☒ No

i. Who bears the burden of proof in regard to whether the information that was disclosed was in the public interest?

ii. What factors must be present to meet this burden?

iv. Is a showing of actual or probable harm to the national security, resulting from the disclosure, required in order for a penalty to be imposed?

Please check one: ☐ Yes, actual ☒ Yes, probable ☐ No, neither

If you checked "No", is it a defence or mitigating circumstance that the disclosure did not harm national security?

Please check one: ☐ Yes ☐ No

v. What other defences are available?

See comments at the end about question 7 were we explain how in some judicial decisions the courts have ruled that a testimony given to a court about criminal activities by the intelligence services could not be considered to amount to a revelation of classified information and national security would not be affected by those testimonies. Analogously, we consider that the journalist could argue that he was revealing criminal activities and that would not meet the conditions to be punished for a crime of disclosure of classified information.

b. Have any members of the media (journalists, editors, publishers, etc.) been charged with a crime for publishing government secrets in the past two decades? *[Principle 50b]*

Please check one: ☐ Yes ☒ No

If you checked "Yes":

i. Approximately how many times have charges been brought?

ii. Approximately how many convictions have there been, and what punishments were imposed, if any?

If you checked "No", have any member of the media been investigated or otherwise threatened with government sanction as a result of publishing government secrets in the past two decades?

Please check one: ☐ Yes ☒ No

If you checked "Yes", please explain what happened:

c. Are there criminal penalties for the *possession* of classified information by a person who did not have authorized access to that information (such as a journalist)? *[Principle 50a]*

Please check one: ☒ Yes ☐ No Cite: article 600 of the Spanish Criminal Code

If you checked "Yes":

i. What is the maximum penalty for this crime?

Three years

ii. What must the government prove in order to obtain a conviction?

That the information was classified and the activity carried out by the journalist threatens or harms national security or national defence. The government will also have to prove that the journalist by chance obtained the classified information (someone else gave him the information or he got it by chance) and knowing that it was classified (that is important) he did not return it to the empowered authority, as article 9 of the Official Secrets Act oblige to do (whether there is disclosure of the information or not is not relevant to the commission of the crime).

iii. What are the defences?

That any information about criminal activities cannot be considered to be classified and damage national security. Analogously to what we explained in the comments to question 7.

d. May the government compel a member of the media to reveal a confidential source in the interests of national security? *[Principle 51]*

Please check one: ☐ Yes ☒ No

e. May the government prevent the media from publishing information on the basis of national security? *[Principle 52]*

Please check one: ☐ Yes ☒ No

If you checked "Yes":

i. What information must the government provide to justify a prior restraint on publication?

ii. To whom must this information be provided?

f. May the government prevent or sanction the dissemination of information even after that information has entered the public domain (*e.g.*, having been published on the Wikileaks website)?

Please check one: ☒ Yes ☐ No

If you checked "Yes", please explain what is required for the government to prevent or sanction dissemination of this information:

The Government cannot prevent further publication of the information as there is a prohibition of prior restraint (article 20 section 2 of the Spanish Constitution). The Supreme Court said that even if a classified information has been published by the press it still does not lose its classified character (Supreme Court Decisions of 4th of April of 1997). So the Government should prove that its dissemination can still pose a threat or harm national security or national defence.

11. Record Maintenance

a. Is there a duty to archive classified documents? *[Principle 17]*

Please check one: ☒ Yes ☐ No

If you checked "Yes", does the duty to archive classified documents apply to the security sector, defence, and intelligence agencies?

Please check one: ☒ Yes ☐ No

b. Under what circumstances is classified information permitted to be destroyed? *[Principle 49]*

In relation to documents, article 55 section 1 of the Historic Heritage Law provides that the destruction of any document generated, preserved or gathered by a public institutions or organs, by legal persons in which the state or other public entities have a majority participation in their capital or by private persons that manage public services in performing those public tasks (and that includes classified documents) must be authorized by the competent authority. Article 55 section 2 provides that the documents cannot be destroyed when they still have evidential value related to rights or obligations affecting public persons or entities. Article 55 section 3 provides that in the rest of the cases the destruction must be proposed by the possessor of the document and will have to be authorized by the competent authority, in the way established by the regulations detailing the procedure. Article 28 of the Decree 242/1969 developing the Official Secrets Act

provides that whenever the authority in charge of the classification of the information considers the classified material (information) to be useless he/she will order all the entities possessing the material or copies or reproductions of it to destroy them. In ordinary circumstances, nobody will be allowed to destroy classified information without the permission of that authority.
Article 10 section 1 of the Norm NS/04 of the Delegated Authority for the Security of the Classified Information even relax this requirements. and provides that in order to avoid the accumulation of classified information that information considered useless by its users will be destroyed, and there will be no need to get the authorization of the international organism, organism, ministerial department or person that generated the information saved it is so expressly required, and that will normally be required only when the information is classified as top secret or equivalent.

i. May classified information ever be destroyed before becoming declassified?

Please check one: ☒ Yes ☐ No

ii. What oversight is involved in the decision to destroy classified information?

There is no oversight outside that exercised by the Executive (the Ministerial Departments) or the Armed Forces. There are control organs that supervise the destruction of the information depending on the degree of the classification of the information (Norm NS/04 of the Delegated Authority for the Security of the Classified Information). Top Secret Information destruction is done under the oversight of the Central Registry or Central Service of Protection of Classified Information existing in the Ministerial Departments and armed forces. Secret information can be destroyed under the supervision of the "main and secondary subregistries or general protection services" (Norm NS/04 of the Delegated Authority for the Security of the Classified Information). The Government is the only one with power to classify this information so according to article 55 of the Historic Heritage Law the destruction should be authorised by the Government. The control organs under which the destruction is done must fill in a file with data about the destruction and the fact of the destruction will be record in the registry (see the form that must be filled in when destroying classified information in http://www.cni.es/comun/recursos/descargas/NS-04_Seguridad_de_la_Informacion.pdf,Annex VIII to norm NS/04 of the Delegated Authority to the Security of Classified Information, page 77 of the document.

iii. Are there certain categories of information that are not permitted to be destroyed (*e.g.*, information pertaining to human rights violations or corruption)?

Please check one: ☒ Yes ☐ No

If you checked "Yes", please indicate which categories of information are not permitted to be destroyed:

Article 55 section 2 of the Law of Historic Heritage provides that the documents (it affects only documents) cannot be destroyed when they have evidential value related to rights or obligations of public persons or entities (The problem is if there are mechanisms of oversight that this is so).

c. Is each public authority that classifies information required to maintain a list of classified documents that it holds? *[Principle 16]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. What information must be included in this list?

Organ of origin of the document, date and classification degree. If the information is displaced and its destruction if it is destroy (article 25 of the Decree 242/1969 that develops the Official Secrets Act).

ii. What information from this list, if any, must be made available to the public?

None.

Sources: To the extent not already provided, please cite the key laws and regulations that provide the legal framework for allowing, and controlling, public access to information, including national security information. If you are aware of any useful secondary materials, please cite these resources as well. Please also note any significant case law or examples, exemplifying or contradicting the draft Principles.

See main text and comments.

Additional comments? (optional)

Spain unbelievable still does not have a Freedom of Information Act. Article 105 b) of the Spanish Constitution of 1978 gives citizens the right to access to administrative archives and registries except when this could affect national security and national defence. It is a restrictive clasuse as far as it is only refering to access to information contained in archives and registries and does not refer to all, but only to the administrative ones. This right is regulated in article 37 and 38 of the Law regulating the fuctioning of the Public Administration (Ley 30/1992, of 26th November, de Régimen Jurídico de las Administraciones Públicas y el Procedimiento Administrativo Común).
Law 27/2006 of 18th of July, regulating the Right of Access, Public Participation and Access to Jurisdiction in Environmental Matters (that incorporates Directives 2003/4/CE and 2003/35/CE) recognize citizens a rigth of access to environmental information that can be requested to any public authority holding the information (article 10 of the Law 27/2006 of 18th of July).
On the other hand, there is the Official Secrets Act of 1968, reformed in 1978. It establishes in articles 2 and 4 that the Government and the Committee of the Chiefs of Staff of the Armed Forces within their area of competence may classify those acts,

issues, documents, data or objects the knowledge of which could cause harm or threaten (put at risk) national security or national defence. As the Committee of the Chiefs of Staff has only consultative powers and article 97 of the Spanish Constitution (posterior to the Official Secrets Act) gives the Government the power of direction of the internal and external policy, the civil and militar administration and the national defence, I understand that the Committee of the Chiefs of Staff cannot really exercise any power to classify information, and in fact so has been the case so far as far as I am aware. Article 1.2 of the Official Secrets Act says that a law can also classify information as secret.

Comments to A National Security Exception to the Right to Information:
Question 1.c: In Spain the citizens' right to access to information is limited to access to that information collected in administrative archives and registries or to environmental information, so that no public authority is excluded from the obligation of disclosure if the informations forms part of those archives or registries or to environmental information. Otherwise there is no disclosure duty.
Question 1 d: The answer to question 1d is "no" because in general it is so, there are only a few laws that contemplate the affirmative obligation to publish information (and none are laws regulating a general right of access to any kind of information). This is the case, for example, of article 126 of the Public Sector Law of Contracts (Law 30/2007, of 30th October) that requires public authorities to publish the offers of contracts to be done with the public sector and the conditions of the offer; the case of article 18 of the Grants Act (Law 38/2003, of 17th November), that obliges the administrative organs to publish the results of the grants awarded and its characteristics, or the case of articles 6 to 9 of the Law 27/2006 of 18th of July, regulating the rights of access, public participation and access to jurisdiction in environmental matters (that incorporates Directives 2003/4/CE and 2003/35/CE).

Comments to question 2.a (requirements for denying request for information): One must remember that citizens can only request access to documents that form part of an administrative archive and registry except in the case of access to environmental information that can be requested to any public authority holding the information (article 10 of the Law 27/2006 of 18th of July).

Comments to section 3.- Classification Procedures:
We have answered section 3 of the questionnaire exclusively taking into account the law (the Official Secrets Act), but there has been a parallel developing of rules regulating classification of information that are not contained in the law and that therefore are not known by the majority of the public. They introduce important nuances to what we have said. The question here is the legitimacy of this regulation creating new categories of classified information outside the scope of the law (although the National Security Delegated Authority considers it a derivation of the Official Secrets Act, but I would not consider it that way).
The Ministerial Order 76/2006, of 19th of May approving the policy for the security of information of the Defence Ministry (Official Journal of Defence.- Boletín Oficial de Defensa (BOD) núm. 103, of 29th May 2006, page 5856) in its article 6 (dealing with "clasification of information") considers as "the subject matter of internal secret" the acts, issues, documents, data or objects the knowledge of which could affect the security of the Ministry of Defence, threaten its interests or hinder the accomplishment of its mission. These informations will be classified as "confidencial" (confidential) or as "difusión limitada" (restrited) .

[http://www.defensa.gob.es/Galerias/docs/politica/infraestructura/sistemas-cis/DGN-CIS-Orden-Ministerial-76-2006-Politica-Seguridad-de-Informacion.pdf]
The use of these two categories of classified information not contemplated by the Official Secrets Act has been extended to all Ministerial Departments as we will see.
In 1982, the incorporation of Spain to the NATO required the creation of a National Security Authority to control and protect classified information. By Government agreement of 25 June 1982 the Goverrnment created the National Security Authority. The Minister of Defence and the Minister of Foreign Affairs were designated together as National Security Authority (see http://www.cni.es/es/queescni/ans/). The Agreement allowed them to appoint a National Security Delegated Authority (ANS-D). The Order of the Ministry of Presidency of 31th July 2009 appointed as National Security Delegated Authority the Secretary of State-Director of the National Intelligence Centre -the Spanish Intelligence Services- (Orden PRE/2130/2009, de 31 de julio, por la que se designa la Autoridad Delegada para la Seguridad de la Información Clasificada originada por las partes del Tratado del Atlántico Norte, por la Unión Europea y por la Unión Europea Occidental, publish in the Spanish Official Journal the 5th of August of 2009.- BOE núm. 188, sec. III, page 66915). A so called norm -rule-coming from the National Security Delegated Authority (Norm NS/04, Security of the Information), in accordance, says the regulation, with the Security Policies of International Organizations and Agreements for the Protection of Classified Information and to some Ministerial Departments, states that these two other categories of classified information not envisaged by the Official Secrets Act - "confidencial" equivalent to confidential, and "difusión limitada" equivalent to restricted- can be used by any other Ministries. In fact, according to section 3.1.3.2 the Ministers of the different Departments of Government, the Secretaries of State of each Department, the Subsecretaries of State, in their respective Department, as well as the Chief of the Defence Staff, Chief of the Army Staff, Chief of the Navy Staff and Chief of the Air Forces Staff can classify information in these two categories, and the authority to classify information in those two categories may be delegated.

Comments to question 3.e: Curiously, while the law does not really define the different classification levels, the National Security Delegated Authority (the Director of the National Intelligence Centre), without any cover from the law, has done so in his norm NS/04 (Annex I). He distinguishes between classified matters and matters of internal restriction.
Classified Matters.
He declares that the information will be classified as:
TOP SECRET ("secreto") when it needs the upmost level of protection because its non-authorized disclosure or incorrect use could cause a extremely serious threat or harm to the Spanish interests in the following spheres:
a) The sovereignty or national integrity;
b) The Constitutional order and the national security;
c) The public order and the life of citizens;
d) The combat capability or the security of the Spanish Armed Forces or their allies;
e) The effectivity or security of special valuable operations of the Spanish Intelligence Services or their allies;
f) The Spanish International Relations or International tension situations or
g) any other information which needs the highest protection to be safeguarded
SECRET ("reservado") when the information needs a high degree of protection because its unauthorized disclosure or incorrect use can cause a serious threat or harm to the Spanish interests in the following spheres:

a) The Constitutional order and national security
b) the public order and the security of the citizens
c) the combat capabilities or the security of the Spanish Armed Forces or their allies
d) The effectivity or the security of operations of the Spanish Intelligence Services or their allies.
e) The Spanish diplomatic relations or international tension situations;
f) The economic or industrial interest of strategic character, or
g) Any other that requires a high degree of protection to be safeguarded.
Matters of Internal Restriction.
He declares that the information will be classified as:
CONFIDENTIAL ("confidencial") when the disclosure of the information or its incorrect use may cause a threat or harm for the Spanish interests in the following spheres:
a) The effective development of the country policies or the functioning of the public sector;
b) Spanish political or commercial negotiations versus other states;
c) The economic or industrial interests;
d) The operation of the public services;
e) When it will hinder the investigation of a crime or facilitate its commition;
f) any other that can cause a threat or harm to the interests of Spain.
He declares that the information will be declare RESTRICTED ("de difusión limitada") when the non-authorised disclosure or incorrect use may be contrary to the Spanish interests in any of the fields mentioned in the previous sections.

Comments to question 3 h: The duty to state the reasons to classify is really only a duty to specify the area affected by the information according to article 2 of the Official Secrets Act [Article 11 of the Decree developing the Official Secrets Act (Decree 242/1969)]. Article 2 of the Official Secrets Act states that the Government and the Committee of the Chiefs of Staff of the Armed Forces within their area of competence can classify those acts, issues, documents, data or objects the knowledge of which could cause harm or threaten (put at risk) national security or national defence.

Comments to question 3 j.ii: Article 11 section c of the Decree developing the Official Secrets Act (Decree 242/1969) states that whenever some parts of a document must bear the classification of secret but there are some other parts that can be classified in an inferior degree, those parts should be classified in that inferior degree but the whole document will have the upper grade of classification.

Declassification. Comment to questions 4 a) and 4 b): There is not an absolute obligation to specify a time date or event that triggers the declassification of the information, the law (article 3 section III of the Decree 242/1969, of 20th February) states that "whenever possible" the classifier will specify the duration of the classification mentioning if the classification could be finished or lowered the classification level to the inferior category of classification. To that end the classifier can fix a date or refer to an event or fact that will limit the duration of the classification. Law 18/1985, of 25th of June, Law of Historic Heritage (Ley del Patrimonio Histórico Español) in its chapter dedicated to the documental heritage provides that all the documents that are generated, kept or gathered by public institutions or organs, by legal persons in which the state or other public entities have a majority participation in their capital or by private persons that manage public

services when performing those public tasks can be defined as documental heritage (article 49 section 2 of the Law), and it establishes that they will be of open access save those classified (article 57 section a). While this law establishes a limit duration of 25 years from the death of the person to access to those documents that contain personal data and have a police-related, clinical or procedural character or any other character which could affect the security of persons, their honour, privacy or image (and if the death date of the person is not known, 50 years), it does not establish such a limit when it comes to classified documents; there the law does not establish any temporal limit to the prohibition to access those documents and only says that the person interested in those documents can ask the authority that made the classification of the information for an authoritation to have access to those documents (article 57 sections b and c of the law). There are no fixed periods for automatic declassification.
Comment to question 4 f): There is no specific procedure for the public to ask for the declassification of information, but there is the Petition's Right Act (Organic Law 4/2001, of 12 November) that recognizes any person the right to make a formal request to any public institution, Administration or authority, including the Government. The petitions, says the law, can have as its object any issue or matter within the scope of powers of the authority, institution or organ (article 3 of the Petititon's Right Act). Article 7 of the Official Secret Act gives the Government the power to declassify documents. That would make declassification of information a possible object of a petition by any person to the Government (as can be seen this can be only a substitute procedure in the absence of a specific procedure to ask for the declassification of classified information).

Categories of information that are classifiable:
Additional explanation to question 5.a.i: The Official Secrets Act establishes that the Government and the Legislature can classify information (articles 1 and 2 of the Official Secrets Act). The Government has to do a test of whether the disclosure of the information to a non-authorised person could (not even would) threaten or harm national security or national defence (article 2 of the Official Secrets Act). If the test is positive, the Government can classify the information, but it is not obliged to do so. The Legislature does not even have to make such test. It can directly classify any information as secret and it has done so in some occasions. So the list of categories of classified information comes from the Legislature decisions through some laws and from the Government agreements (as the Official Secrets Act itself does not contain a list of categories of classified information).
What has been done by the Government? The Spanish Government has decided to classify different categories of information (as we can see in the answer to question 5.a.i). There are different decisions taken by different governments expanding the list of categories of information exempted from the right of access to information. These decisions taken by the Government are not published in the Official Journal. We know that there was an order to classify information (a list of categories exempted from disclosure) taken on the 28th of November 1986 thanks to a question done by a congressman in Parliament that was answered by the Government (answer published in the Official Journal of Parliament on the 6th of November of 1987 -BOCG, Serie D, núm. 122, page 6243-). We know that there was another order including new categories of information exempted from the right of access to information in 1996 thanks to a report done by the Spanish Ombudsman on this issue.
http://www.defensordelpueblo.es/es/Documentacion/Publicaciones/anual/Documentos/INFORME1995informe.pdf
Finally, this year (2012) we learned about a new decision to classify categories of

documents (list of exemptions) thanks to the press (see for example, http://politica.elpais.com/politica/2012/06/03/actualidad/1338750887_077908.html). The case was the following: two researchers wanted to access to some documents kept in the General Archive of the Foreign Affairs Ministry, including access to some documents that they have already seen. The Foreign Affairs Ministry answered, first orally and then through a written reply that those documents were covered by secrecy as they could be covered by some of the categories of information exempted from disclosure because of their classification according to an agreement taken by the Government on the 15th of October of 2010. The Foreign Affairs Ministry sent the researchers a letter containing the agreement including the list of categories of classified information. These researchers told the press about the letter (containing the list of categories of information classified by the Government in 2010) and the press published the list. (http://ep00.epimg.net/descargables/2012/06/03/81b3c3748773b522e38eb34079877132.pdf). Anytime the law or the Government include a category on a list, it is an absolute exemption to the right of access to information.
Comment to question 5 b: The Official Secrets Act does not establish a prohibition of classification of any categories of information, but article 9, section 1 of the Spanish Constitution provides that all citizens and public powers are bound by the Constitution and by the legal order. That means that secret can not cover human right violations or illegalities like government corruption. On the other hand, the Spanish Constitution in article 103 determines that all organs of the Administration are created in accordance with the law, and laws must be public (there can be no secret laws). Article 9 section 3 of the Spanish Constitution provides that the norms will be public.

Does the law prohibit any categories of information from being classified (question 5 b): see please comments to question 7.

Comments to question 7.- Judicial Proceedings:

Article 120 of the Spanish Constitution says that “(1) Judicial proceedings shall be public, with the exceptions contemplated in the laws on procedure. (2) Proceedings shall be predominantly oral, especially in criminal cases. (3) Judgments shall always specify the grounds therefore, and they shall be delivered in a public hearing”.

Judicial Oversight of Classified Information:

In the case refer to in question 7 g, the so called "case of the CESID documents" Judge Garzón was the enquiring judge in a cause about the killing of some people presumably linked with the ETA. There were suspicions that the killings had been planned and executed by people integrated in public institutions of the State in charge of the fight against ETA. The judge asked the CESID (now called National Intelligence Centre) to inform him about the existence or inexistence of a group called GAL (Grupos Armados de Liberación: Liberation Armed Group) who would have been the group responsible for the killing of those supposed members of ETA. Garzón also asked for documents that would prove the participation of members of the national security forces or the own CESID in those criminal activities, and he asked also the CESID to confirm the existence of “office” notes over the activities of the GAL. The classified information consisted of some “office” notes, a document about illegal armament and a report about activities carried out by members of the

security forces in the fight against terrorism in the south of France.
The Director of the CESID answered that he could not comply with the requirement of the judge because the information was covered by secrecy according to the Official Secrets Act of 1968. After the Government, by Agreement of the Council of Ministers of 2nd August 1996, denied the declassification of the documents, the prosecution appealed to the Supreme Court against the Government decision. The Supreme Court decided that national security has to do with the notion of permanence of the constitutional order, and so that allowed the court to state that the documents that were asked to be declassified by the accusation at the trial affected national security and could be secret, as part of a set of studies, measures, information, decisions and actions directed to fight terrorism, because terrorism wants to alter the constitutional order, using as one of its methods violence against life and physical integrity and ignoring the ways to reform the constitution included in Title X of the Constitution. But then the court added that it will review the concurrence of elements that either suppressed the affection to national security of the documents or reduced it – balancing the interests at stake– giving preference to the due process clause and the rights invoked by the appellants (article 24 of the Spanish Constitution, right to the evidence relevant to the case). It reviewed the documents in camera, without the presence of the parts of the process a quo, and analyzed document by document when national security had to give way to the right to the relevant evidence, because of the special importance of that evidence to the case. The Court turned to the allegations of the parts and the facts of the process to determine the elements to be taken into account.

- The first element put in the scales was that the case in which the information would be used as evidence was a criminal case in which the judge tries to discover the truth about crimes that attacked rights and interests of a maximum value, like the life of the people.
- The second was that according to articles 303 and 311 of the Code of Criminal Procedure, the decision about the adequacy and the importance of the evidence to the procedure belongs to the Judge preparing the case, although he must justify his decision (art. 187 Code of Criminal Procedure).
- The third was that the documents that the judge wanted to incorporate to the cause were illegally taken from the CESID facilities (they were stolen by some members of the CESID and afterwards published by the press). That could have made them loose its evidential value as they could have been manipulated, but the Court maintained that the relevance as evidence must be decided by the Judge.
- Fourth element: the documents, despite their partial publication, and their removal from the facilities of the CESID were still classified and should be treated as such.
- Fifth: the Court would take into account whether the declassification of the documents would produce a serious harm to the international reputation of Spain in its external relations, and in particular as it comes to the exchange of intelligence and classified information with friends and allies. The Court analyzed if the declassification could mean a breach of any of the international obligations of Spain derived from the treaties on protection of classified information and concluded that there was no evidence that the documents in the case contained any information of this kind. On the other hand, the Court declared that its judicial review of the classification did not per se deteriorate the international reputation of Spain as it would carry out a serious and founded review.
- Sixth: the Court took into account if the information revealed the structure and the operational methods of the CESID and the integrity of those who were or are

members of the Intelligence Service, as well as that of their families and relatives in order to protect them. In this sense, for example, it took these criteria into account in relation to documents named 6.f), 11.k) and 17.p) and concluded that the criminal relevance of the said documents did not compensate the harm that could be done to these other interests if declassified and incorporated into the cause, and left them secret.
Taking into account all those elements, the Court examined document by document and decided in particular (not in abstract) the value of each document to the due process, and weighted them in relation with the harm that their declassification and incorporation to the cause could do to national security, deciding which of them would have to be declassified by the Government and incorporated into the cause followed in the Audiencia Nacional (the Court in charge of judging terrorism cases) and which wouldn't.

Now we will refer to some rulings of the Supreme Court, affirmed by the Constitutional Court, that have an important impact on the question whether there is a prohibition to classify any categories of information:

The Supreme Court departs from the idea of protecting the rule of law and article 9 of the Spanish Constitution, which establishes that citizens and public authorities are bound by the Constitution and all other legal provisions. The National Intelligence Centre Act (Ley del Centro Nacional de Inteligencia. Law 11/2002, of 6th of May) in its article 2.1 also says that the National Intelligence Centre -CNI- must act under the rule of law. Taking this into account, the Supreme Court affirms that the classification of secret information is made in broad categories by the Government. The aim of this classification is to protect national security. This, to the Supreme Court, means that the activities or information that clearly exceed the aims to which the declaration of secrecy were made, cannot automatically be covered by secrecy and the effects that the law recognizes to classified information (crimes cannot be treated as classified information). Let us see the cases that illustrate this:

Supreme Court Decision, Criminal Division, Section 1, 921/2006, of 26th of September (Auto del Tribunal Supremo, Sala de lo Penal, Sección 1ª, auto núm. 921/2006 de 26 de septiembre).

In 1995 it was discovered by the Press ("El Mundo") that the CESID (the old Intelligence Service) had monitored the communications of many different Spanish personalities, including His Majesty the King, between the years 1983 to 1991. In 1982 the CESID created the Monitoring of Communications Office. The Office was supposed to get information and record communications related with other Intelligence Services that could operate in the Spanish territory, terrorism, activities contrary to the constitutional order, counterintelligence, economy and technology, laundering of money, analysis of the communications of the CESID and analysis of interferences with the frequencies used by the CESID in its communications. The fact was that the members of the unit carried out massive interception of communications in different frequencies and they recorded multiple conversations of different persons, including that of very relevant public figures on very different issues and of very different kind. The Madrid Court (Audiencia Provincial de Madrid) convicted some members of the CESID because of these activities. They were convicted to different penalties for having committed a crime of interception of communications. One of the persons convicted appeal to the Supreme Court.

The appellant claimed there had been an infringement of his right to an effective legal remedy and the due process clause laid down in article 24 of the Spanish Constitution because the Court accepted the testimony of the Director of the CESID which was essential to the cause and which he considered to involve classified information (information classified by the Government Resolution of 1986 cited in the questionnaire). The testimony of the Director of the CESID was about the secret interception of private communications without judicial authorization and he also told the court who was the person responsible of the unit in which those interceptions were carried out. For the appellant that information was classified because it was about the activities of the Monitoring of Communications Office, its methods, the identities of the persons working there, the equipment they had and the responsible people for them. He considered that this information came under two of the categories of information classified by the Government Resolution of 1986 cited above in the questionnaire: the one classifying the structures, organization, methods and sources of the intelligence services and any other information that can reveal them, classified as Top Secret, and the one classifying the positions of the special personnel, classified as Secret.

He considered that the Madrid Court should have followed the proceedings to incorporate the "classified" evidence to the cause explained before (in the so called CESID documents case), asking the Government to declassify the information and in the case of a negative answer, appealing to the Supreme Court in order to get the declassification of the information. Not having done so meant for the appellant the nullity of all the proceedings before the Madrid Court.

The Supreme Court rejected the appeal (Supreme Court decision, Criminal Division, Section 1, 921/2006 of 26th September.- Tribunal Supremo, Sala de lo Penal, Sección 1, Auto núm. 921/2006 de 26 de septiembre).

The Supreme Court said that our legal system admits the classification of information to protect national security. The sacrifice of some rights or parcial aspects of those rights could be sometimes necessary to protect the own survival of the democratic order and the own existence of the citizens rights. But this legitimate aim cannot serve as an excuse to create impunity spheres when the use or abuse of those means goes far beyond what is constitutionally admissible and cover criminal acts. It is true that generically the information mentioned by the appellant could have been considered to come under the categories of classified information mentioned by him, and then the proceedings to ask for the declassification of the information mentioned in the CESID documents case ought to have been followed, but in this case there were some elements, said the Supreme Court, that ought to be brought into consideration. Those elements implied that the activities that clearly exceeded the reason that justified the declaration of classified information could not automatically be covered by the effects that the law gives to the declaration of classified information.

The Supreme Court departs from the idea of protecting the rule of law. Article 9 of the Spanish Constitution establishes that citizens and public authorities are bound by the Constitution and all other legal provisions and that also affects the Intelligence Services -CNI- (the National Intelligence Centre Act in its article 2.1 also says that the CNI acts under the rule of law). The importance of the activities of the CNI for the survival of the state does not prevent that. On the other hand the Constitution recognizes the right to respect for private life and specifically for private communications (article 18 section 3 of the Spanish Constitution). Apart from that, those categories of information mentioned by the appellant were classified by the Government, but the Official Secrets Act in article 2 states that the information that can be classified (under those broad categories) is only the one that can cause harm or

threaten national security or national defence. On the other hand, the regulation of the secret services in force at the moment said that the activities of the CESID were aimed at protecting the national defence and security of the state. Any activity exceeding those aims should be understood to be excluded from the generic declaration of classified information made by categories according to the Supreme Court.
The Director of the CESID -said the Court- revealed activities of his subordinates that exceeded their mandate. The subordinates used their powers to commit a crime, and this could not be considered to be classified as the classification of the information is done in general categories but no particular fact or activity is classified and in this case, the information communicated by the Director of the CESID did not affect national security or national defence. The facts were related with a category of classified information but their criminal nature and its lack of affection to national security or national defence made that they could not considered to be covered by those categories of classified information. The Supreme Court rejected the claim of the appellant to declare nulle all the previous proceedings at the Madrid Court.

Supreme Court Judgment, Criminal Division, number 1074/2004, of 18th of October

This case is related with the use of secret funds by some members of the security services. They were accused of embezzlement. They used the funds to enrich themselves as then there was no real control on the use of secret funds by the security services (now there is the Secret Funds Act of 11th May 1995 (Act 11/1995) that has introduced a better system of control of the use of these funds). One of the appellants said that there had been a breach of his rights to an effective legal remedy, to the due process clause and to his right to a defence because the information about the use of secret funds was classified in the category of top secret as concerning the structures, organization, methods, and sources of the security services and all the information that could reveal them (Government Resolution of 1986) and the information should have been declassified to be used as evidence in court, being otherwise all the proceedings carried out at the inferior court invalid (the inferior court, the Madrid Court -Audiencia Provincial de Madrid- did not ask for the declassification of the information). The Supreme Court decided that there was no violation of the rights of the accused to an effective legal remedy, to the due process clause and to the right to the defence. It said that the Official Secrets Act and the regulations and complementary agreements in this matter must be interpreted in accordance with the Constitution. Secret funds must be used for the aims established in the law.The cover of secrecy only applies in those cases. The category of top secret information mentioned by the appellant and pertaining to the Government Resolution of 1986 cannot be interpreted to cover expenses done not for the protection of national security and national defence but to commit a crime of embezzlement. It must be interpreted that the Government acts subject to the Constitution. Any criminal activity must be considered to be excluded from the protection of the declaration of classified information.
This case, as well as the previous one, was discovered by the press and there were no judicial proceedings against the press for revealing classified information. Also the CESID documents case was uncovered by the press and no judicial steps were taken against the press.

Constitutional Court Judgment (Section 2) number 126/2011, of 18th of July.

This case is related to the last one. One of the accused of embezzlement because of the misappropriation of secret funds was Rafael Vera. He was Director of National Security of the Ministry from 1982 till 1984, deputy Secretary of the Internal Affairs Ministry between 1984 and 1986 and National Security Secretary from 1986 to 1994. Rafael Vera was found guilty of embezzlement and appealed against the Supreme Court Sentence of 18th of October of 2004 mentioned above (he was condemned to seven years imprisonment and prohibited from holding public office for 18 years). He asked the Constitutional Court to declare null the Supreme Court's Judgment and the Madrid's Court Judgment. He considered that there had been a violation of his rights to an effective legal remedy and to his defence, in relation with the legality principle (articles 24 and 25 of the Spanish Constitution). He argued that any inquiry into secret funds required a previous declassification of the information because secret funds constitute classified information (now secret funds are classified directly by law, by the above mentioned Secret Funds Act). The information in this case was not declassified as we have explained before, so he considered that the evidence used to convict him was illegal and his lawyer also argued that the defendant could not defend himself because revealing classified information is a crime and because revealing data about the real use of those secret funds would have threaten the security of the state and the security of persons with authority inside the state.
The Constitutional Court said that the argument of the former National Security Secretary had to do with the interpretation of the law. His interpretation was different from that done by the Supreme Court and the Madrid Court. Those two courts understood that there was no need to ask for the declassification of the information because the use of those funds to commit a crime and, therefore, for a different purpose as the one established by the law, would not be cover by any classification. The Constitutional Court stated that the interpretation and application of the law belongs to the ordinary judges (including the Supreme Court), not to the Constitutional Court, and that there was no arbitrariness in the interpretation of the law made by those two courts, it was not an unreasonable interpretation (that's the only aspect the Constitutional Court can analyse as the Constitutional Court is the supreme interpreter of the Constitution and the Supreme Court the supreme interpreter of the law). On the other hand, the Constitutional Court said that the appellant had had all the means to refute the information about the use given to the secret funds and considered that there was no lack of proper defence in this case, so it rejected the appeal.

Finally, there is a special judicial proceeding for the issuing of the warrants needed by the National Intelligence Centre for the interception of communications and the searches of premises. In 2002, the Spanish Parliament passed two acts applicable to the National Intelligence Centre: the National Intelligence Centre Act (Law 11/2002, of 6th of May) and the Ex Ante Judicial Oversight of the National Intelligence Centre Act (Organic Law 2/2002 del Control Judicial Previo del Centro Nacional de Inteligencia). According to the Ex-ante Judicial Oversight of the National Intelligence Centre Act (2002) the Secretary of State Director of the Intelligence Centre must ask a particular judge for the warrants. The judge is a Supreme Court judge elected by the Judges' Government body for a period of 5 years. All the proceedings and the decisions taken by the judge are classsified information. The judge must justify his decision.

Comment to question 8 a ii (Autonomous Oversight Bodies): The CNI Act of 2002 establish the obligation by the National Intelligence Centre to inform annually the

Parliament Committee that controls it about its activities and despite the vague character of the information, it can always give clues to Parliament on what to ask for (art. 11 section 4 CNI Act 11/2002, of 6th of May). Obviously, the Director will have means to hide what he does not want Parliament to know, and obviously, an annual report can be too general or vague. There should be more frequency in the reports that the Agency should send to the Committee or in the appearances of the Director before the Committee, but actually the law does not envisage it. The Committee develops usually more of an ex post oversight than an ex ante control. The avoidance of possible abuses demands an active Committee with time to devote to its task, who uses every means at reach and a law that oblige the security services to report more often, also about some operations.

Comment to question 9 d (Whistleblower protections): According to the legal scholars' interpretation of article 598 of the Spanish Criminal Code, public personnel could be prosecuted for disclosing classified information, in making a complaint internally, to someone within their own ministry, department or unit ony if this person that receives the information does not have the authority to access to that classified information .

Media Protection (question 10)
Article 598 of the Spanish Criminal Code: Article 598 provides that he who seeks and obtains, reveals, falsifies or renders useless information classified as secret or confidential, related to national security, will be sanction with one to four years imprisonment.
Article 9 of the Official Secrets Act provides in section one that anyone who gets to know or to possess classified information and know that the information is classified must keep the secret and give it back to the nearest civil or military authority, and if that was not possible, communicate to them their discovery.
Article 600 section 2 of the Spanish Criminal Code provides that the person who possess classified information (without express authorization) and does not comply with the legislation in force (article 9 of the Official Secrets Act) will be sanction with six months to three years imprisonment.
Article 20 of the Spanish Constitution:
1. The following rights are recognized and protected:
a) To express and disseminate thoughts freely through words, writing, or any other means of reproduction.
b) Literary, artistic, scientific, and technical production, and creation.
c) Academic freedom.
d) To communicate or receive freely truthful information through any means of dissemination. The law shall regulate the right to the protection of the clause on conscience and professional secrecy in the exercise of these freedoms.
2. The exercise of these rights cannot be restricted through any type of prior censorship.

Record Maintenance

Question 11 a sources: Articles 49.2, 52 and 54 of the Law of Historic Heritage (Law 16/1985 of 25th of June).

The person responsible for the Classified Information Protection Service will supervise the registry of all the classified material (article 25 of the Decree 242/1969

of the regulation developing the Official Secrets Act). Article 9 of the Decree says that the Classified Information Protection Services from the Ministries will control and registry the classified material. In every Classified Information Protection Service the person in charge of it will annually -in January- create an updated index of the classified information it holds and will send a certificate with the results to the Ministry of his Department (article 26 of the Decree 242/1969 of the regulation developing the Official Secrets Act).

Feedback on Draft Report from Susana Sanchez Ferro – SPAIN

It is very important to me that my response to question 7 g I and 7 g ii is clarified in the report, otherwise it could lead to misunderstandings. The questions, as remembered were Question (7)(g)(i): "May the government refuse to disclose information to the opposing party in [a habeas corpus claim] on the basis of national security? And question 7 (g) (ii): "May the government refuse to disclose information to the opposing party in [a claim of grave human rights violations (e.g., torture) brought against a public authority] on the basis of national security? I answered that the Government could refuse to disclose information on the basis of national security to the opposing party (whenever the information is classified), also in those proceedings. But I should have explained that refusal by the Government to disclose the information is not conclusive.

In fact, in his jurisprudence, the Supreme Court said that articles 9.1 and 24 of the Spanish Constitution obliged it to accept the review (in camera) of the possible abuses or failures to comply with the law in which the Government could have incurred when taking the decision to classify the information (when the opposing party challenges the refusal to declassify the information by the Government, who alleges that the information is classified in order to refuse the disclosure). The Supreme Court controls if there are elements that either suppressed the affection to national security of the documents or reduced it –balancing the interests at stake–. The Supreme Court after balancing the fundamental rights at stake with national security can decide that the Government must disclose the information to the opposing party (Decision of the Supreme Court of 4th April 1997). In fact, the Supreme Court has said that a very important element in its decision will be to analyze if the information regards a case in which the judge seeks to discover the truth about crimes that has jeopardized rights and interests of maximum value, such as the life of people. In a case like that (Decision of the Supreme Court of 4th April 1997), the Court obliged the Government to disclose the information or parts of it (other parts were left in secret: basically those that could reveal the sources and methods of the intelligence services).

Page 9: you are right, when answering to question 1c I was just thinking about the examples given in question 1c. In Spain the law on access to information is restrictive, it provides access to administrative information held by public authorities in public registries and archives, that is, of information related to the performed of administrative functions. There is no law regulating access to information held by the legislative branch for example.

Page 14, footnote 54: The general time to respond to a request of information in Spain is three months as you can see in the questionnaire. The 30 days period only applies to access to environmental information, so the sentence “Notably, since in Spain there is no specific legislation dealing with access to information, the time to respond (30 days) is a general one to respond to any request directed to the public administration” should be changed (the time to respond is three months, not 30 days).

Page 15 and footnote 66, Confirming or Denying the Existence of Requested Information: in Spain a clarification should be introduced. The right of access to information is so limited (right to information contained in public archives and public registries) that the requests will be answered only in those petitions concerning access to archives and public registries. Public authorities are not obliged to answer to general petitions of information made by the public apart from those petitions of access to administrative archives and registries. The obligation to answer to the latter petitions is the general one established by article 42 of the Law regulating the fuctioning of the Public Administration (Ley 30/1992, of 26th November, de Régimen Jurídico de las Administraciones Públicas y el Procedimiento Administrativo Común).

Review of a Denied Request for Information
Page 19. In relation to question 6 it is important to clarify that in Spain if the information denied is classified, the only court to be able to reverse the classification decision and to oblige the Government to declassify the information is the Spanish Supreme Court (no other judge).

Note 143, page 25, question 3 h). In theory, there is a duty for public authorities to state reasons for classifying information which derives from article 54.1 a) of the Law regulating the fuctioning of the Public Administration (Ley 30/1992, of 26th November, de Régimen Jurídico de las Administraciones Públicas y el Procedimiento Administrativo Común). This law states that the acts restricting subjective rights or legitimate interests have to include brief reasons of fact and law to do so. But I am afraid that in reality this duty in most of the cases having to do with the classification of information is not complied with.

Whistleblower protection: In Spain, similar to Italy, article 262 of the Code of Criminal Procedure states that anyone who by reason of his/her duty becomes aware of a crime, must report it to the prosecutor office or the competent court. There is a fine for those who do not report.