instruments or data protection impact assessments by providing tools (software or other), templates or guidelines?

Funding bodies, such as the national Slovenian Research Agency (ARRS), require ethics self-assessment from the applicants to their open calls from 2006. However, the ethics checks during implementation phase of the research projects that the Agency funds are not systematically conducted and remain underdeveloped. The Agency does not offer support in the sense of, for instance, providing templates of informed consent form, or similar guidance for applicants.

(iii) Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

The national legislation that implements Dual-Use Regulation no 428/2009 of 5 May 2009 and Council Joint Action of 22 June 2000 concerning the control of technical assistance related to certain military end-uses (2000/401/CFSP) consists of:

- Act Regulating the Control of Exports of Dual-Use Items (Zakon o nadzoru izvoza blaga z dvojno rabo, ZNIBDR); and

- Decree on procedures for issuing authorisations and certificates and on competence of the Commission for the Control of Exports of Dual-Use Items (Uredba o načinu izdaje dovoljenj in potrdil ter vlogi Komisije za nadzor izvoza blaga z dvojno rabo).

However, there is no guidance for researchers when dual use items may be involved, e.g. similar to Guidance notes of the H2020, such as:

- Guidance note — Research involving dual-use items, or

- Guidance note — Research with an exclusive focus on civil applications.

I am not aware of any national specific tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches.

26 Spain

Aliuska Duardo (UPV/EHU), Lorena Campillo (UPV/EHU), Iker Conal (UPV/EHU),

26.1 Informed consent

26.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos	https://www.boe.es/boe/dias/2018/1	Hard law	This law aims to:

***Personales y garantía de los derechos digitales.* (LOPDGDD) Organic Law on the Protection of Personal Data and Guarantee of Digital Rights**	2/06/pdfs/BOE-A-2018-16673.pdf (Spanish)		(To adapt the Spanish legal system to GDPR, and to complement its provisions. To establish provisions for the exercise of the fundamental right of individuals to the protection of personal data, protected by Article 18.4 of the Constitution. To guarantee the digital rights of citizens in accordance with the mandate established in Article 18.4 of the Constitution.
Ley 14/2007, de 3 de julio, de Investigación biomédica (LIB) Biomedical Research Act	https://www.boe.es/buscar/pdf/2007/BOE-A-2007-12945-consolidado.pdf (Spanish)	Hard law	The purpose is to regulate, with full respect for human dignity and identity and the inherent rights of the individual, biomedical research.
Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. ***Law 41/2002, of 14 November, on patient autonomy and rights and obligations regarding clinical information and documentation***	https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188 (Spanish)	Hard law	Regulates the rights and obligations of patients, users and professionals, as well as public and private health centres and services, in terms of patient autonomy and clinical information and documentation
Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, los Comités de Ética de la Investigación con medicamentos y el Registro Español de Estudios	https://www.boe.es/boe/dias/2015/12/24/pdfs/BOE-A-2015-14082.pdf (Spanish)	Hard law	Transposes specific provisions of the European Regulation on clinical trials, and regulates research ethics committees for medicines, as well as the Spanish register of clinical trials. Specifically, Article 3.3. states that the subject's rights to physical and mental integrity and privacy will be respected, and personal data will be protected.

Clínicos./*Royal Decree 1090/2015 of 4 December, which regulates clinical trials with medicines, the Ethics Committees for Research with *Medicines and the Spanish Clinical Trials Register.			
***Ley 33/2011, de 4 de octubre, General de Salud Pública* (LGS). Law 33/2011, of 4 October, General of Public Health**	https://www.boe.es/buscar/pdf/2011/BOE-A-2011-15623-consolidado.pdf (Spanish)	Hard law	Establishers the basis for the population to achieve and maintain the highest possible level of health through policies, programmes, services and, in general, actions of all kinds carried out by public authorities, companies and citizens' organisations with the aim of acting on the processes and factors that most influence health, and thus prevent disease and protect and promote people's health, both in the individual and collective sphere[205].

Main regulatory tools addressing data protection issues and informed consent in Spain

(i) The GDRP does not apply to purely personal or household activity. Is there any provision under national law for the protection of these data categories?

There is no express definition in the Spanish LOPDGDD in this regard. However, protection in this area can be guaranteed through the *right to honour, personal and family privacy and self-image* (article 18.4 of the Spanish Constitution). In turn, in the Penal Code, through the typification of various criminal conducts protects this legal right (Articles 197 to 201).

(ii) The GDPR does not apply to national security. Is there any national regulation covering this topic (in terms of data protection issues)?

Specific provisions related to this matter can be found in the Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and the execution of criminal sanctions. This law transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. Likewise, the Spanish law on data protection and guarantees of digital rights, regulates in its article 22 the processing of personal data carried out for video surveillance purposes. It is also possible to find security-related provisions in Law 25/2007, of October 18, 2007, on the conservation of data relating to electronic communications and public communications networks, and in

[205] Specifically, it is stated that "the health administrations will NOT need to obtain the consent of the persons concerned for the processing of personal data, related to health, as well as its transfer to other public health administrations, when this is strictly necessary for the protection of the population's health".

Royal Decree 3/2010, of January 8, 2010, which regulates the National Security Scheme in the field of Electronic Administration.

Name of Authority	Is this an independent body?	Number of employees	Level of activity	Response to requirements, questions, etc. made by the public
Spanish Data Protection Agency[206] **Agencia Española de Protección de Datos (AEPD)** **https://www.aepd.es/es**	Yes	203 in 2020: The Director, 196 (official staff), 4 for staff working under a single agreement and 2 for staff working outside an agreement[207]	High.	In 2019, 11,590 complaints, 21 cross-border procedures and 79 notifications of security breaches were lodged with the Agency. In addition, 152 consultations and 76 mandatory reports were made according to the Agency's own reports[208]

Information regarding Data Protection Authority

(iii) Does your national legislation introduce a specific definition of "data processing for research purposes"?

There is no express definition in the Spanish LOPDGDD.

However, mention is made of "data processing in health research, and in particular, biomedical research". Specifically, the purposes of such data processing "may cover categories related to general areas relating to a biomedical or research specialty" (Provision XVII 2a. LOPDGD). It is worth to mention that the Biomedical Research Act 14/2007 of 3 July 2007, establishes what is considered research in this field, including clauses on the protection of personal data, in general, and in particular on the "processing of genetic data of a personal nature".

(iv) Does your national legislation define "research in public interest", e.g. referring to Ministerial lists of expected research, etc.?

[206] It should be noted that, from a political-administrative point of view, Spain is divided into Autonomous Communities. In this respect, there are two Autonomous Communities which have their own supervisory authorities, according Art 57 LOPDGDD: the Catalonian Data Protection Authority (APDcat) and the Basque Data Protection Agency (AVPD)).

[207] Detailed information, in Spanish, at: https://www.aepd.es/es/la-agencia/transparencia/informacion-economica-presupuestaria-y-estadistica/retribuciones-y-compatibilidades-del-personal

[208] https://www.aepd.es/sites/default/files/2020-05/memoria-AEPD-2019.pdf

As regards the *reuse of personal data for research purposes* in the field of health and biomedicine, once *consent* has been obtained for a specific purpose, and in cases of use for other purposes or areas related to that of the initial study, those responsible for processing the data must publish this information in an easily accessible place on the corporate website of the centre where the research or clinical study is carried out and, where appropriate, on that of the sponsor, and notify the affected parties of the existence of this information by electronic means. If data subjects do not have the means to access this information, they may request that it be sent to them in another format (other than the corporate website). In addition, a prior favourable report from the Research Ethics Committee will be required.

In any case, data processing in health research, particularly in biomedical research, shall be lawful where pseudonymisation exists. [209] The use of pseudonymised personal data must be subject to the prior report of the research ethics committee provided in sectoral regulation. In absence of such a committee, the entity responsible for the research shall require a prior report from the DPO or, in its absence, from an expert with prior knowledge (Art 37.5 GDPR).

In addition, an impact assessment will also be carried out to determine the risks derived from the treatment of the cases provided for in Art 35 GDPR. In particular, the risks of re-identification linked to the anonymisation or pseudonymisation of data. Scientific research must be subject to quality standards. In addition, measures must be taken to ensure that researchers do not have access to data identifying the data subjects. A legal representative established in the EU should also be appointed if the sponsor of a clinical trial is not established in the EU (Art 27.1 GDPR)

(v) Does your national legislation provide specific cases and safeguards for processing sensitive data beyond article 9 of the GDPR? Which cases? Which safeguards?

The processing of personal data in the public interest - public health field- should be subject of a regulation with the status of law. This may establish additional guarantees regarding security and confidentiality (Art. 9.2. LOPDGDD). They shall refer to regulations such as the General Public Health Law (LGS), the Biomedical Research Law (LIB) or the Spanish Clinical Trials Regulations. It is possible that the Spanish legislator means measures related to the professional secrecy of researchers.

(vi) Do you have a national (or some regional) Code(s) of Conducts or national Code of Ethics for data processing in research? Could you please summarize the content of such codes (specifying scope, suggested measures to protect individuals, prohibitions, exemptions, etc.)?

Yes, the "Pharmaceutical Industry Code of Conduct for the Protection of Personal Data in the Field of Clinical Research and Pharmacovigilance"[210]. This code is outdated. In any case, in 2017, it was announced that “Farmaindustria” was working on the

[209] For this purpose, will be made: 1. A technical and functional separation between the research team and those who carry out the pseudonymization. 2. Pseudonymized data should only be accessible for the investigation team when specific security measures are taken to prevent re-identification and access by unauthorized third parties. Re-identification of data at source may be carried out when, in the course of an investigation using pseudonymised data, it becomes apparent that there is a real and specific danger to the safety or health of a person or group of persons, or a serious threat to their rights, or that it is necessary to ensure adequate health care.

[210] Vid. https://www.farmaindustria.es/web/documento/codigo-tipo-de-farmaindustria-de-proteccion-de-datos-personales-en-el-ambito-de-la-investigacion-clinica-y-de-la-farmacovigilancia-2/

development of a new code[211]. Its stated aim is to ensure that responsibilities and rights are shared by all actors involved. This is intended to respond to the challenges posed by the various sources of big data (genomic information, clinical trials, electronic medical records, etc.). They are proposing topics likewise: pseudonymisation, management of incidental findings or promoting the use of genomic data repositories.

It is worth mentioning, in this sense of innovation and technology, the Model Code for big data projects created by the Spanish DPA (AEPD) and the ISMS Forum.

On the other hand, the recent AEPD (Spanish DPA) guide on accreditation criteria for supervisory bodies of codes of conduct may be of interest to the reader[212].

Does your national legislation give specific definitions of data processing for "statistical purposes"?

No. There is no specific definition of "statistical purposes" in the Spanish LOPDGDD.

In any case, the regulations indicate that they will be of strictly voluntary contribution, and consequently, the data of articles 9-10 GDPR (Art 11.2 LFEP) may only be collected with the express consent of those affected[213].

(vii) Are there specific rules that apply to such data processing?

We are not aware of that.

(viii) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

Yes, this regulation is mainly based on the LOPDGDD. For details, see the answer to question (vi) above.

26.1.2 Rights of data subjects and data processing

(i) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

The Art 19 LOPDGDD where the processing of personal data of contact, of individual employers and of liberal professions is regulated can be of interest. This processing is legally permitted based on legitimate interest and taking into account that the data is necessary for the "professional location". However, the AEPD has stated that "both legal entities and professionals presenting their services in the AEPD are outside the scope of the GDPR".

(ii) Are there any special requirements regarding informed consent at the national level?

Specific reference is made to consent, which must come from a declaration or clear affirmative action by the affected person, excluding what was known as "tacit consent". It is stated that in the case of consent by the person concerned for a number of purposes, it must be specifically and unequivocally stated that it is given for all of them (Article

[211] Vid. https://www.farmaindustria.es/web/otra-noticia/nuevo-codigo-conducta-la-industria-farmaceutica-garantizara-equilibrio-la-proteccion-datos-fomento-la-investigacion-biomedica-la-del-big-data/

[212] Vid. https://www.aepd.es/sites/default/files/2020-02/acreditacion-organismos-supervision-cc.pdf

[213] Vid. https://www.boe.es/buscar/doc.php?id=BOE-A-1989-10767

6.2. LOPDGDD). The age from which the minor can give his or her consent is maintained at fourteen years. In addition, Spanish law adapts the principle of transparency in the processing of the GDPR and includes so-called "layered information"[214].

(iii) Are there any special requirements regarding data processing at the national level?

Yes, regarding the processing of health data and research. In particular, the processing of pseudonymized personal data for the purposes of health research, and in particular, biomedical research, shall be lawful.

the following requirements will be demanded:

a.) A technical and functional separation between the research team and those who carry out the pseudonymization and keep the information that makes reidentification possible.

b.) That the pseudonymised data are only accessible to the research team when there is an express commitment to confidentiality and not to carry out any reidentification activity and that specific security measures are taken to prevent reidentification and access by unauthorised third parties.

(iv) Are there any special requirements to exercise data subject's rights (right of access, correction, deletion of personal data)?

Yes, when there is processing of personal data for the purpose of health research, and in particular, biomedical research. For the purposes of Article 89.2 GDPR may be exempted from the rights of access, rectification, limitation of treatment and opposition, when:

a.) They are exercised directly against researchers or research centres using anonymised or pseudonymised data.

b.) The exercise of such rights concerns the results of the research.

c.) The research has an essential public interest related to State security, defence, public security or other public or general interest objectives, provided that in the latter case the exception is expressly covered by a rule with the rank of law.

26.1.3 Minors, sensitive data and other additional categories of data

(i) Are there additional rules beyond the ones enforced by the GDPR for processing special categories of personal data (e.g. sensitive data or data of legal persons/entities)?

We are not aware of that.

(ii) Are there any special rules when processing personal data of children? At what age can a minor provide consent according to your regulation?

Some of the special rules are:

(a) Data controllers and processors must appoint a DPO in the case of sports federations when they process data on minors. (b) When the use or dissemination of images or

[214] Generally accepted in areas such as video surveillance, devices or installation of mass data storage devices, where it is indicated an address or other means for the affected to easily and immediately access the remaining information. For more information: https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf

personal information of minors in the digital environment could imply an illegitimate interference with their fundamental rights, the intervention of the Public Prosecutor's Office will be determined, who will urge precautionary and protective measures in accordance with the Law on Protection of Minors. (c) A draft law is planned to guarantee the rights of minors in the face of the impact of the Internet in order to ensure their safety and to combat discrimination and violence through new technologies.

With regard to consent:

The processing of a minor's personal data may only be based on his or her consent when he or she is over 14 years of age. Exceptions are made in cases where the law requires the existence of the holders of parental authority or guardianship for the conclusion of the legal act or business in the context of which consent for processing is sought.

The processing of the data of minors under 14 years of age, based on consent, will only be lawful if the holder of the parental authority or guardianship is known, with the scope determined by the holders of the parental authority or guardianship. The latter may exercise their rights of access, rectification, cancellation, opposition or any other of the LOPDGDD.

(iii) Are there other vulnerable individuals identified in your national legislation?

Persons with disabilities are referred to as "particularly vulnerable groups". (See Art 28.2.e LOPDGDD)

26.1.4 Deceased individuals and personal data

(i) As recital 27 clarifies, the GDPR does not apply to deceased individuals. However, some countries provide people with the right to have all their personal data deleted once they pass away. Some others empower their close relatives to do the same. In some others, these data cannot be used at all without an explicit judicial mandate. What is the situation in your country?

The regulation empowers relatives or heirs to request access to the personal data of the deceased and, where appropriate, their rectification or deletion. However, the relatives or heirs cannot exercise these rights when the person who has died has previously expressed himself or is contemplated by a law (Art 3.1. LOPDGDD).

26.1.5 Accountability and Data Protection Impact Assessment

(i) Does your national regulation introduce further provisions related to general accountability? Any particular requirements? Any specific procedures?

Yes. There are some specific provisions, such as:

1. With respect to electronic identification for public administrations, new regulations were established in 2019[215] requiring that the technical resources for the collection, storage, processing and management of these systems be located in the European Union.

2. With regard to the register of processing activities (Art 31. 2 LOPDGDD), it is compulsory for public bodies and public law entities or public universities (Art 77.1. LOPDGD) to publish an inventory of their processing activities, accessible by electronic means, containing the corresponding information in accordance with Article 40 GPRD and its legal basis (Art 31.2. LOPDGD).

[215] Vid. https://www.boe.es/boe/dias/2019/11/05/pdfs/BOE-A-2019-15790.pdf . Art. 3.3.

3. With regard to the blocking of data, it is stated that the data controller is obliged to do so when rectifying or deleting the data (Art 32.1 LOPDGDD).

(ii) Are data protection impact assessments requirements specified by your national regulation? Any particular requirements? Any specific procedures? Any specific reference to data processing in research?

There is no regulation containing criteria for carrying out an impact assessment.

However, there is soft law in the form of AEPD guidelines:

- Practical guide to data protection impact assessments subject to the GDPR[216].

- Model data protection impact assessment report for public administrations[217].

On the other hand, with regard to public health research, the LOPDGDD establishes the obligation to carry out an impact assessment that determines the risks of Art 35 GDPR, or those established by the control authority, which include the risks of reidentification linked to the anonymisation or pseudonymisation of the data.

26.2 Commercialization of data

26.2.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Royal Legislative Decree 1/2007, of 16 November, approving the revised text of the General Law for the Defence of Consumers and Users and other complementary laws (LGDCYU).	https://www.boe.es/buscar/act.php?id=BOE-A-2007-20555	Hard law	This rule shall apply to relations between consumers or users and employers.
Law 34/2002, of 11 July, on information society services and electronic commerce (LSSI).	https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758	Hard law	Legal regime for information society services and electronic contracts, with respect to the obligations of service providers including those acting as intermediaries in the transmission of content via telecommunications networks, commercial communications by electronic

[216] Vid. https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd_0.pdf

[217] Vid. https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-un-modelo-de-informe-para-ayudar-las

			means, information prior to and following the conclusion of electronic contracts, conditions concerning their validity and effectiveness and the sanctions applicable to information society service providers.

Main regulatory tools addressing data commercialization in Spain.

26.2.2 Practice

(i) In practice, does your country allow contracts based on exchange of personal data for services (for instance, to gain access to an app)?

To our knowledge, no specific regulations for contractual exchange of personal data exist.

In any case, the entrepreneur must inform the user about the legal terms and conditions relating to a free product or service, meet the requirements of electronic sales and the requirements of the LSSI. Thus, for example, "significant failure to provide information" will be considered a serious infringement (Article 38.3 ISESA).

Furthermore, the LGDCYU regulates abusive clauses (Art 82-91 LGDCYU), which shall be null and void, and shall be considered "not taken into account".

(ii) Do you know if these practices are routinely performed?

In Spain, the company *Privacy Cloud*, developed the app (now inactive) *We Rule*[218], as the first company digital data broker for users. In the health field, one of the best-known is the *Aseguradora del Corte Inglés*, an insurance company, which gives bonuses to policyholders who do physical activity[219].

(iii) Does your country have any specific regulation on the remuneration of data subjects if profit is made out of their data?

There is no such legislation.

(iv) Do you have any particular national regulation on the secondary use of data?

The LOPDGDD, in its Transitional Provision VI, regulates the reuse of personal data for health and biomedical research purposes. It specifically states: "The re-use for health and biomedical research purposes of personal data lawfully collected prior to the entry into force of this Organic Law shall be considered lawful and compatible when any of the following circumstances apply: a) such personal data are used for the specific purpose for which consent was given. b) having obtained consent for a specific purpose, such data are used for purposes or areas of research related to the medical or research specialty in which the initial study was scientifically integrated".

---

[218] For more info: https://werule.app/ and: werule@privacycloud.com. The website´s information appoints that they are not developing this activity anymore and that their aim was to give control of the data of users who gave their data to companies.

[219] Vid http://www.expansion.com/empresas/banca/2018/04/10/5accd666ca4741fa528b4635.html. In the future, it is possible that technologies such as blockchain/DLT will encourage the exchange of personal data for services or compensation, especially in relation to clinical trials. Such compensation may be in the form of services (e.g., telemedicine services), economic services (e.g., with crypto-currency) or in the form of discounts or promotions for services, bonuses, etc. The same applies to technologies such as IA. The AEPD has issued a very interesting report in this regard: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf)

During the parliamentary process, this provision was criticised by the health sector and institutions such as the Spanish Biomedical Society, as it did not authorise the re-use of data or the provision of consent for purposes other than those initially envisaged. They disapproved the fact that medical research had not been taken into consideration as an activity of general public interest. In this regard, the AEPD Report 073667/2018 on biomedical research may be of great interest.

(v) Do you have any specific protection for metadata or non-personal data in your country?

No, nationwide. However, some experts consider that metadata could be included as personal data since it is invisible data that can be used for advertising or health marketing purposes.

In any case, we will await the adoption of the European Electronic Communications Regulation (ePR) [220].

26.2.3 Nature of Data

(i) How does your country classify data? Is it a product/commodity/good or service? Do you have an additional construct for data?

There is no such classification

(ii) Except for the Sui Generis Right on the protection of databases, do you have a legislation protecting data in your country (e.g. like copyright)? Are you aware of any mechanisms to determine the value of data?

Yes, LPI Article 12. Databases.

1. Collections of other people's works, data or other independent elements such as anthologies and databases which, by virtue of the selection or arrangement of their contents, constitute intellectual creations are also the subject of intellectual property rights under the terms of Book I of this Law, without prejudice, where appropriate, to any rights that may subsist in such contents.

The protection afforded to these collections by this Article relates solely to their structure as a form of expression of the selection or arrangement of their contents, and does not extend to them.

2. For the purposes of this Law, and without prejudice to the provisions of the foregoing paragraph, collections of works, data or other independent elements arranged in a systematic or methodical way and individually accessible by electronic or other means are considered databases.

3. The protection accorded to databases under this Article shall not apply to computer programs used in the making or operation of databases accessible by electronic means.

Regarding the value, perhaps we could take as a reference the amount of compensation for specific situations (Art 25 LPI).

On the other hand, it could also apply: (i) the Industrial Property Act when dealing with non-personal data, for example, in the pharmaceutical field in big data environments; (ii) the Business Secrets Act (2019). Any information or knowledge, including technological, scientific, industrial, commercial, organizational or financial, is considered a professional

[220] Vid. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=ES

secret. For this purpose, it must be secret, have a business value and have been subject to reasonable measures to keep it secret. The business secret is transmissible and may belong to several persons individually. Vid. https://www.boe.es/buscar/pdf/2019/BOE-A-2019-2364-consolidado.pdf

26.3 Security and cybersecurity

26.3.1 General Regulatory Framework

Regulation	Type of regulation	Brief description and scope
Spanish Constitution (Preamble and articles 18.4, 8, 97 and 104) **http://www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/Norm/const_espa_texto_ingles_0.pdf**	Hard law	Before the current technological development (since this legal text is almost thirty years old, and has not been modified to adapt it to the evolution of technology), it was already considered relevant for the security of Spaniards and their Fundamental Rights and Freedoms to adopt measures by public authorities to ensure a safe cyberspace. Its inclusion in the Constitution means that it makes sense as a matter of major State policies, for which clear and stable guidelines are necessary over time and, above all, an adequate legal framework to regulate the actions of the

		State and the rest of the Public Administrations in a coordinated and coherent manner.
Spanish Criminal Code (articles 197-201, 248.2.a) & b), 264, 270, 274, 346 and 560) https://www.legislationline.org/ download/id/6443/file/Spain_CC _am2013_en.pdf **Warning: the last update of the Spanish Criminal Code took place in 2015. However, the last version translated into English is from 2013, which is why this one is included.**	Hard law	The Criminal Code, as part of the prosecution of "computer crimes", seeks to prosecute all criminal offences carried out through computer means, and those that are linked to legal assets related to information technology, as well as those that have as their purpose these assets.
Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones* *** Repealed and replaced by:** **Ley 9/2014, de 9 de mayo, General de Telecomunicaciones** **(Currently in force)**	Hard law	A fundamental rule when it comes to establishing the regulatory framework for Cybersecurity in Spain. This is the central regulation of telecommunications in this country, reformed ten times since its approval, showing how difficult it is to maintain an adequate regulatory framework in a matter so subject to change and so immersed in the field of advances

		in information technologies.
Organic Law 3/2018 of December 5, 2018, on the Protection of Personal Data and guarantee of digital rights. (LOPDGDD) https://www.boe.es/eli/es/lo/2018/12/05/3 Spanish	Hard law	It is an essential rule in the protection of the fundamental rights of citizens who could be attacked from cyberspace. It establishes the tutelary role of the Spanish Data Protection Agency, conceived as the State body in charge of ensuring compliance with legislation in this area and controlling its application.
Law 34/2002, of July 11, 2002, on information society services and electronic commerce. https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758 (Spanish)	Hard law	Article 12a of this rule imposes a series of security obligations on providers of Internet access services, such as permanently, easily, directly and free of charge informing their customers of the various technical means of increasing the levels of information security and allowing, inter alia, protection against computer viruses and spyware and the restriction of unsolicited e-mails.

Law 11/2007, of June 22, on electronic access of citizens to public services, and the National Security Scheme * *** Repealed and replaced by:** **Law 39/2015, of October 1, on the Common Administrative Procedure of Public Administrations** **(Currently in force)** https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10565 (Spanish)	Hard law	Applicable to all Spanish Public Administrations, it was fundamental for creating the National Security Scheme, which established the principles and requirements of a policy of security in the use of electronic means that allows the adequate protection of information.
Law 8/2011, of April 28, which establishes measures for the protection of critical infrastructures https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/Ley82011-de28deabril-PIC.pdf Spanish)	Hard law	Another major element to safeguard against possible attacks is critical infrastructure, a strategic element to guarantee the country's own security and that of its citizens. The aim of this Law is to prevent possible attacks, reduce vulnerability and, in the event of crisis situations affecting basic infrastructures, minimize damage and the recovery period.
Royal Decree Law 12/2018 of 7 September on the security of networks and information systems. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257 (Spanish)	Hard law	This is, as I will point out later, the transposition of Directive (EU) 2016/1148 of the European Parliament and of

		the Council of 6 July 2016 on measures to ensure a high common level of security of networks and information systems in the European Union, known as the NIS Directive.
Royal Decree Law 14/2019 of October 31, 2019, adopting urgent measures for reasons of public security in the areas of digital administration, public sector procurement and telecommunications. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-15790 (Spanish)	Hard law	Possibly the most controversial piece of legislation in this area, given that it has been approved by the Spanish Government in office. In this sense, information to the public has been really scarce and inefficient, and there has been a great deal of confusion among citizens, with all sorts of rumours and misinformation in relation to it. Thus, there has been talk of the possibility of it being a governmental tool that would diminish the rights of citizens to a decision taken quickly because of the political situation in Catalonia, where, hypothetically, the intention was to create a

		communications network autonomous and differentiated from that of Spain. Disinformation and the abyss between the administration and the citizenry, therefore, define this piece of legislation.
Royal Decree 421/2004, of March 12, 2004, regulating the National Cryptologic Center. https://www.boe.es/eli/es/rd/2004/03/12/421 (Spanish)	Hard Law	Creates the National Cryptology Centre (CCN), which is the organization responsible for coordinating the different organizations' activities in the Public Administration, using resources or encryption procedures and ensuring the security of the information technologies in all areas, keeping informed concerning the coordinated acquisition of the cryptology material and it is also responsible for providing training for Public Administration resources who specialise in this field.

		Royal Decree 421/2004, assigned to CNI (National Centre of Intelligence). In fact, the Spanish Act 11/2002, of May 6, regulating the National Intelligence Center, which regulates the CNI, entrusts to the said Centre, all functions regarding the security of information technologies and protection of classified information, while the responsibility of running the National Cryptology Centre is conferred to the Secretary of State Director. That is why the CCN shares environments, procedures, regulations and resources with the CNI.

Main regulatory tools addressing security and cybersecurity in Spain

26.3.2 Implementation of EU Law

(i) Are any particular procedures described in your national regulation?

No as far as we are concerned.

(ii) What is the status of the implementation of the NIS directive in your country towards data protection/security of data?

The NIS Directive has been transposed into our state law through the Royal Decree Law 12/2018 of 7 September on the security of networks and information systems.

(iii) The GDPR stipulates that appropriate technical and organisational measures to protect personal data must be implemented. Is this prevention reflected in your national regulation?

Yes, and this system is, like the legislation, prior to the transposition of the NIS Directive, in many cases. Thus, in Spain there is the National Cryptologic Center (CCN), dependent on the National Intelligence Center (CNI), the National Institute of Cybersecurity of Spain (INCIBE), the National Center for the Protection of Critical Infrastructures (CNPIC), the Guardia Civils' Telematic Crimes Group and the National Police's Information Technology Crime Investigation Unit, the Spanish Data Protection Agency (AEPD) and, of course, the respective CERTs created by some Autonomous Communities, such as the recently created Basque Cybersecurity Centre.

26.3.3 Personal Data Breach Notification

(i) What requirements in relation to data breach notifications exist in your national regulation? Is this issue regulated in the national implementation of the NIS Directive?

The Royal Decree Law 12/2018 of 7 September on the security of networks and information systems, as a transposition of the NIS Directive, also requires essential service operators and digital service providers to notify incidents on the information networks and services they use for the provision of essential and digital services, and to have significant disruptive effects on them, while providing for the notification of events or occurrences that may affect essential services, but have not yet had a real adverse effect on those services, and outlining the notification procedures.

Incident reporting is part of the risk management culture promoted by the Directive and the Royal Decree Law 12/2018. Therefore, it protects the reporting entity and staff reporting incidents; confidential information is reserved from disclosure to the public or to authorities other than the notified authority; and incident reporting is permitted when communication is not required.

Various articles (such as 19.3, 20, 21) of the Royal Decree Law 12/2018 establish specific obligations and rights in accordance with the provisions of the NIS Directive.

26.3.4 Supervision of cybersecurity

(i) Does a supervisory body in a narrow sense with enforcement powers exist in your country?

Yes, the Spanish National Institute for Cybersecurity (INCIBE) exists specifically in the field of Cybersecurity. However, I believe that the National Cryptology Centre (CCN), which depends on the National Intelligence Centre (CNI), may be more in line with the supervisory figure with executive powers.

(ii) Is in your country an institution like the German BSI (Bundesamt für Sicherheit in der Informationstechnik) established. The Federal Office for Information Security is the national cyber security authority of Germany. It shapes information security in digitisation through prevention, detection and reaction for government, business and society. (https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html) or

something similar established? If yes, what are the competences and responsibilities?

Yes, the Spanish National Institute for Cybersecurity (INCIBE). Its capabilities are as follows:

- Wide scope of action in the response to security incidents ranging from the citizen to the business sector (especially strategic sectors and critical infrastructure) and to the specific scope of RedIRIS.

- Implementation of public-private collaboration initiatives to improve cybersecurity levels in Spain.

- Monitoring and study of emerging risks in order to anticipate needs, adopt preventive measures and, in short, have early warning mechanisms.

- Coordination with key national and international cybersecurity actors.

(iii) How can damages caused by lack of cybersecurity be claimed (and compensated)? Are such issues sufficiently regulated in your country?

At present, governmental institutions such as the National Institute of Cybersecurity of Spain (INCIBE) or, at the autonomous level, the Basque Cybersecurity Centre ensure the protection of citizens, but do not take direct responsibility for it. In other words, in the event of an attack that violates the cybersecurity of a private company or an individual, the measures that can be taken against those who were supposed to guarantee it will have to be analysed. Royal Decree Law 12/2018 provides, for example, the sanctions that the State may impose on those who do not comply with its provisions, but does not give individuals the option of claiming damages.

26.4 Enforcement: fines and sanctions

(i) Is a crime related to data protection or cybersecurity punished by a fine or imprisonment?

Yes, several crimes related to the protection of personal data can be found in the Spanish Penal Code (CP), in particular:

Crime of discovery and disclosure of secrets. A prison sentence of 3 to 5 years is imposed if the data or facts discovered are disseminated, revealed or transferred to third parties or the images captured are carried out through the unauthorized use of the victim's personal data (Art 197.4 CP).

Crime of computer damage. A prison sentence of two to five years and a fine of up to ten times the damage caused will be imposed (Art 264.2 CP), for example, when the facts have affected the computer system of a critical infrastructure, an element or part of it that is essential for the maintenance of vital functions of society and health, for example. But with regard to data protection, the penalties will be aggravated when the acts have been committed through the illicit use of the data of another person to facilitate access to the computer system or to gain the trust of a third party (Art 264.3 CP).

(ii) Are there administrative fines related to data protection issues?

Yes:

- Using a person's personal data or communicating them to third parties without their consent, in particular if sensitive data such as ideology, religion, beliefs, ethnic origin, health, life and sexual orientation are involved.

- Obtaining a person's personal data in an unlawful and misleading manner

- Using a person's personal data for purposes that are incompatible with those for which they were collected without their consent. Victims of gender-based violence enjoy special protection covering the use, access and dissemination of their personal data, in order to avoid being exposed to new risks of this nature.

The amount is imposed according to the infringement committed and is graduated taking into account, among other elements, the nature of the personal rights affected, the benefits obtained, the degree of intentionality, recidivism and above all the damages caused to individuals.

(iii) Do data protection offences constitute an official offence or are only prosecuted by the injured party's request?

Both the offence of "discovery and disclosure of secrets", as well as "computer damage" and "harassment", explained above, constitute official offences and when these are not considered a crime, they will be referred to the AEPD (Spanish DPA).

26.5 Governance

(i) At least in the biomedical sciences research involving human participants usually is subject to ethical review by research ethics committees or similar bodies. Data protection, however, not only affects the biomedical sciences, but potentially all fields of research. Are you aware of any committees (e.g. research ethics committees, ethical review boards) or agencies (e.g. national research funding agencies, national security agencies) in your country that review data protection issues in research projects? If yes, are reviews mandatory and governed by specific guidelines or regulations? Do you know which aspects of data protection review bodies focus on? Are reviews only conducted before the actual research starts or is the research process monitored as well?

There are a large number of local, regional and national Healthcare Ethics Committees (HECT) and Research Ethics Committees (REC) in Spain. The HECT are independent interdisciplinary bodies to provide support in ethical dilemmas in healthcare settings, ensuring that patients are informed about their treatments and procedures and make free decisions on health. The RECs are focus on the rights and welfare of the potential participants in the research. These committees are called to play an important role in respecting and guaranteeing the right to protect personal data, in health practice and in research. In practice this committees gradually have been incorporating data protection assessment. For example, the Research Ethics Committee of the University of Basque Country (CEID-UPV/EHU) has published guidelines aimed at facilitating GDPR compliance in scientific research involving human beings. The document is freely available in three languages (English, Basque and Spanish):

CEID-UPV/EHU, A guide of data protection in human research (https://www.ehu.eus/documents/2458096/3401856/12_ProteccionDeDatos.pdf/ca7ca82a-ddca-ac1b-40a3-c5b29c0ec5c5?t=1610535319020)

Healthcare Ethics Committees (HETC)

The Health Care Ethics Committees (HECT) are set up as a consultative interdisciplinary committee to analyse and advise on the resolution of ethical conflicts that arise during the clinical practice of health care, to improve such care and to guarantee that patients are informed and can make freely voluntary decisions regarding their health.

In Spain, with the publication of the Order of 14 December 1993 on the accreditation of the Autonomic Ethic Committee in Catalonia, the Decree 143/1995 of the Basque Government, Circular 3/1995 on the creation and accreditation of the Ethic Committee in the INSALUD system, the way was opened to this effect. The creation of the HECT was initially voluntary, but in some regional regulations it is now mandatory. Among its members, the majority must be doctors and nurses, a law graduate, a person in charge of religious assistance at the centre, a person from outside the institution with training in bioethics, a member of the Research Ethics Committee, healthcare professionals from other specialties and members of the Quality Commission and the Patient Care Service. Currently, most of the Autonomous Communities have proceeded to create these committees, together with their respective regulatory development, not only in hospitals, but also in some Primary Care Services.

Autonomic (Regional) Bioethics Committees

In order to coordinate and accredit the HETC, evaluate the proposed action protocols and promote bioethics training for healthcare professionals, in some Spanish Autonomous Communities (Acs), the same order or decree that regulates the HETC establishes Bioethics Committees at the regional level. They also have the function of advising and guiding the regional ministries and organizations. The members include the Councillor and Vice-Councillor in charge of health matters and members appointed by them of recognized professional and scientific prestige in disciplines considered to be of interest.

Bioethics Committee of Spain

The Spanish Bioethics Committee, attached to the Ministry of Health and provided for in Law 14/2007 on Biomedical Research, was created to encourage the collaboration of the autonomous community organizations and to advise the public authorities at the state level. It is made up of members proposed by the Autonomous Regions and by the General State Administration, with each of the different Ministries and the *Instituto de Salud Carlos III* being represented.

Spanish Research Ethics Committee

With functions similar to those of the Bioethics Committee of Spain, Law 14/2011 on science, technology and research, incorporates a set of measures aimed at placing Spanish legislation on science and technology and innovation at the international forefront, including the incorporation of the professional ethical dimension, embodied in the creation of a committee that applies internationally accepted criteria and guidelines. It is made up of 12 members, six of whom are proposed by the National Government and the other six by the Autonomous Regions. Its functions include resolving conflicts between public and private activities and representing Spain in supranational and international forums and bodies.

In Spain, at both state and autonomous community level, there are other advisory committees whose functions also include ethical-social and legal issues related to certain biomedical activities, such as the Advisory Council of Health and Social Services or the National Commission on Assisted Human Reproduction.

Research Ethics Committees (REC)

In 2007, the Biomedical Research Law defined the RECs to guarantee in each research centre the adequacy of the methodological, ethical and legal aspects of research involving interventions on human beings or the use of biological samples of human origin. The LIB establishes the general principles for the elaboration of codes of good practice in scientific research and the functions to be carried out by them. The RECs must be duly accredited by the competent bodies of the Autonomous Regions or, in the case of centres dependent on the National Government, by the competent body of the latter.

Drug Research Ethics Committees (DREC)

Royal Decree 1090/2015 regulates the Drug Research Ethics Committees (DREC), not only circumscribed to the field of clinical trials and observational studies with drugs, but also to all research conducted with medical devices. The DREC is nothing more than an REC accredited in accordance with the terms of Royal Decree 1090/2015 to issue an opinion on research with medicines or medical devices. The DREC will be made up of a minimum of ten members, including physicians, one of whom will be a clinical pharmacologist, a hospital or primary care pharmacist and a graduate in nursing. If the centre has a research committee or a CEA, one member of each must be a member of the DREC. At least two members must be from outside the health professions, one of whom must have a law degree. In addition, at least one of its members must have accredited training in bioethics. Royal Decree 1090/2015 establishes that DRECs will be supervised in the same way as RECs, in accordance with the regulations governing the latter.

(ii) What instruments (e.g. ethics self-assessments at the proposal stage), if any, do research funding agencies and other research supporting bodies in your country use to promote data protection in ICT R&I? Do they facilitate the use of these instruments or data protection impact assessments by providing tools (software or other), templates or guidelines?

As stated, before Ethic Committees, especially research ethic committee at universities and research centres are called to play an important role in respecting and guaranteeing the right to protect personal data. In practice this committees gradually have been incorporating data protection assessment. Also, DPO[221] at these centres have to deal with ethical and legal issues regarding data protection. The level and quality of assessment, however, may vary from centre to centre depending on the degree of preparation and level of commitment of each DPO.

On the other hand, regarding DPIA, the Spanish data protection authorly (AEPD) has issued many guidelines: "Risk management and impact assessment processing of personal data processing" https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf (Spanish). While these are not specific to

[221] According to LOPDGDD, public and private universities, as well as health centres legally obliged to maintain the medical records of patients, have to appoint a data protection officer (art. 34).

research, they contain important information applicable to research. AEPD has also produced a "Code of good practice on data protection for Big Data projects" https://www.aepd.es/es/documento/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf (Spanish).

(iii) Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

As far as we are concern there are not specific regulation or procedure for ICT R&I involving defence, dual use of technology or affected by embargoes. In terms of regulation there exist a specific framework for dual use technology trade, established in the Law 53/2007 of 28 December 2007 on the control of foreign trade in defence and dual-use material and the related Royal Decree 679/2014, of 1 August, approving the Regulation on the control of foreign trade in defence material, other material and dual-use products and technologies. Nonetheless this regulation does not directly affect R&I.

On the other hand, there are concrete program for promoting research of Centre for the Development of Industrial Technology (Centro para el Desarrollo Tecnológico Industrial (CDTI)). CDTI is a Public Business Entity, under the Ministry of Science and Innovation, which promotes innovation and technological development of Spanish companies. It is the entity that channels applications for aid and support for R&D&I projects from Spanish companies at national and international level. A Collaboration Protocol has recently been signed between the Ministry of Defence and the Ministry of Science and Innovation involving the CDTI, in which the parties undertake to exchange information and act in coordination to support R&D&I in the defence sector.

The CDTI has created a specific department for Large Installations and Dual Programmes to directly attend to the needs of the defence and security sector in terms of business R&D&I, with tasks of promotion, management, representation, advice and strategic evaluation.

27 Sweden

Patricia Jonason, Anders Wainikka (University of Södertörn)

27.1 Informed consent

27.1.1 General Regulatory Framework

Regulation	Link (English version if possible)	Type of regulation (hard law, soft law…)	Brief description and scope