Spain: Technology

This country-specific Q&A provides an overview of technology laws and regulations applicable in Spain.

For a full list of jurisdictional Q&As visit here
1. Are communications networks or services regulated?

Yes. Act 9/2014, of 9 May, on Telecommunications (hereinafter, “Spanish Telecommunications Act”), covers the provision of electronic communication networks (“ECN”), as well as the provision of electronic communication services (“ECS”). Certain additional requirements apply to providers of publicly available telephone services (“PATS”), which are a sub-set within ECS. PATS is a service made available to members of the public for making and receiving national or international calls through a number in a national or international telephone numbering plan.

Also, it is important to highlight that on December of 2018, the European Union adopted the Directive (EU) 2018/1972, establishing the European Electronic Communications Code (hereinafter “the EECC Directive”). In some aspects, the EECC Directive is a recast text of the previous directives establishing the regulatory framework within the EU in the field of the electronic communications, although it also addresses changes such as 5G and spectrum, a broadened scope of application, access regulation, reinforces end-users rights, etc. Although the EECC Directive is already in force, Member States have a transposition period until 21 December 2020 to adopt the laws, regulations and administrative provisions necessary to comply with such directive.

2. If so, what activities are covered and what licences or authorisations are required?

Pursuant to item 26 of Annex II of the Spanish Telecommunications Act, an operator means a legal or natural person, which provides public communications networks or provides electronic communication services to the public and has notified the relevant authority at the beginning of its activity, or is registered under the Registry of operators.

Therefore, while in Spain an authorisation or license is not necessary in order to provide ECS or ECN, notification to the relevant authority remains mandatory. Prior to the provision of services or networks, the provider shall give notice of the start of the activity to the Registry of operators, which is overseen by the Spanish Regulator, the National Commission on Markets and Competition (“Comisión Nacional de los Mercados y de la Competencia”, in Spanish), commonly known simply as “CNMC”.

The CNMC will then issue a reasoned decision accepting or rejecting the notified activity within 15 days. If it fails to issue a decision within this period, the provider will be able to commence its activity.

Once registered, a service provider must notify the CNMC every three years of its intention to continue providing the ECS or ECN in question. Failure to notify will result in proceedings that may lead to the cancellation of the registration of the operator concerned. In this scenario, the operator would not be able to continue providing the ECS or ECN, and would be required to proceed to a new notification.
The following link provides the template for making the notification (https://sede.cnmc.gob.es/sites/default/files/2016-12/Notifica.pdf). Apart from information related to the identification of the company, a description of the activity to be carried out must also be included, as well as an estimated start date for the activity.

Although registration with the Registry of operators is free of charge, an annual administrative fee does apply (which is itself calculated on a yearly basis, currently 0.1% of the gross annual income generated with the provision of the relevant ECS or ECN) for each operator.

3. **Is there any specific regulator for the provisions of communications-related services?**

The CNMC, referred to in the previous answer, is the Spanish regulator that promotes and defends the proper functioning of the markets in the interest of consumers and companies, including the electronic communications market. Under Article 6 of Act 3/2013, adopted on 4 June 2013, regarding the creation of the CNMC, its main functions in the electronic market are to:

- Define and analyse markets related to electronic communications services and networks, including retail and wholesale markets, and its geographical range, whose features can justify the imposition of certain obligations.
- Identify the operator or operators that have significant power in the market and analyse when the markets are not developed in an effective competitive environment.
- Establish the applicable obligations for those operators with significant power on the market.
- Resolve electronic communications disputes in the market.
- Fulfil other obligations established by law.

In addition, the Secretariat of State for Digital Progress also has competences – both with regards to infrastructures, but also, for instance, concerning net neutrality and end user protection, in accordance with Article 8 of the Royal Decree 1046/2018, of August 24, by which the basic organic structure of the Ministry for Economy and Business is organised.

4. **Are they independent of the government control?**

The CNMC is independent from the Spanish Government, although it is subject to parliamentary control. According to Article 39 of Act 3/2013 on the CNMC’s creation, the President of the CNMC has to appear annually before Congress in order to outline the basic plan for its actions and priorities for the year ahead. In addition, the President must, every three years, present in person their evaluation of the action plan and the results achieved by the CNMC. Without prejudice from this annual appearance, the President must appear before the corresponding commission of the Senate or Congress on the same terms established in their respective regulations.
On the other hand, the Secretariat of State for Digital Progress is within the structure of the Ministry for Economy and Business.

5. **Are platform providers (social media, content sharing, information search engines) regulated?**

In Spain there is no regulation that specifically targets platform providers such as social media or content sharing yet. However, video sharing platforms are soon to be covered by regulation given a recent change to the Audio-visual Services Directive (Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010), by means of the Directive (EU) 2018/1808, which establishes a specific audio-visual regulatory framework for those platforms. Member States have a transposition period until 19 September 2020 to adopt the laws, regulations and administrative provisions necessary to comply with such directive.

On the other hand, Law No. 34/2002 of 11 July 2002 on Information Society Services and Electronic Commerce (hereinafter “the E-commerce Act”) establishes the liability regime applicable to the intermediation activities carry out by Internet Service Providers (“ISP”) that applies to platform providers. The E-commerce Act states that linking and hosting ISP will not be liable for the information to which they direct or host if: (i) they do not have actual knowledge that the information is unlawful and (ii) they do have knowledge that the information is unlawful and act diligently to remove or disable the content.

This said, the recently adopted Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market (hereinafter “Copyright Directive”) puts more direct responsibility on platforms to make sure that copyright infringing content is not hosted on their sites. Specifically, Article 17 of the Copyright Directive states that online content sharing service providers (category in which YouTube or Facebook would fall) shall obtain from license holders a license to publicly communicate the content protected by intellectual property rights that their users upload. In the event that it does not have the corresponding license, the platform must adopt measures to prevent the infringing contents from being available in it, which in practice will involve resorting to content recognition technologies. This has been one of the most controversial issues of the Copyright Directive, therefore we will have to wait and see how it is develops in practice and its implementation by Member States, which will have until 21, June of 2021 to do so.

In addition, there are other measures that will probably be implemented at European level in the following months regarding the monitoring of content online that will affect platform providers. For example, there is a UE regulation proposal called “preventing the dissemination of terrorist content online” that would force platforms to remove terrorist content in one (1) hour; otherwise they could face huge economic penalties.

Finally note that there are other regulations that indirectly affect platform providers. For example, a platform provider whose services fall within the scope of Regulation (EU)
2017/1128 on cross-border portability of online content services in the internal market shall comply with the obligations underlined in such regulation, which mainly consist in enabling a subscriber who is temporarily present in a Member State to access and use the online content service in the same manner as in the Member State of residence, including by providing access to the same content, on the same range and number of devices, for the same number of users and with the same range of functionalities.

6. If so, does the reach of the regulator extend outside your jurisdiction?

Yes. The E-commerce Act, in addition to ISP(s) domiciled/resident or with a permanent establishment in Spain applies to:

a) ISP(s) established in another Member State or the European Economic Area (“EEA”) when the services recipient is located in Spain and those affect one of the following matters: intellectual property, rights, advertising emission by investment institutions, insurances activities, consumers, applicable law, legality of email commercial communications; and

b) ISP(s) established outside the European Union or EEA provided that they directly offer their services to Spain except when it contravenes applicable international treaties.

Therefore platform providers not domiciled (or without permanent establishment) in Spain complying the requirements above and that infringe the E-commerce Act provisions might respond before the Spanish Court/regulator provided. For example, in case of intellectual property third party right’s infringements, the Second Section of the Intellectual Property Commission of the Ministry of Culture (“Sección II de la Comisión de Propiedad Intelectual”) will be the main body responsible for carrying out the proceeding of removing or blocking online content against non-compliance platform providers.

7. Does a telecoms operator need to be domiciled in the country?

Any natural or legal person from or established in the European Union can provide ECS or ECN in Spain. Companies registered in non-EU or European Economic Area countries can only enter the telecoms market and provide services in Spain through bi- or multi-lateral agreements, conventions or treaties to which both countries are party. In addition, the Spanish government is free to make any exceptions to these rules and can grant direct authorisations.

Among other things, a foreign operator not belonging to the EU would need to present a certificate issued by the respective Spanish diplomatic representation stating that they are listed in their local professional, commercial or similar register or, failing that, that they act legally and regularly in the scope of the corresponding activities. Furthermore, they must also point out in their notification the international agreement enables them to operate networks or provide electronic communications services in Spain or, otherwise, provide the agreement from the Council of Ministers which authorises such documentation in exceptional circumstances.
8. **Are there any restrictions on foreign ownership of telecoms operators?**

   Please see Question 2.

9. **Are there any regulations covering interconnection between operators?**

   Yes. First of all, please note that, in accordance with Article 3.c of the Spanish Telecommunications Act, one of the objectives is precisely “to promote the deployment of networks and the provision of electronic communications services, fostering end-to-end connectivity and interoperability and access, on conditions of equality and non-discrimination”. In this sense, Article 12 of the Spanish Telecommunications Act (in line with Article 4.1 of the EU Access Directive 2002/19/EC) states that operators of public electronic communications networks shall have the right and, when requested by other electronic communications network operators, the obligation to negotiate mutual interconnection for the purpose of providing publicly available electronic communications services, with the aim of thereby ensuring the provision and interoperability of services.

10. **If so are these different for operators with market power?**

    Yes. Article 14 of the Spanish Telecommunications Act states that the CNMC may impose on operators with significant market power certain specific obligations, which include amongst others:

    - Transparency obligations; according to which operators may be required to publish information relating to accountability, technical specifications, network characteristics, supply conditions, and/or the publication of a reference offer etc.;
    - Non-discrimination obligations; according to which operators may be required to apply equivalent conditions in similar circumstances to other operators that provide equivalent services and provide third parties with services and information of the same quality as those provided for their own services or those of their subsidiaries or associated and in the same condition;
    - Other obligations include the separation of accounts, access to specific elements or resources from the network as well as other related services as identity, location and presence services, pricing control, etc.

11. **What are the principal consumer protection regulations that apply specifically to telecoms services?**

    Most important piece of legislation concerning end user’s rights is Royal Decree 899/2009, of 22 May 2009, which approves the Charter of rights of telecommunication services users.

    The following parts of regulations are also applicable specifically to telecom consumers:
12. **What legal protections are offered in relation to the creators of computer software?**

Computer software is regulated by the Spanish Intellectual Property Act 1/1996 (hereinafter “the Intellectual Property Act”). The protection given by the Intellectual Property Act is provided not only for computer software, which is defined as any sequence of instructions or data intended for either direct or indirect use in a data processing system to perform a function or task or to secure a specific result, regardless of its form of expression and recording, but also for the preparatory documentation, technical literature and manuals for the use of the program.

Article 97 of the Intellectual Property Act regulates the holding of computer software rights and provides the following rules:

- The individual or group of individuals that has created a computer program, or the legal person deemed the copyright holder, shall be deemed the author thereof.
○ If the computer program is a collective work, unless otherwise agreed, the individual or legal person who published and makes the computer program available under his/her name shall have the status of author.
○ If the computer program is a collaborative work made by two or more authors, they shall be joint owners of the program and it shall pertain to all of them in the proportions determined by them.
○ Where the computer program is created by an employee in the execution of his/her duties or following the instructions given by his/her employer, the ownership of the relevant exploitation rights in the computer program so created, including both the source program and the object program, shall pertain exclusively to the employer, unless otherwise provided by contract.

Regarding the term of protection provided by the Intellectual Property Act, the duration of these intellectual property rights depend on the specific owner of the rights:

○ Where the author is an individual: copyright shall run for the life of the author and for 70 years after his/her actual or declared death.
○ Where the author is a legal person: copyright shall run for 70 years counted from the 1st January of the year following that of the lawful communication of the program or that of its creation if it has not been made available to the public.

13. Do you recognise specific intellectual property rights in respect of data/databases?

Yes, data bases are granted with two specific types of protection according to the Intellectual Property Act:

- Protection provided due to their structure and form of expression:

Article 12 of the Intellectual Property Act provides protection for collections of the works of others or of data or of other independent elements, such as anthologies and databases, which, by reason of the selection or arrangement of their contents, constitute intellectual creations, without prejudice to any rights that might exist in such content. This protection shall solely apply to their structure, meaning the form of expression of the selection or arrangement of their contents, but shall not extend to those contents. Collections of works, data or other independent elements systematically or methodically arranged and individually accessible by electronic or other means shall be deemed to be databases.

- Protection provided due to the substantial investment in the database (sui generis right):

Article 133 of the Intellectual Property Act protects the substantial investment, assessed either qualitatively or quantitatively, made by its manufacturer in the form of finance, time, effort or energy or other means of similar nature spent in the obtaining, verification or presentation of its contents. By the protection provided through this article, the manufacturer of a database may prohibit:
a) the extraction and/or re-utilisation of all or a substantial part of the contents thereof, evaluated qualitatively or quantitatively, provided that obtaining, verification or presentation of such contents represents a substantial investment in terms of quantity or quality; and/or

b) the repeated or systematic extraction and/or re-utilisation of insubstantial parts of the contents of a database implying acts that conflict with normal exploitation of that database or unreasonable prejudice towards the legitimate interests of the manufacturer of the database.

The sui generis rights shall apply regardless of whether or not such database is vested with other intellectual property rights and without prejudice to any rights existing within their contents. Therefore, the same database can be protected both by Article 12 and Article 133 of the Intellectual Property Act in case its structure, meaning the form of expression of the selection or arrangement of their contents can be considered as “original” (Article 12) and in case of the database’s obtainment, verification or presentation has constituted a substantial investment for the database manufacturer (Article 133).

14. **What key protections exist for personal data?**

In Spain, until 25 May 2018, personal data has been regulated under Organic Law 15/1999, of 13 December 1999, on the Protection of Personal Data (“LOPD”) and Royal Decree 1720/2007, of 21 December 2007, that approves the implementation of Regulation of the LOPD (“RLOPD”). Since the 25 May 2016, the GDPR has partially de-regulated both the LOPD and the RLOPD and is now the main regulation that sets out how personal data shall be processed in Spain. A new Spanish data protection act, which implements and complements the GDPR, was adopted on December 2018; the LOPDGDD.

The GDPR lays down many obligations for companies that process personal data within the EU and/or personal data of EU nationals. In general terms, under the GDPR personal data shall be processed in accordance with the data protection principles (“lawfulness, fairness and transparency”); collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes; adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”). Other obligations include the need to satisfy the data protection rights of data subjects, to notify the Spanish Data Protection Supervisory Authority (Agencia Española de Protección de Datos, in Spanish or “AEPD”) of personal data breaches, the need to have in place a record of processing activities, the obligation to adopt appropriate security measures or the need to respect the restrictions for international transfers of personal data.

15. **Are there restrictions on the transfer of personal data overseas?**

⊙ The EU Commission has decided that the country from which the company importing the data offers an adequate level of data protection. Currently the EU Commission has stated that the following countries provide such an adequate level: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New
Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework); or
  - The data controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. In practice this means that where the data exporter and the data importer adopt contractual safeguards (such as entering into the Standard Contractual Clauses published by the EU Commission or Binding Corporate Rules), the transfer of personal data will be deemed lawful; or
  - One of the de-regulations foreseen by Article 49 of the GDPR applies to the transfer. These include the consent of the affected individuals, the need to ensure the adequate enactment of a contract with the data subject, the need to establish, exercise or defend legal claims or the need to protect a vital interest of a data subject.

16. **What is the maximum fine that can be applied for breach of data protection laws?**

The fines imposed under the LOPDGDD follow the same criteria as the GDPR, and it establishes three different types of infringements (minor, serious and very serious). Under the GDPR maximum fines for infringements can be up to 20,000,000 EUR, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever amount is higher. This maximum fine would only be imposed for the breach of certain obligations under the GDPR, such as infringing the data protection principles, not observing the restrictions for international data transfers or failing to satisfy the rights of the data subjects.

On the other hand, persons who have suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered. The total amount that will have to be paid for an infringement that resulted in damages would ultimately depend on those damages, which will be decided by a court. A company may be required to pay a fine as well as compensation to the data subjects.

17. **What additional protections have been implemented, over and above the GDPR requirements?**

The LOPDGDD has recognized a new catalogue of digital rights to protect people using different digital tools in order to avoid discrimination; it includes net neutrality, universal internet access, digital security, digital literacy, the online protection of minors, the amendment or updating on information online, the right to be forgotten on search engines and social networks, and the regulation of the right to a digital will. Additionally, it strengthens the privacy of employees and their right to digital disconnection, and privacy during the use of digital services, video surveillance and geolocation in the workplace. Articles 80 to 96 of the LOPDGDD set out 16 Digital Rights:

1. **Right to Internet neutrality**: internet service providers shall provide a transparent offer of services without discrimination on technical or economic grounds.
2. **Right of universal access to Internet**: everyone has the right to access the Internet
regardless of personal, social, economic or geographical status. Under this right, universal, affordable, quality and non-discriminatory access for the entire population is guaranteed.

3. **Right to digital security**: users have the right to the security of the communications they transmit and receive over the Internet. In addition, Internet service providers shall inform users of their rights.

4. **Right to digital education**: all educational plans must now include modules for learning to use new digital technologies. The use must be safe and respectful of human dignity, constitutional values, fundamental rights and, in particular, respect for and guarantee of personal and family privacy and the protection of personal data. The law refers to the fact that university studies should also train students in the use of digital media. In addition, it stresses that public administrations must include in the competitions specific tests to evaluate their use, as well as on data protection when employees perform functions that involve access to personal data.

5. **Online protection of minors**: families and guardians shall ensure that minors make balanced and responsible use of digital devices in order to ensure the proper development of their personality and preserve their dignity and fundamental rights.

6. **Right of rectification on the Internet**: those responsible for social networks and equivalent services will adopt appropriate protocols to enable the exercise of the right of rectification for users who disseminate content that undermines the right to honour, personal and family privacy on the Internet and the right to freely communicate or receive truthful information, in accordance with the requirements and procedures set out in the law.

7. **Right to update information in digital media**: data subjects have the right of requesting the digital media to include a sufficiently visible update notice next to the news that concerns them. This amendment should be made when, as a result of events occurring after the publication of the news item, it no longer reflects the current situation causing harm to the subject. In this regard, the law makes particular reference to judicial decisions that alter previous ones.

8. **Right to privacy and use of digital devices in the workplace**: it recognizes the privacy of employees during the use of electronic devices provided by their employer.

9. **Right to digital disconnection in the workplace**: the purpose of this right is to ensure that employees, outside legally or conventionally established working time, respect their time for rest, leave and holidays, as well as their personal and family privacy.

10. **Right to privacy from the use of video-surveillance and sound recording devices in the workplace**: microphones may be installed only when the risks to the safety of installations, goods and persons arising from the activity taking place in the workplace are relevant. In addition, under no circumstance it is allowed the installation of video-surveillance systems in changing rooms, toilets, dining rooms or places intended for the entertainment of employees.

11. **Right to privacy when using geolocation systems in the workplace**: employers may use geolocation systems to check the location of their employees, provided that employees and their representatives are informed about the existence and characteristics of these devices.
12. **Digital rights in collective bargaining:** it is recognised the right for collective agreements to establish additional guarantees of the rights and freedoms related to the processing of employees personal data and the safeguarding of digital rights in the workplace.

13. **Data protection of minors on the Internet:** educational establishments and any person who publishes minors’ personal data through social networks or similar services, it is necessary to obtain the consent of the minor or his or her legal representatives.

14. **The right to be forgotten on search engines and social networks:** everyone has the right to obtain the deletion of personal information when it has become inadequate, inaccurate, irrelevant, out of date or excessive.

15. **Portability rights in social network and equivalent services:** the right to transfer content and personal data from one social network to another automatically.

16. **Right to a digital will:** persons linked to the deceased will be able to access social networks, e-mail or instant messaging services such as WhatsApp, as well as to modify or delete the information they contain. They may also decide to delete the profile.

In addition to these digital rights, the LOPDGDD gave political parties, coalitions and electoral groups the power to use data obtained through technological means to send electoral propaganda electronically or messaging systems such as WhatsApp. This possibility was appealed before the Constitutional Court by the Ombudsman. As a consequence, the Spanish Data Protection Supervisory Authority issued a circular which states that, before they begin to process data, parties should submit to the AEPD, 14 weeks before the start of the election campaign, documentation specifying what measures they will take to assess the impact of data collection and mitigate risks.

Finally, regarding personal data related to minors, the GDPR confers to the Member States the option of establishing a lower age than 16 to obtain valid consent and no less than 13 years. The LOPDGDD foresees in its Article 7 that the processing of personal data of a minor may only be based on his or her consent if he or she is over 14 years of age.

18. **Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?**

The Spanish legislation does not foresee specific restrictions or limitations for cloud-based services. However, where the use of cloud-based services entails the processing of personal data, the requirements of the data protection legislation will have to be complied with. In general terms, the GDPR will require companies using such services to:

- Certify that when processed in the cloud-based platform, the personal data are processed in accordance with the data protection principles set out in the GDPR.
- Ensure that the use of such services complies with the requirements laid down by the GDPR for international data transfers (especially relating to where the cloud service provider is located, or where data are hosted in countries that are located outside the EEA).
- Ensure that the relationship with the service provider is regulated under a written
agreement that provides the mandatory provisions required by Article 28 of the GDPR, which sets out the requirements for the relationship between data controllers and data processors.

- Guarantee that the affected data subjects can exercise the rights recognised under the GDPR for the data stored in the cloud.
- Guarantee that the cloud-based service is subject to appropriate technical and security measures that prevent personal data from being lost, altered or accessed by unauthorised personnel.

19. **Are there specific requirements for the validity of an electronic signature?**

Currently, the Spanish E-signature regulatory framework is composed by: (i) EU Regulation Number 910/2014 on electronic identification and trust services for electronic transactions in the internal market (“eIDAS Regulation”) and (ii) Spanish Law 59/2003 on Electronic Signatures (“E-Signature Act”). Even though the E-Signature Act has not been formally repealed yet, most doctrine considers it applicable to any matters not regulated by the eIDAS Regulation and/or that do not contradict the provisions of the eIDAS Regulation.

In light of the above, there are three types of e-signatures:

- Simple electronic signature, that is data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
- Advanced electronic signature, that is an electronic signature which meets several legal requirements, for example, is uniquely linked to the signatory or capable of identifying the signatory.
- Qualified electronic signature, that is an electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures. Qualified e-signatures must be validated through the fulfilment of several requirements according to the law.

The above types of e-signature must comply with different requirements. In general, electronic contracts will be binding, whatever the form under which they have entered into, provided that they comply with the contract requirements under Spanish law, which are: consent; a certain object; and cause of the obligation.

Most transactions do not require e-signatures. In principle, there are no limitations applicable to the use of e-signatures but only a qualified electronic signature satisfies the legal requirements of a signature in the same manner as a handwritten signature.

This said, in April 2018 a Spanish draft bill regulating certain aspects of “Trust Electronics Services” was issued and this is expected to formally repeal the E-Signature Act. This new law will develop certain aspects of Trust Electronic Services not covered by the eIDAS Regulation and so, once in effect, the Spanish E-signature regulatory framework will be
composed of: (i) the eIDAS Regulation (Advance E-electronic signatures will be mostly regulated by this EU Regulation) and (ii) the new law on certain aspects of “Trust Electronics Services”.

20. **In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?**

No, employees, assets or contracts are not normally automatically transferred in the event of an outsourcing of IT services. The parties involved in the provision of outsourcing services need to negotiate how the services are structured and the resources (employees, assets) to be managed. A mere provision of services with no transfer of a business unit, does not in principle entail a transfer of any resources.

Concerning the possible transfer of employees involved in an IT outsourcing, the most important point to consider is that for the employees to transfer automatically to the outsourcing supplier as per Article 44 of the Spanish Statute of Employees (Royal Decree 2/2015, of October 23), the principal must transfer its own IT production unit (i.e. including all the assets, agreements etc.) as a whole, autonomous business unit. Otherwise, if the IT production unit is not entirely transferred by the principal to the supplier, the employees would not transfer automatically to the supplier and would remain employees of the principal.

Finally, note that the outsourcing supplier must provide its services with its own resources and organisation, in order to avoid the declaration of an illegal transfer of employees, prohibited by Article 43 of the Spanish Statute of Workers.

21. **If a software program which purports to be a form of A.I. malfunctions, who is liable?**

For the time being, there is no specific Artificial Intelligence regulation in Spain. Notwithstanding the above, on 10 April 2018, 25 European Union Member States, including Spain, signed a Declaration of Cooperation on Artificial Intelligence. Consequently, the European Commission will now work with Member States on a coordinated plan.

On June 2018 the European Commission appointed experts to build a new High Level Group on Artificial Intelligence, who will be in charge of making recommendations on how to approach these innovative techniques. The European Commission has taken many initiatives to regulate liabilities arisen from Artificial Intelligence, among others; it has issued the Commission Staff Working Document about Liability for emerging digital technologies dated on April 25, 2018 or the Ethics Guidelines for Trustworthy Artificial Intelligence, dated on April 8, 2019.

Europe wants to be at the forefront of these developments and therefore its intention is to enact a legal framework that the continent can meet together for artificial intelligence to
succeed and work for everyone.

In light of the above, as Spain has not any specific Artificial Intelligence responsibility framework, current software provisions will generally apply to early forms of Artificial Intelligence malfunctions, being the software developer entity generally found liable for the malfunction of the program.

22. **What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?**

Please note that Spain has a complex network of laws that aim to cover the various situations involving cybersecurity. As the study and analysis of cybersecurity is essential to ensure adequate protection of companies, institutions and citizens, a Law Code for Cybersecurity was published by the Spanish Official Gazette (“BOE”) in 2016 outlining the main laws impacted by cybersecurity. This code is regularly updated by the National Institute of Cybersecurity (“INCIBE”) and can be accessed here: https://www.boe.es/legislacion/codigos/codigo.php?id=173&nota=1&tab=2

a) obligations as to the maintenance of cybersecurity; and

There are two main pieces of regulation in terms of maintenance of cybersecurity:

- **The NIS RD.** This Royal Decree implements EU Directive 2016/1148 in Spain. It concerns certain measures for achieving a common high level of security for network and information systems across the Union (NIS Directive), and is regarded as a key element in Spain’s regulatory framework for cybersecurity. Through the enactment of the NIS RD, important security obligations are established for operators of essential services and digital services providers, as well as a system for the notification of incidents.

- **Law 8/2011, of 28 of April on Critical Infrastructures.** This law defines Critical Operators as those entities responsible for the investments or the daily operation of an installation, network, system, or physical equipment or information technology designated as critical infrastructure. According to this law, critical infrastructures are those strategic infrastructures whose operation is essential and does not allow alternative solutions, so that their disruption or destruction would have a serious impact on essential services. This law also defines strategic infrastructures as those facilities, networks, systems and physical equipment and information technology on which the operation of essential services rests. Amongst other obligations, Critical operators have the obligation to develop an Operator Security Plan (“OSP”) or (if required by subsequent regulation) a Specific Security Plan for each of the Infrastructures considered critical. OSP are the strategic documents that define the general policies of the Critical Operators to guarantee the security of all the facilities or systems under their ownership or management.

b) the criminality of hacking/DDOS attacks?
The Spanish Criminal Code (Organic Law 10/1995) includes the so-called “computer-related crimes”. Whether an act of hacking falls within one of the types of crime will depend on the circumstances of the case. However, most of hacking actions would fit into Article 197 of the Spanish Criminal Code that regulates the illegality of obtaining data from third parties through unauthorized entry into computer servers.

23. **What technology development will create the most legal change in your jurisdiction?**

Many digital technology trends will require the enactment of specific laws, otherwise our current legal system will be applied analogically to regulate these new legal trends. It is no secret that Artificial Intelligence and its derivatives would preferably need a specific regulation not only as regards its ethical use but also information obligations, liabilities etc. Also the regulation of blockchain (and/or cryptocurrencies) is also to be considered one of the most challenging legal changes that must be faced in order to totally secure all transactions and products based upon such technology. In February 2018, the Banco de España (Spanish Banking Authority) and the National Securities Market Commission (Comisión Nacional del Mercado de Valores, in Spanish o “CNMV”) issued a joint declaration about “cryptocurrencies”. In this declaration both bodies declared that “cryptocurrencies” are not regulated in the European Union. This implies that if a person buys or keeps “cryptocurrencies”, he/she does not benefit from the guarantees and safeguards associated with regulated financial products. Additionally, both entities also argued that on many occasions the different actors involved in “cryptocurrencies” businesses are located in different countries, so that the resolution of any conflict could be outside the competence scope of the Spanish authorities and would be subject to the regulatory framework of the country in question, which may be a problem for the person acquiring these products.

It is also to be noted that the Royal Decree Law 19/2018 of November 23, on payment services and other urgent financial measures, which has transposed the Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market (Payment Services Directive or “PSD2”) into the Spanish legal system, does not expressly consider cryptocurrencies as payment methods. Hence, transactions made by blockchain technology, including but not limited to financial transactions, would be one of the biggest legal changes not only for Spain but also for the European Union.

Additionally, 3D and 4D printing technology will have a huge impact on many fields, as it could imply a substantial change to the implementation of intellectual property and health regulations. In Spain 3D printing technology has been used in the food, architectural or clothing industries, where lot of start-ups are becoming specifically focused on 3D printing technology, whereas 4D printing technology has been tested and issued in the field of health. Certainly this technology will have to be regulated in order to protect everyone’s rights as this printing technology must be controlled in order not to breach third parties’ rights and to not create products which are subject to authorisations in Spain or even illegal items.
24. **Which current legal provision/regime creates the greatest impediment to economic development/commerce?**

In relation to data protection matters, it is important to highlight that the AEPD is quite active in opening up investigation proceedings. In this sense, the AEPD has recently publicly stated that its enforcement actions will be focused on the health and telecommunication sectors.

Also, the PSD2 will require online platforms operating as central portals that, acting as intermediaries, enable payment transactions between buyers and sellers and entering into possession of the funds – without themselves selling the product or service – to obtain an authorisation as a “payment service provider” from the relevant authority, which in Spain is the *Banco de España*.

This would mean that marketplaces such as Amazon or eBay may be required to obtain an authorisation and may not be exempted anymore, as they were under PSD1 (Directive 2007/64/EC of 13 November 2007 on payment services in the internal market), if they wish to continue providing this “payment service” to buyers and sellers.

25. **Do you believe your legal system specifically encourages or hinders digital services?**

The Spanish legal system enacts laws according to the European Union legal system. Therefore, most of the Spanish regulations have been harmonised according to European Union law. We do not believe our system differs much from others in the EU in this respect.

26. **To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?**

Spain has not provided a specific legal framework applicable to artificial intelligence yet but, as explained above, on 10 April 2018, Spain signed a Declaration of Cooperation on Artificial Intelligence, as Artificial Intelligence will be approached from a European Union law perspective. Also, on March 4, 2018, the Government presented the Spanish RDI Strategy in Artificial Intelligence, which will be the basis for the future National Artificial Intelligence Strategy, which will allow for the coordination and alignment of national investments and policies. The strategy emphasizes as a priority the implementation of ethical principles applicable to artificial intelligence, including the drafting of an Artificial Intelligence Code of Ethics.

Regarding autonomous vehicles, Spain is doing its best to regulate driverless cars circulation through a “XXI Traffic Act”. Nowadays, although there is still no law which specifically regulates autonomous vehicles in Spain and autonomous vehicles are currently governed by the broader regulatory framework that is applicable to vehicles, since 2015 there is an
instruction (Instruction 15/V-113) issued by the Spanish General Directorate of Traffic related to the granting of special authorisations for the testing of such vehicles in Spanish public roads.