THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FIFTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Fifth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2018
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

SENIOR ACCOUNT MANAGER
Pere Aspinall

ACCOUNT MANAGERS
Jack Bagnall, Sophie Emberson, Katie Hodgetts

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Keavy Hunnigal-Gaw

EDITORIAL COORDINATOR
Thomas Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-912228-62-1

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

BTS&PARTNERS

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

M&M BOMCHIL

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 22

SPAIN

Leticia López-Lapuente and Reyes Bermejo Bosch[1]

I OVERVIEW

Data protection and privacy are distinct rights under Spanish law, but both are deemed fundamental rights derived from respect for the dignity of human beings. They are primarily based on the free choice of individuals to decide whether to share with others (public authorities included) information that relates to them (personal data) or that belongs to their private and family life, home and communications (privacy). Both fundamental rights are recognised in the Lisbon Treaty (the Charter of Fundamental Rights of the European Union) and the Spanish Constitution of 1978. Data protection rules address, *inter alia*, security principles and concrete measures that are helpful to address some cybersecurity issues, in particular, because specific cybersecurity legislation (which not only covers personal data and private information but rather any information) is new and not sufficiently developed yet.

Spain had an omnibus data protection framework law along the lines of the EU approach (mainly Law 15/1999 of 13 December on the Protection of Personal Data (the DP Law), as developed by Royal Decree 1720/2007 of 21 December (RD 1720/2007), jointly the DP Regulations), applying both to the private and public sectors. In addition, there are certain sector-specific regulations that also include data protection provisions.

The General Data Protection Regulation (GDPR) has not automatically repealed the DP Regulations; however, the DP Regulations remain in force only to the extent that they do not contravene the GDPR. For this reason, a new draft data protection law (the Draft Bill) is currently under discussion in the Spanish parliament that will provide for local rules and administrative proceedings adapted to the GDPR. Approval of the Draft Bill is expected by the end of 2018.

In addition, some personal data and or some processing activities may require specific protection such as certain financial, e-communications or health-related data or processing activities. There are several codes of conduct for data protection that were approved under former legal regime (i.e., the DP Regulations) in various sectors but, in general, they merely adjusted the general obligations to the specific needs of the corresponding sector or organisation. These codes will have to be reviewed pursuant to the GDPR.

The rights to data protection and privacy are not absolute and, where applicable, must be balanced with other fundamental rights or freedoms (e.g., freedom of information or expression) as well as other legitimate interests (e.g., intellectual property rights, public security and prosecution of crimes).

1 Leticia López-Lapuente and Reyes Bermejo Bosch are lawyers at Uría Menéndez Abogados, SLP.

In the case of data protection, this balance must be assessed by the organisation and could be challenged before the Spanish Data Protection Authority (DPA), which is in charge of supervising the application of the regulations on data protection (see Section III.i). Privacy infringements must be claimed before the (civil or criminal) courts.

The DPA was created in 1993, and has been particularly active in its role of educating organisations and the general public on the value of data protection and of imposing significant sanctions. In 2017 alone, the DPA received 10,651 claims from individuals and authorities, and issued and published 852 sanctioning resolutions within the private sector. These sanctions are published on the DPA's website, which is used by the media (and others) as an important source of data protection information. However, as a consequence of the GDPR's approval, the DPA is reviewing the contents to be published on its website (www.aepd.es) and it is likely that a significant part of the resolutions issued in the past will be removed from the website.

II THE YEAR IN REVIEW

In November 2017, the Draft Bill was published and submitted to the parliament for discussion and approval. This has been the most relevant milestone on data protection in Spain over the course of the past year. The initial wording of the Draft Bill has been subject to more than 300 proposed amendments by the different parliamentary groups and, thus, the draft is expected to change. Its approval is not expected until the end of 2018. Regarding the implementation of the Security of Network and Information Systems Directive (the NIS Directive), the Spanish government published a draft royal decree (see Section IX) that has not yet been sent to the parliament for discussion and approval.

Finally, as a consequence of the *Google Spain v. Costeja (Google Spain)* case in 2014 before the Court of Justice of the European Union (CJEU) (regarding the 'right to be forgotten'), the DPA has continued to initiate certain proceedings on this matter; several judicial rulings of relevance on a national level (mainly from the Spanish Supreme Court) have been issued in Spain modulating the scope of the 'right to be forgotten'. In this regard, more recently, on 4 June 2018, the Spanish Constitutional Court has issued its first ruling regarding the scope and nature of the 'right to be forgotten' (see Section VII.ii). The relevance of this ruling is that the Spanish Constitutional Court has recognised that the 'right to be forgotten' has an independent nature from the data protection rights.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The legal framework for the protection of personal data in Spain is regulated by the Lisbon Treaty; Article 18(4) of the Spanish Constitution; the GDPR and, until approval of the Draft Bill, by those provisions of the DP Regulations that are compatible with the GDPR.

Sector-specific regulations may also contain data protection provisions, such as the E-Commerce Law 34/2002 (LSSI), the General Telecommunications Law 9/2014 (GTL), anti-money laundering legislation or the regulations on biomedical research. However, they generally refer to the DP Regulations and, now that the GDPR is in force, will either be subject to review or should at least be reinterpreted according to GDPR rules.

Privacy rights are mainly regulated by the Spanish Constitution, Law 1/1982 of 5 May on civil protection of the rights to honour, personal and family privacy, and an individual's own image, and by the Spanish Criminal Code.

Personal data and private data are not synonymous. Personal data are any kind of information (alphanumeric, graphic, photographic, acoustic, etc.) concerning an identified or identifiable natural person, irrespective of whether or not this information is private. However, data regarding ideology, trade union membership, religion, beliefs, racial origin, health or sex life as well as criminal and administrative offences are deemed more sensitive and require specific protection.

Protecting personal data is achieved by allocating specific duties to both 'controllers' (i.e., those who decide on the data processing purposes and means) and 'processors' (i.e., those who process the data only on behalf of a controller to render a service).

The DPA is the entity in charge of supervising compliance with the data protection duties imposed by the GDPR and DP Regulations (fair information, legitimate ground, security, notification, proportionality and quality, etc.).[2] The DPA has carried out *ex officio* audits of specific sectors (including online recruitment procedures, TV games and contests, hotels, department stores, distance banking, hospitals, schools, webcams and mobile apps). However, the DPA's activity in terms of individual compliance investigations has significantly increased over the past 10 years, as has the number of fines imposed. Indeed, failure to comply with the GDPR and DP Regulations may result in the imposition of administrative fines depending on the severity of the offence (and regardless of whether civil or criminal offences are also committed, if applicable). Neither harm nor injury is required (i.e., the infringement itself suffices for the offender to be deemed liable), but the lack of any harm or injury is considered an attenuating circumstance to grade the amount of the administrative fine. However, harm or injury will be required to claim damages arising from breaches of data protection rights before civil and criminal courts.

ii General obligations for data handlers

Since the Draft Bill has not been approved, the main obligations of data controllers and data processors are those set out in the GDPR.

Obligations of data controllers

a Any processing activity should be internally monitored and, in certain cases, duly registered and documented;

b data subjects from whom personal data are requested must be provided beforehand with information about the processing of their personal data (the DPA has published specific guidelines to comply with the GDPR rules on information duties);

c the processing of personal data must be based on a legitimate ground, among others, have the prior and explicit consent of the data subject, be based on the existence of a contractual relationship that makes the processing unavoidable, the existence of a legal obligation imposed on the controller or a legitimate interest;

2 The data protection right is enforced by the DPA at a national level with limited exceptions. For example, Catalonia and the Basque country are regions that have regional data protection authorities with competence limited to the processing of personal data by the regional public sector.

d when the recipient is not located in the EU or EEA (or in a country whose regulations afford an equivalent or adequate level of protection identified by the European Commission or the DPA), appropriate guarantees must be adopted, unless a legal exemption applies;

e controllers should adopt appropriate security measures, as explained in Section IX; and

f data subjects have a right to access all data relating to them, to rectify their data and have their data erased if the processing does not comply with the data protection principles, in particular, when data are incomplete, inaccurate or excessive in relation to the legitimate purpose of its processing. Data subjects are also entitled to object to certain processing activities that do not require their consent or are made for direct marketing purposes, as well as to request the restriction of processing and the portability of their data.

Obligations of data processors

Data processors must:

a execute a processing agreement with the relevant data controller;

b implement the above-mentioned security measures;

c process data only to provide the agreed services to the controller and in accordance with its instructions;

d keep the data confidential and not disclose it to third parties (subcontracting is not prohibited but is subject to specific restrictions); and

e upon termination of the services, return or destroy the data, at the controller's discretion.

In addition to the above, the GDPR has added specific mandatory content for a processing agreement to be valid (as provided by Article 28.3 of the GDPR) including the duty to provide assistance to the controller in the event of data breaches or the duty to allow audits to its processing of data. Since the duties under the GDPR became applicable as from May 2018, the DPA has published specific guidelines on how to comply with the GDPR rules regarding processing agreements.

iii Specific regulatory areas

The DP Regulations apply to any personal data, but they provide for reinforced protection of data related to children (e.g., the verifiable consent of the minor's parents is required) and to certain categories of especially protected data, such as health-related data (e.g., they may require the performance of a privacy impact assessment). Under local laws (i.e., the DP Regulations) specific rules also apply to the information processed by solvency and credit files, and to the processing of data for video surveillance or access control purposes. Some of these matters are proposed to be specifically regulated also in the Draft Bill and, thus, the final version of the Draft Bill will be highly relevant for these processing activities.

In addition, certain information is also protected by sector-specific regulations. This is the case for, *inter alia*:

a financial information that is subject to banking secrecy rules (Law 10/2014 of 26 June 2014 on the regulation, supervision and solvency of credit institutions);

b the use (for purposes other than billing) and retention of traffic and location data (GTL);

c the sources of information and intra-group disclosures to comply with regulations concerning anti-money laundering and combating the financing of terrorism, and restrictions on the transparency principle in relation to data subjects (Law 10/2010 of 28 April on the prevention of money laundering and financing of terrorism);

d the use of genetic data or information contained in biological samples (Law 14/2007 of 3 July on biomedical research);

e information used for direct-marketing purposes (LSSI);

f the outsourcing of core financial services to third parties (Royal Decree 84/2015 of 13 February developing Law 10/2014, and Bank of Spain Circular 2/2016 on the supervision and solvency of credit institutions, which adapts the Spanish legal regime to EU Directive 2013/36/EU and EU Regulation 575/2012); and

g the use of video-surveillance cameras in public places (Law 4/1997 of 4 August governing the use of video recording in public places by state security forces).

Since the above regulations generally refer to the DP Regulations and after May 2018 they will need to be reviewed according to the GDPR or, at least, reinterpreted according to GDPR rules.

iv Technological innovation

Technology has created specific issues in the privacy field, including:

a online tracking and behavioural advertising: as a general rule, explicit prior consent is required. The DPA does not generally consider that online behavioural advertising or profiling activities can be based on the existence of a legitimate interest. In addition, the DPA has expressly announced that profiling activities must be considered as separate processing activities from any others, such as advertising ones, and, as such, a specific and separate legal ground must legitimate these activities (e.g., a separate consent);

b location tracking: the DPA considers that the use of this technology in work environments may be reasonable and proportionate and subject to certain requirements (mainly, that specific information has been previously provided to data subjects on the potential monitoring of IT resources);

c use of cookies: as a general rule, explicit prior consent is required for installing cookies or similar devices on terminal equipment. In June 2018 the DPA announced that cookie policies must be adjusted according to the GDPR's requirements and has issued certain guidelines on how banners and privacy policies should be adapted accordingly. In 2017, the DPA initiated 395 investigations and issued 55 sanctioning resolutions regarding Internet services (certain of which included the use of cookies);

d biometrics: traditionally, the processing of biometric data has not been considered 'sensitive' and, therefore, the DPA has made no specific requirements in this area. The implementation of the GDPR in Spain implies a change in the concept of biometrics, which are now considered especially protected data, and we are currently awaiting the DPA's guidelines in this regard;

e big data analytics: in April 2017, the DPA published guidelines on how to implement big data projects according to GDPR rules;

f anonymisation, de-identification and pseudonymisation: the DPA has adopted an official position regarding the use of 'anonymous' data and open data in big data projects.

In particular, the DPA published guidelines at the end of 2016 on the protection of personal data related to the reuse of public-sector information and guidelines on anonymisation techniques;

g internet of things and artificial intelligence: the DPA has not adopted an official position regarding the internet of things and artificial intelligence;

h data portability: the DPA has published a legal report on, among other issues, the data portability right. The DPA stated that the portability right includes not only data subjects' current data, but also their former data (either provided by them or inferred from the contractual relationship); however, the information obtained from the application of profiling techniques (e.g., algorithms) would not be subject to portability. Although the DPA's legal reports are not binding, they are highly useful since they reflect the DPA's doctrinal tendency;

i right of erasure or right to be forgotten: the right to be forgotten in relation to search engines is actively pursued both by Spanish data subjects and the DPA. Notably, *Google Spain*,[3] in which the CJEU's ruling recognised the right to be forgotten, was initiated in Spain and the Spanish DPA had a significant role in the case. There are several DPA resolutions issued every year recognising the right of Spanish individuals to be forgotten and also setting out certain exceptions to the applicability of the right. Recently, the Spanish Constitutional Court, in its ruling dated 4 June 2018, confirmed this approach and has recognised the right to be forgotten as a new fundamental right, different but related to data protection rights; and

j data-ownership issues: to date, there is no Spanish legislation that specifically regulates the question of ownership of data. Notwithstanding this, several regulations exist that may have an impact on data ownership including, among others, data protection legislation, copyright law (which regulates rights over databases) or even unfair competition rules.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

According to the DP Regulations, data transfers from Spain to (or access by) recipients located outside the EEA used to require the prior authorisation of the DPA, unless the transfer could be based on a statutory exemption.[4] Even though these rules, contained in the DP Regulations, have not been formally repealed when the GDPR became applicable in May 2018, these local rules are considered to be incompatible with the GDPR's regime on international transfers of data and, thus, are considered inapplicable. For this reason, GDPR's regime on international transfers is the only regime that applies to transfers in Spain. Also, the Draft Bill that will contain the new data protection law is not expected to include changes to the GDPR's general regime.

Turning to data localisation, there are no specific restrictions in Spain; however, along with the GDPR (which imposes certain restrictions and requirements on disclosing data to non-EU entities), there are specific laws imposing requirements that could be understood as 'restrictive measures', including, among others, tax regulations (Royal Decree 1619/2012 of 30 November on invoicing obligations), gambling regulations (Royal Decree 1613/2011)

3 Case C-131/12.

4 The DPA's prior authorisation is not required in the cases set out in Article 26 of EU Directive 95/46/EC.

and specific public administration regulations (Law 9/1968 of 5 April on secrecy pertaining to official issues, Law 38/2003 of 17 November on subsidies and Law 19/2013 of 9 December on transparency and access to public information).

V COMPANY POLICIES AND PRACTICES

i Privacy and security policies

Organisations that process personal data must comply with the accountability principle and, thus, are required to have both 'general' and 'specific' privacy policies, protocols and procedures. In addition, such policies are useful for (1) complying with the information duties regarding processing activities (see Section III.ii) and (2) complying with the duty to have all employees aware of the applicable security rules since organisations must implement appropriate technical and organisational measures to ensure a level of security that is commensurate with the risk (see Section IX).

Privacy officers

Before May 2018, a chief privacy officer was not mandatory, but in practice this role was deemed crucial for the controller or the processor to comply with the DP Regulations, in particular when the organisation is complex or if the data processed are sensitive or private.

From May 2018, several Spanish data controllers and processors are required to appoint a data protection officer according to Article 37 of the GDPR. Although the Draft Bill of the new data protection law is not definitive, it is expected to expand and detail more the cases in which the appointment of a data protection officer will be mandatory.

Under DP Regulations, the appointment of a security officer was required under certain circumstances but from 25 May 2018, the appointment of this role is no longer mandatory.

Privacy impact assessments

Privacy impact assessments have been mandatory for certain data processing as from May 2018. For this reason, the DPA recently published guidelines on privacy impact assessments. However, the DPA has been encouraging the adoption of privacy impact assessments in certain cases (e.g., big data projects) since 2014 (when it published its first guidelines on the matter). Finally, it must be noted that the Draft Bill also includes a list of cases in which a privacy impact assessment must be carried out (e.g., when the processing involves data subjects in special conditions of vulnerability or when special categories of data are processed and the processing is not merely incidental or accessory).

Work councils

Any employee representative in the organisation is entitled to issue a non-binding report before the implementation of new methods of control of the work. Although it is unclear what qualifies as a 'method of control' of the work, it is advisable to inform the works council of the implementation of new methods (e.g., whistle-blowing systems) and offer their members the possibility of issuing the above-mentioned non-binding report before its implementation.

VI DISCOVERY AND DISCLOSURE

Non-EU laws are not considered, as such, a legal basis for data processing, in particular regarding transfers to foreign authorities and especially if they are public authorities. This approach is consistent with Article 6.3 of the GDPR.

E-discovery and any enforcement requests based on these laws require a complex case-by-case analysis from a data protection, labour and criminal law point of view (and other sector-specific regulations, such as bank secrecy rules).

From a data protection point of view, the Spanish DPA's position is the one adopted by all EU DPAs in the Guidelines on Article 49 of Regulation 2016/679 adopted by the Article 29 Working Party. According to this joint position, data transfers for the purpose of formal pretrial discovery procedures in civil litigation or administrative procedures may fall under derogation of Article 49 of the GDPR. According to the DPAs, this rule of the GDPR can also cover actions by the data controller to institute procedures in a third country, such a commencing litigation or seeking approval for a merger. Notwithstanding this, the derogation cannot be used to justify the transfer of personal data on the grounds of the mere possibility that legal proceedings or formal procedures may be brought in the future.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The DPA is the independent authority responsible for the enforcement of the GDPR and DP Regulations[5] and the data protection provisions of the LSSI and the GTL.

Among other powers and duties, the DPA has powers that include the issuing of (non-binding) legal reports, recommendations, instructions and contributions to draft rules; powers of investigation; and powers of intervention, such as ordering the blocking, erasing or destruction of unlawful personal data, imposing a temporary or definitive ban on processing, warning or admonishing the controller or processor, or imposing administrative fines (fines are only imposed on private-sector entities). The DP Regulations establish three classifications of infringements (and their correlative administrative fines): minor, serious and very serious, resulting in administrative fines ranging from €900 to €600,000 depending on the severity of the infringement. However, this former sanctioning regime, although not officially repealed, was considered incompatible with GDPR rules and, thus, inapplicable from 25 May 2018. Thus, the applicable sanctioning regime under the GDPR did not have a full set of compatible local administrative rules to operate and implement the sanctions. Since this could have caused some formal problems, the Spanish government approved in July 2018 an urgent partial legal reform of sanctioning regime that allows sanctions under the GDPR to fully operate in Spain at least until the Draft Bill is finally passed.

Disciplinary procedures start *ex officio*, but generally stem from a complaint submitted by any person (e.g., the data subject, consumer associations, competitors or former employees).

The DPA is very active: in addition to *ex officio* inspections of specific sectors (always announced in advance), in 2017 (the most recent official statistics published by the DPA): 11,617 complaints from individuals were solved; over 1,200 sanctioning resolutions were

5 See footnote 2.

issued; and the fines imposed amounted to approximately €17.3 million. Most of the sanctions imposed on the private sector were for lack of consent and breach of the quality principle.

ii Recent enforcement cases

The following are the most significant enforcement issues to have arisen in Spain in the period 2017–2018.

The DPA has carried out numerous disciplinary proceedings related to the disclosure of data to solvency and credit agencies (284), to unlawful contracting (131) and unsolicited marketing (124). The DPA has also issued several reports assessing the application of the legitimate interest as a legitimate ground for the processing, including a legal report issued as a response to the Spanish Banking Association's questions on this matter or the Guidelines on how to carry out big data projects.

In addition, the number of proceedings carried out and sanctions imposed by the DPA against non-Spanish and non-EU controllers has also increased. In fact, the DPA is participating in coordinated activities with other EU authorities to investigate companies that are based in the United States but carry out intensive processing activities in the EU.

Finally, the Spanish Constitutional Court has issued a significant ruling (ruling dated 4 June 2018) assessing the scope of the right to be forgotten in a wide manner. In particular, the Spanish Constitutional Court has set out the right to be forgotten may include not only the duty of the internet search engine to remove the relevant links, but also an additional duty of the relevant media or newspaper that initially published the information to remove the personal information from the news in its internal site's search engines. Moreover, this ruling considers the right to be forgotten as a new and separate constitutional right.

iii Private litigation

Data subjects may claim damages arising from the breach of their data protection rights before the civil courts. Claims for civil damages usually involve pecuniary or moral damages, or both, linked to the violation of honour (such as the improper disclosure of private information) and privacy rights (such as the dissemination of private images). In general, indemnities granted to date have been exceptional and have not exceeded €3,000 (with limited exceptions such as one awarding €20,000). Notwithstanding this, recognition under the GDPR of the possibility to initiate class actions related to data protection matters has created a new framework and there are news in the market around the potential initiation by Spanish consumers association of class actions related to data protection alleged infringements.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The application of the DP Regulations for foreign organisations was triggered by either the existence of a data processor or processing equipment in Spain or, according to *Google Spain*, the existence of an establishment in Spain the activity of which is inextricably linked to that of the foreign organisation. Following 25 May 2018, after GDPR rules became applicable, the extraterritorial applicability of EU data protection legal framework is reinforced as a result of the GDPR's territorial scope rules under Article 3.2 of the GDPR.

According to them, offering goods and services to EU citizens and online tracking addressed to the EU or Spanish market may trigger the application of the data protection

provisions not only of the GDPR but also of the LSSI, as well as the consumer regulations (only if consumers resident in Spain are involved), irrespective of where the organisation is established.

IX CYBERSECURITY AND DATA BREACHES

The approval in July 2016 of the NIS Directive was the most significant cybersecurity milestone in recent years. It marks the first instance of EU-wide rules on cybersecurity. The NIS Directive has not yet been implemented into Spanish law, although the government has published a first draft of a law that is consistent with the EU approach. Until implementation occurs, the regulation of cybersecurity matters in Spain will remain diffuse and insufficient, particularly in light of the steady rise in cybersecurity attacks involving Spanish organisations and infrastructure. Furthermore, as a consequence of cybersecurity, the number of cybersecurity certifications has also increased. However, a clear market leader has yet to emerge.

The DPA has also been highly active in relation to cybersecurity matters. Following certain global attacks, the DPA published a post in its website regarding ransomware attacks and how to guard against them. Among other recommendations, the DPA made the following key points: (1) companies should have a complex security plan for the protection of their networks (including a training plan for staff and the continuous updating of all software programs used by the company – especially those used for antivirus purposes); (2) they should have an action plan for how to react in the event of an attack; and (3) they should have a remedial plan to be implemented once the attack is contained.

Also, during 2017 and 2018 the DPA has published other guidelines regarding how to react in the event data breaches including general 'Guidelines on how to manage and notify data breaches' and the 'Guidelines on how to manage an information leakage in law firms'.

As to criminal law, the Spanish Criminal Code was amended in 2010 to implement the Convention on Cybercrime and Council Framework Decision 2005/222/JHA on attacks against information systems. Specifically, this entailed the introduction of two new criminal offences:

a the discovery and disclosure of secrets – namely, the unauthorised access to data or applications contained in an IT system – by any means and infringing implemented security measures; and

b the intentional deletion, damage, deterioration, alteration or suppression of data, applications and electronic documents of third parties rendering them unavailable, as well as the intentional serious hindering or interruption of the functioning of an information system.

Other criminal offences that could be related to cybercrime were also modified (computer fraud, sexual offences, technological theft, and offences against intellectual and industrial property). The Criminal Code was amended again in March 2015. Specifically, aligned with European regulations on computer-related offences, the following new criminal offences are regulated: (1) intercepting data from information systems for the discovery and disclosure of secrets; and (2) creating computer programs or equipment for the purposes of discovering and disclosing secrets or committing damage to IT systems. Finally, legal entities can be held criminally liable for the above-mentioned offences.

Without prejudice to the above, there are no cybersecurity laws and requirements applicable to organisations 'generally', but rather a certain number of rules that address specific cybersecurity issues:

In 2012, the security breach notification regime was introduced in Spain through the GTL in line with Directive 2009/136/EC: the providers of public communications networks or publicly available electronic communications services must notify any security breaches, when personal data are involved, to both the data subjects and the DPA. In March 2014, the DPA approved an online system to notify security breaches. The requirements of the notification itself are those established in EU Regulation 611/2013. Since the notification of data breaches is not mandatory in general (except for the above-mentioned service providers), most of them remain unknown to the DPA and the public. One of those made public was the security breach suffered by BuyVip (which belongs to the Amazon group) in 2011, which involved the names, dates of birth, email addresses, phone numbers and shipping addresses of its customers. Although BuyVip was not subject to a notification duty in Spain, it decided to inform all its users of the security breach, and the notice went viral on the internet. The DPA then initiated an *ex officio* investigation, but the sanction imposed on BuyVip, if any, was not made public.

The LISS was amended in 2014 to establish specific obligations on cybersecurity incidents applicable to information society services providers, domain name registries and registrars. These obligations are twofold:

a to collaborate with the relevant computer emergency response teams to respond to cybersecurity incidents affecting the internet network (to this end, the relevant information – including IP addresses – must be disclosed to them, but 'respecting the secrecy of communications'); and

b to follow specific recommendations on the management of cybersecurity incidents, which will be developed through codes of conduct (these have not yet been developed).

Operators of critical infrastructure[6] (entities responsible for investments in, or day-to-day operation of, a particular installation, network, system, physical or IT equipment designated as such by the National Centre for Critical Infrastructure Protection (CNPIC) under Law 8/2011) are subject to specific obligations, such as providing technological assistance to the Ministry of Home Affairs, facilitating inspections performed by the competent authorities, and creating the specific protection plan and the operator's security plan.

Furthermore, these operators must appoint a security liaison officer and a security officer. The security liaison officer requires a legal authorisation (issued by the Ministry of Home Affairs), and his or her appointment must be communicated to this Ministry. The security officer does not need a legal authorisation, but his or her appointment must nevertheless be communicated to the relevant government delegation or the competent regional authority.

Royal Decree 3/2010 establishes the security measures to be implemented by Spanish public authorities to ensure the security of the systems, data, communications and e-services addressed to the public, and they could apply by analogy. These security measures are classified into three groups: the organisational framework, which is composed of the set of measures relating to the overall organisation of security; the operational framework, consisting of

6 The following infrastructure areas have been considered 'critical' by Law 8/2011 (which transposes Directive 2008/114/EC into Spanish law): administration, water, food, energy, space, the chemical industry, the nuclear industry, research facilities, health, the financial and tax system, ICT and transport.

the measures to be taken to protect the operation of the system as a comprehensive set of components organised for one purpose; and protection measures, focused on the protection of specific assets according to their nature, and the required quality according to the level of security of the affected areas. Spanish law does not directly address restrictions to cybersecurity measures.

Although cybersecurity requirements do not specifically refer to personal data (but rather to any kind of information), specific security measures will have to be implemented when personal data are involved. In particular, the GDPR requires controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. There is no a mandatory list of security measures to be implemented; however, RD 1720/2007 provides a list of security measures (e.g., establishing an incidents record), distinguishing three levels of security measures depending on the nature of the data, which can be used as a standard specially for SMEs (taking into account the state of the art; costs of implementation; and nature, scope, context and purposes of processing as well as the risk of the varying likelihood and severity for the rights and freedoms of natural persons).

In addition to the above-mentioned laws, certain authorities with specific cybersecurity responsibilities have issued guidance, such as:

a the guidelines published by the Spanish National Institute of Cybersecurity (INCIBE) in 2015 regarding, *inter alia*:
- how companies should manage information leaks;
- cybersecurity on e-commerce;
- security-related risk management for companies; and
- protocols and network security in industrial control systems infrastructures;

b the publication by INCIBE in 2016 of a consolidated code of cybersecurity rules in Spain;

c the National Cybersecurity Strategy issued by the presidency in 2013;

d the strategy series on cybersecurity issued by the Ministry of Defence; and

e the Supervisory Control and Data Acquisition Guidelines issued by the CNPIC in collaboration with the National Cryptological Centre (CNN) in 2010.

The agencies and bodies with competences on cybersecurity are numerous:

a the CCN, which is part of the National Intelligence Centre;

b the CCN Computer Emergency Response Team;

c the CNPIC;

d the Cybersecurity Coordinator's Office (which is part of the CNPIC);

e the Secretary of State for Telecommunications and Information Society; and

f INCIBE (previously known as the National Institute of Communication Technologies), which is the public sector company in charge of developing cybersecurity.

X OUTLOOK

Data protection is constantly evolving. In the past, it has been neglected by both private and public organisations or deemed an unreasonable barrier for the development of the economy. However, this trend has definitively changed in the past five years.

This change is mostly due to the sanctions imposed by the DPA, the role of data in the development of the digital economy (the 'data driven economy'), the active voice of users in the digital environment (developing new social interactions and not only acting as

consumers) and the fact that the European Commission and the European Parliament have definitively embraced a strong 'privacy mission'. Decisions of the CJEU (such as the in the *Schrems v. Facebook* or in the *Google v. Costeja* cases) have also sent out a clear message on the importance of data protection rules in Europe.

The adoption in 2016 of the GDPR constituted a significant milestone in the construction of a new data protection environment. In Spain, the Spanish parliament is currently working on the approval of the Draft Bill, although this approval is not expected before the end of 2018. Although the GDPR provides for data protection principles that are similar to those of the former DP Regulations, as construed by the CJEU and the Article 29 Working Party, it also provides for new rules and standards. Spanish organisations are particularly concerned about the new fines (the applicable criteria for which would be similar to those used in antitrust regulations – a percentage of annual worldwide turnover), the accountability principle, the general security breach notification and the mandatory implementation of a data-protection officer. Additional requirements regarding information and consent duties set out in the GDPR will also be a challenge for Spanish data controllers.

Also, changes in the regulation of the cybersecurity legal regime are expected to happen in Spain in the next year, particularly if the NIS Directive is finally implemented.

Appendix 1

ABOUT THE AUTHORS

LETICIA LÓPEZ-LAPUENTE

Uría Menéndez Abogados, SLP

Leticia López-Lapuente is a lawyer in the Madrid office of Spanish law firm Uría Menéndez. She heads the firm's data protection and IT practice, and leads the LATAM data protection group.

Leticia focuses her practice on data protection, commercial and corporate law, especially in the internet, software, e-commerce and technology sectors. She also advises on privacy law issues. Leticia provides clients operating in these sectors with day-to-day advice on regulatory, corporate and commercial matters, including the drafting and negotiation of contracts, M&A, privacy advice, consumer protection and e-commerce issues, corporate housekeeping, public procurement and RFP procedures, and dealings with public authorities. She has been involved in major transactions and assisted businesses and investors in these sectors.

She regularly speaks in national and international fora regarding personal data protection and technology, in addition to having written numerous articles on data protection-related matters.

REYES BERMEJO BOSCH

Uría Menéndez Abogados, SLP

Reyes Bermejo is a lawyer in the Madrid office of Uría Menéndez. She became a lawyer in 2006 and joined the firm in 2011.

She focuses her practice on data protection, e-commerce and IT. Reyes provides national and multinational companies with day-to-day advice in the above-mentioned areas, on matters such as privacy, consumer protection and e-commerce, and dealings with public authorities, including the drafting and negotiation of IT agreements. In particular, she has extensive experience in the data protection design of commercial and M&A transactions, in the preparation of notices, clauses, contracts, protocols and training programmes, in authorisation proceedings for international transfers and administrative and judicial proceedings, and in preparing website terms and conditions and cookie policies and in advising on direct marketing activities by electronic means.

Reyes is also a professor of data protection and e-commerce law on various master's degree programmes and seminars (the University of Valencia, and the Financial and Stock Market Studies Foundation and CEU Cardenal Herrera University, both also in Valencia).

She contributes to the firm's data protection newsletter and legal magazine (*Actualidad Jurídica Uría Menéndez*) on aspects of and updates relating to data protection regulatory issues and case law.

URÍA MENÉNDEZ ABOGADOS, SLP
c/Príncipe de Vergara, 187
Plaza de Rodrigo Uria
28002 Madrid
Spain
Tel: +34 915 860 131
Fax: +34 915 860 403
leticia.lopez-lapuente@uria.com
reyes.bermejo@uria.com
www.uria.com

ISBN 978-1-912228-62-1