THE ADAPTATION OF THE GDPR IN SPAIN: THE NEW DATA PROTECTION ACT (LOPD)

By Cristina Pauner
Associate professor in Constitutional law at the Universitat Jaume I and member of the PRODADEF Research Group (Data Protection and Fundamental Rights).
She has conducted and participated in European projects on certification (CRISP project) and cooperation among data protection authorities (PHAEDRA project) and various national projects on the impact of GDPR. Her scientific production focuses on freedom of expression and information, privacy and data protection.

By Jorge Viguri
PhD Student in Constitutional Law at the Universitat Jaume I of Castellón (UJI). He has a Master’s Degree in Legal Practice (2014-2016) and was involved in the European project on certification (CRISP project). He widened his studies at the International Institute of Human Rights in Strasbourg (2016), and the Poznań Human Rights Centre (2017). His scientific production focuses on privacy and data protection including certification schemes and the impact of European Dactyloscopy System (Eurodac) on asylum seekers.

I-INTRODUCTION

Spain is a country where the culture in data protection matters is strongly rooted thanks to its norms published from 19921. The Organic Law 5/1992, of 29 October, of the Automated treatment of Data (LORTAD), the Organic Law 15/1999, of 13 December, of Data Protection (LOPD), the Royal Decree 994/1999, of 11 June, that approved the Regulation on Security Measures for automated files that contain personal data (RSM) and the Regulation of Development, Royal Decree 1720/2007, of 21 December, which approved the Regulation implementing the LOPD (RLOPD).

This entire legislative compendium constitutes a consolidated framework that develops article 18 (4) of the Spanish Constitution of 1978 (CE) with states that “the law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights”. Those norms have strengthened the foundations for a legal and institutional framework effectively and efficiently for the protection of personal data in Spain.

The new GDPR is posing a significant challenge to Spain, which commenced in February 2018 the first discussion of the Draft before the Parliament, four months before the application of the new GDPR2.

Currently, the Draft Law for the amendment of the LOPD is Legislative proposal in the Spanish Parliament and a broad agreement on the prioritisation of the Project exists among the main political parties. Despite the critical time lost for the GDPR implementation process in the Spanish framework, the definitive approval is expected before the end of the year.

Likewise, the Spanish Data Protection Agency (AEPD) made and continues to make a fundamental effort to facilitate the adequately implementation of the measures required by the GDPR. Among many other initiatives3, it has brought forward a new Guide by creating an efficient and innovative tool to help organisations to comply with the requirements stipulated by the GDPR. They are available to citizens and public and private organisations and was developed for a wide range of different purposes: to help data controllers to carry out their work, comply with the duty to inform, prepare the contract between a controller and a processor, perform risk analysis and Privacy Impact Assessment (PIAs) and to implement

1 VVAA, 20 años de Protección de Datos en España, AEPD, 2015.
2 Other European countries have already adapted their national legislations to the new European legal framework. For example, the German government passed an implementation Act to Adapt Data Protection Law to regulation (EU) 2016/679 and to implement Directive (EU) 2016/680 dated 30 June 2017; in Austria, the Data Protection Amendment Act 2018 was published on 31 July 2017; Belgium passed its GDPR implementing legislation on 3 December 2017 Loi relative à la protection de la vie privée à l’égard des traitements de données à caractère personnel, on 29 November 2017, the Slovak Parliament adopted a Bill which repealed the incumbent Act on Data Protection, n. 122/2013 and implements the GDPR effective 25 May 2018. Italy approved the Law n.167/2017 to reform the Codice in materia di protezione dei dati personali, that was approved in 2003. Adjoining the Code, the Garante per la protezione dei dati personali has published a Guide (Guida all’applicazione del Regolamento UE 2016/679) where explains in detail the values changes that the new GDPR will demand for citizens and organisations.
3 The AEPD has placed the following link containing a complete section concerning the implementation of the GDPR in Spain (http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php).
relevant techniques to facilitate public authorities switching to the GDPR.

II-LEGISLATIVE PROCESS. KEY DATES

On 10 November 2017, the former Spanish Government, led by Mariano Rajoy, in the meeting of the Council of Ministers, approved the preliminary draft law amending the LOPD (APLOPD)\(^5\) at the behest of the Ministry of Justice. The APLOPD was followed by the mandatory impact reports\(^6\) and the consequent opinion of the Council of State\(^7\). On 24 November 2017, the new draft LOPD was presented for the corresponding parliamentary procedure\(^8\).

After three months of inactivity and the successive postponements, on February 15, during the first session of debate in the Chamber of Deputies, different positions of the political groups were presented and the proposal for rejection tabled by the Mixed Parliamentary Group (PDeCAT) was discussed. It focused on the competence issue, that is, the lack of legal guarantees and competences performed by the supervisory authorities of the Autonomous Communities. This issue and the delay of the government to submit the draft before the chambers were conveyed in the whole discussion. The overall amendment was passed\(^9\) moving to the reading in the Committee of Justice where the partial amendments to the enacting terms are being discussed at present.

A total of 368 amendments were presented\(^10\), which are intended to make substantial improvements to certain relevant points in the final text of the Spanish Act. During the months of November 2017 to March 2018, the Committee of Justice received a large number of parliamentary hearings related to the field of data protection, not only assessing the draft LOPD but also providing substantive input that have been reflected in the partial amendments, as it is explained in this paper.

III-NOTEWORTHY ASPECTS

The draft LOPD is adapted to the new GDPR but it does not reproduce its content requiring a common reading of both legal texts. In fact, it starts with an explanatory statement and consists of 78 articles structured in 9 titles, 17 additional provisions, 6 transitory provisions, 1 derogatory provision and 5 final provisions. In addition, it introduces important changes to the following key questions:

1. A change of the compliance model of data protection provisions: from the traditional model of verification of compliance towards a new dynamic perspective based on active security measures.

Data protection flows will be monitored instead of the structure of the filing systems in order to establish protection measures. Among others, a “register of processing operations/activities” is expected to be established in the final text for every organisation/company (according to article 33 LOPD). A revision of data processing is included before commencing the authorized activities carried out in the process.

The register of processing activities is performed in two phases. The first stage consists of a revision of the data treatment carried out by the organisation. The second stage revises the new obligations provided in the GDPR, specifically those imposed for the responsible authorities of the Autonomous Communities. This issue and the delay of the government to submit the draft before the chambers were conveyed in the whole discussion. The overall amendment was passed\(^9\) moving to the reading in the Committee of Justice where the partial amendments to the enacting terms are being discussed at present.

2. The data’s consent and the consent needed to process personal data are strengthened (article 6 LOPD). According to the GDPR, the new LOPD aims to ensure that the user’s consent for the data processing is supported by an express declaration of agreement or by a strong affirmative action. This new provision excludes the “implied consent” arising from those actions, which are not explicitly voiced nor necessarily understood. Additionally, the consent of the data subject shall be given unequivocally, specifically for each purpose in the processing of data. Generic or

\(^5\) Ministry of Justice. Preliminary Draft amending the LOPD [in Spanish, Anteproyecto de Ley Orgánica De Protección de Datos de Carácter Personal (ALOPD)]. The information is available at: http://servicios.mpr.es/seacyp/search_def.asp?crypted=ehA%98%85%A2%BD%OD%90%8C%8An%87%A2%7F%88%99t1%84sm%A3%91


https://blogdroiteuropeen.com
diffuse consent for multiple purposes will be prohibited in the new LOPD.

3. The processing of data pertaining to the deceased constitutes another of the significant novelties in the new LOPD (article 3). The draft LOPD excludes from its scope the application the data pertaining to the deceased. However, it allows the direct heirs to access data pertaining to the deceased, including the rights of correction and deletion. This shall be subjected to the instructions given to them by the deceased and incorporated in a special register.

4. The new LOPD adapts the principle of transparency that the GDPR foresees in article 11. It regulates the data subjects’ right to be appropriately informed about any processing of personal data relating to themselves. Information layers are also included, which aim at providing detailed information to the person concerned, allowing a direct and immediate access to information.

The principle of “exclusion of the eligibility of the controllers” is also included in the new LOPD. It establishes the adoption of all reasonable measures to guarantee the rectification or removal of relevant data. The rights of access, rectification, cancellation or objection (known as ARCO rights) and a catalogue of data protection rights (including the deletion of data, the limitation principle of the processing of personal data or data portability) is also set out in articles 15-17.

5. The existence of black lists shall be prohibited for the special categories of data. This involves data concerning ideology, union membership, religion, beliefs, racial origin, health or sex life (article 9).

To avoid discriminatory situations, the subject’s mere consent will not be enough to avoid the general prohibition on processing sensitive data. Nevertheless it will be permissible to process sensitive personal data for certain purposes. For example, the compliance with legal obligations, the protection of the vital interests of the data subject, the processing carried out as part of the activities of an establishment pertaining to the data controller with due guarantees by a foundation, a non-profit association or in any other circumstances contemplated in in paragraph 2 article 9 GDPR.

6. The regulation of the credit information systems, known as “credit blacklists” is another provision referred to in article 20. This specific legal system is complemented by the 8th Additional Provision. It sets a minimum financial limit for the inclusion of this personal data to specific type of files, which strengthens the level of security and avoids the stigmatisation of debtors. Debate revolved around the increase of the limit, which is nowadays established in 50 euros.

7. Strengthening the exclusion files regarding advertisement, the so-called “Robinson lists” (article 23). These are files or folders created with the objective to assist individuals in presenting their complaints against “spam” (unsolicited marketing communications to an individual via telephone, fax, email, text message, etc.). The new LOPD foresees that the processing of the personal data will be lawful in relation to the purposes for which they are collected in order to avoid the despatch of commercial communications to data subjects who have stated their refusal or objection to receiving advertising.

8. Efficient authorisation mechanisms that guarantee the rights of data subjects and the implementation of extra-judicial settlement-of-conflicts policy in order to resolve promptly disputes between citizens and the Data Protection Officer (DPO) regulated in 34 or the implementation of alternative dispute resolution systems through codes of conduct (article 38).

IV-DIGITAL RIGHTS CHARTER

One of the most relevant amendments to the draft LOPD was presented by the Socialist Parliamentarian Group. It aims at transforming the Law into a Digital Rights Charter. To that end, Artemi Rallo, former Director of the AEPD and current member of the Spanish parliament, proposed the addition of a new Title X “Digital Rights Guarantees”, which comprises of 14 articles (79 to 93). They not only reinforce the digital rights of citizens but also extend the application of the rights and liberties enshrined in the Spanish Constitution and by International treaties to the Internet.

12 The «Robinson List of Advertising Exclusion» is a voluntary and free service which is available to all consumers. It aims at reducing personalised publicity. More information can be found at: https://www.listarobinson.es/

13 On May 30 2018, the Spanish parliament unexpectedly approved a constitutional motion of censure against the government of Rajoy in accordance with articles 113 and 114.2 of the Spanish Constitution and in articles 176 to 179 of the Rules of the Congress. Pedro Sánchez, Secretary general of the Socialist Group, was elected the president of the Spanish Government after winning the motion of censure.

https://blogdroiteuropeen.com
The proposal very much takes into account the characteristics of similar regulations approved in countries from the European area (specific legislation, sectoral rules, declaratory nature of some charters recognising these rights). Examples include the French Law No. 2016-1321 of October 7, 2016, for a Digital Republic, the “Right to Disconnect” recognised in the French Labour Code or the Declaration of Internet Rights in Italy. The explanatory memorandum accompanying the proposal states that the legislation should recognise a Digital Rights Guarantees System in a comprehensive and unified manner due to the absence of a constitutional reform that guarantees a new generation of digital rights. This Amendment sets forth the need to implement the following measures:

- **The right to neutral access to the Internet.** Service providers shall offer, as much as possible, transparent services in order to avoid technical or economic discrimination.

- **The right to Internet access,** which shall be universally, accessible, affordable and non-discriminatory.

- **The right to online education** for students on safer use of new media through teacher training programmes.

- **The right to digital security.** This right, which deals with holding technology companies accountable for digital security, has become public policy priority in an increasingly digital and data-dependent economy and society. It implies a guarantee of privacy and security of communications over the Internet by providing information to users and the establishment of swift and uncomplicated complaint procedures.

- **The right to be forgotten,** which postulates that personal data shall be erased when it is inadequate, irrelevant and excessive in relation to the purposes for which it was collected. In these circumstances, a search engine operator would be obliged to delete the links to related pages. Also, personal data, that has been made available by minors, should be deleted at the request of the party concerned.

- **The right to data portability,** which allows users to store, transmit, receive and transmit personal data they provide on social networking websites and other information society services.

- **The right to privacy and the use of new digital devices in the labour field** that protects civil servants, workers and employees against intrusion of their privacy.

- **The right to disconnect.** It allows employees in companies of more than 50 people to ignore emails after work hours to guarantee personal and family privacy. For that purpose, the company shall publish an internal charter or similar internal rules, after seeking the opinion of the employees’ representative bodies. In this case, the employer will be the only decision maker. Employers should not ignore the issues that can arise from excessive use of digital devices. Where possible, they should implement measures to promote the rational use of digital devices, so that employees adopt a healthy lifestyle, and to promote work/life balance.

- **The right to privacy in the use of audio-visual or geo-location systems in the working area.** This right regulates the processing of personal data obtained by employers for labour control purposes through video-surveillance and geolocation systems. Prior information shall be given by the companies to the employees concerned including their rights to access, rectification and erasure of their personal data.

- **The digital rights of collective negotiation** that foresee the possibility of establish additional protection of their rights and freedoms in regard to the processing of personal data of workers.

- **The protection of minors on the Internet** that prompts a whole series of measures that aim to ensure children’s rights. It also acknowledges the

---


15 It is applicable with effects from the 1st January 2017. Article 551.2 de la Loi 2016-1088, du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels, introduces a new paragraph 7 (See in the Chapter II "The adaptation of labour law to the digital age".


17 Brazil has a similar proposal. The Internet Civil Framework introduces a procedure in order to encourage the respect of the civil rights in Internet through the mainstreaming of the network’s neutrality, limitation of liability for intermediaries and Internet users’ freedom of speech, privacy and security. Act num. 12.965, 23 April 2014. Further information available at: http://participacao.mj.gov.br/marccivil/sistematizacao/
huge impact of the Internet on children’s rights in order to promote necessary guarantees to protect their safety and physical integrity.

- Freedom of expression and information on the Internet. It aims to guarantee the accuracy of information through the adoption and implementation of the provisions regarding effective protocols. Social networking site providers, digital platforms and similar information society services may remove “third party content that goes against the constitutional right to freely communicate or receive accurate information by any means of dissemination whatsoever”.

Likewise, the right to honour and to personal and family privacy and self-image needs to be greater assured, particularly in social networks, digital platforms and similar information society services. Providers of those services are also bound to provide necessary protocols to “preserve human dignity” and “guarantee the correct identification and authentication of the users who violates those protocols”.

- Right to digital testament. It will allow the deceased’s relatives or legal successors to access to the personal data and to provide instructions for their use, destination or deletion.

The reforms represent a strong commitment by the Spanish Government in the development of an Internet Access National Plan to overcome digital gaps, by fostering the use of public Internet access spaces and educational initiatives for persons at risk of digital exclusion. In addition, the Government should have approved an Action Plan to improve training and awareness to minors as well as a more responsible, balanced and efficient model to be adapted to the new era of the Internet and the rights, guarantees and mandates included in the initiative.

V-CRITICAL ASPECTS

The content of the draft LOPD is currently being considered in the Spanish Parliament. This draft may undergo major revisions during this period in response to criticisms by a wide range of stakeholders. They are summarised in the following seven action points:

1. The Spanish Government has been criticised for failing to reach agreement on better protection of minors. The minimum age for giving valid consent has been set at 13 years (article 7) in contrast to Germany or France where their national legislation has set the age of consent at 16 years. However, it follows the same approach adopted in other EU countries like Ireland, where children at the age of 13 may legally sign up for services that process personal information. Although the Spanish Government has shown restraint in its response so far, it has claimed that the minimum age is a realistic in accordance with other national laws. The principle of the best interests of the child should require Spanish legislation to raise the minimum age and apply strict safeguards in respect of children.

Efforts need to be made to guarantee the security of minors and the minimum age for consent should be raised, in line not only with the Spanish experience but also following the Facebook and Instagram terms and conditions to create an account.

2. The regulation of the Data Protection Officer (DPO) (articles 34-37). This is structured in an open and flexible manner due to different features: a) its mandatory or voluntary nature, b) its operation within or outside the organisation and c) for both legal entities and individuals.

In any case, the draft lists a series of concrete and potential scenarios that must be communicated to the competent authority who shall maintain a public and regularly updated list accessible by any person. It is considered that the draft LOPD is undermining the figure of the new DPO. This legal uncertainty could undermine their effective implementation as it is not fully regulated in the GDPR nor in the current LOPD.

_____

18 Rallo Lombarte, Artemi and Martínez Martínez, Ricard, Derecho y Redes sociales, Thomson Reuters, Pamplona, 2013, 2nd ed.


20 In fact, they are configured as a flexible body as they can be a natural or legal person. Also, it can be accredited on a voluntary basis by the new certification scheme (in compliance with the standards UNE-ISO/IEC 17024:2012) issued by the AEPD in cooperation with the National Accreditation Body (ENAC). Further information about the certification scheme can be found at: https://www.enac.es/es/esquema-delegado-proteccion-datos-aepd. In addition, the Draft qualifies the narrow list of entities that must have a DPO which includes the following: big companies, network operators and other electronic communications services providers (only if they process large-scale personal data regularly and systematically), information society services (if undertaking large-scale profiling of the service’s users) and organisations operating with commercial reports concerning natural persons.

21 As evidence of the doubts raised by the DPO figure, during the procedure of the LOPD project, some members have registered official questions addressed to the Government and related to the requirement to be DPO (Chamber of Deputies, Parliament—https://blogdroiteuropeen.com
3. Impediments to scientific and biomedical research. Article 6 of the draft LOPD imposes the requirement of different types of consent for different purposes of processing personal data.

This legal requirement may become an insurmountable obstacle to the further development of the biomedical research in Spain. Article 9 draft LOPD regulates that the mere consent of the data subject shall maintain the general prohibition on processing sensitive data. Also, data processing described in article 9 (2) subparagraphs g), h) e i) GDPR shall be covered by the Law, which may set further requirements for the security and confidentiality of the data.

This regulation is somewhat restrictive for the investigation of cases relating to the public health and the reutilisation of personal data within the public sector (health, occupational health, national health systems, biomedical research, trials of medications and general research). A broad consent in this field is claimed in order to ensure the protection of the rights to data subjects. However, the consent shall have legitimate uses (a report issued by the AEPD establishes that the broad consent shall be included in the current draft LOPD). This includes technical measures, access restrictions, ethical committees or the legality in the re-use of personal data or documents containing anonymous data for research purposes and access thereto by unauthorised third parties.

4. The draft LOPD regulates also the scope of use of video-surveillance data. It clarifies that these images can only be obtained by employers in specific cases, for example, where there is a reasonable suspicion that an employee has committed unlawful (Article 22).

However, contributors are unanimous about the need to prevent the serious regression of workers’ rights in the current regulation. It is manifestly diverging from the existing protections recognised in the ruling of the European Court of Human Rights in the case of López Ribalda and Others v. Spain. It should be specified that information must be given in advance including the right to information for workers’ representatives.

The data protection regulation should not be the appropriate legal instrument for assessing the evidential value of the images. The requirements for processing personal data should be delimited appropriately.

5. Treatment processing conducted by Public Administrations. Internal complaints information systems in the private sector are excluded (article 24). On the other hand, the payment of all financial sanctions is not foreseen, pursuant to the “cash unit principle”. This principle implies that the funds collected by the AEPD are directly transferred to the General Administration of the State. This means that in the case of infringement committed by a public office, the public administration that imposed the corresponding penalty would not have its own resources to compensate for damages resulting from its actions and acts. Consequently, citizens would bear the economic burden. This is compatible with article 77 of the draft LOPD, which establishes the sanctions regime in the public sector.

6. The obligation to block as an interim measure (article 32). Blocking is an obligation imposed on data controllers to retain personal data that has been erased so that it may be made available to judicial or administrative authorities. This provision prevents the erasure of personal data that could cover-up potential breaches. However, this measure is not laid down in the GDPR and other EU countries have not included this provision in their national legislations.

In Spain, this provision has given rise to serious misgivings for the following reasons: a) the recognition

---

**THE ADAPTATION OF THE GDPR IN SPAIN: THE NEW DATA PROTECTION ACT (LOPD) by, Cristina Pauner and Jorge Viguri**

---


24 ECHR, Case of López Ribalda and Others v. Spain (Applications num. 1874/13 and 8567/13), Third Section, 9 January 2018.
of the right to purpose limitation principle for the processing of data, which has a similar effect to blocking for those who ensure data subjects’ rights in the event of possible claims, b) the lack of time limits and c) the need to specify when a derogation from this obligation could be feasible.

7. Lack of modernisation of the Spanish Data Protection Agency (Articles 44-56). In the new LOPD, the AEPD is established as an independent administrative authority, whose relations with the Spanish Government is carried out though the Ministry of Justice. A greater cooperation and coordination with the corresponding autonomous community of data protection authorities is required to increase efficiency and improve the internal functioning and transform the structure, staffing and resources. LOPD contains what seems to be a hierarchical relationship between the AEPD and the de facto subordination of the Basque and Catalan Data Protection Agencies. Article 56 draft LOPD states that only the AEPD is responsible for the foreign policy. Articles 57 to 62 draft establishes clearly that both agencies will be competent to exercise the functions set out in article 57 y 58 GDPR as regards the processing of personal data of the public sector for entities in their territory or those providing services relating directly or indirectly in their territory (paragraph a) article 57), data processing carried out by natural or legal persons in the in the exercise of public functions in relation to matters that are within the competence of the regional or local administration (paragraph b) and data processing foreseen in the Statute of Autonomy (paragraph c).

In addition as the process of appointing the AEPD Director is only based on a proposal made by the Ministry through the appearance before the Constitutional Committee and criteria of professionalism and expertise are not foreseen. Only the appointment of a Parliamentary Commissioner is proposed within a demanding process in terms of personal and professional competencies for the sake of independence and professionalization. In addition, membership of the Consultative Council, an advisory body composed initially of a parliamentary Deputy, a Senator, a representative designated by General Council of the Judiciary and the General Administration of the State, has been broadened with the participation of academics and experts on national and international law and specially, in data protection with, at least, ten years of practise in the exercise.

VI-CONCLUSIONS

The GDPR is applicable from May 25, 2018 in all member states to harmonize data privacy laws across Europe. However, the final text of the current draft LOPD is still pending approval. On an optimistic view, the new Spanish Act is expected to come into force six months after the application of the GDPR. The delay in the adoption of the electoral law is creating new legal uncertainties, which can be overcome only through the alignment of the existing data protection legislation. At this stage, the Draft LOPD does not reproduce the full content of the GDPR so both legal texts will have to be read together to ensure the correct application of the GDPR at Spanish level.

However, the following substantive changes have been proposed compared to the current LOPD.

- Firstly, new security measures aimed at adapting appropriately the level of security to the potential risk.
- Secondly, the requirement of consent is reinforced. The explicit consent in article 6 draft LOPD requires the express and unconditional consent given in an intelligible, easily accessible form and also with the purpose for data processing attached. Besides, information layers allow users to have access to basic information and personal data easily through email.
- Thirdly, the implementation of the right to access, correction and deletion of data pertaining to the deceased will be incorporated in the new LOPD.
- Fourthly, the prohibition of black list concerning sensitive data and the transparency requirement shall constitute an important safeguard as Internet users will be better informed about what happens to their personal data but it will also become easier for them to exercise their ARCO rights (access, rectification, erasure and objection). Fifthly, the exclusion files regarding advertisement will be strengthened, so spamming will be prohibited except with respect to subscribers who have indicated that they want to receive unsolicited e-mails for direct marketing purposes.
- Finally, the Spanish LOPD will include some references to the need for an extra-judicial settlement of conflicts policy to “promptly” resolve disputes.

This paper would like to emphasise that the Socialist Group (currently the Spanish Government) presented the most relevant amendments to the draft LOPD. They have been firmly committed to the transformation of the current draft towards a Digital
Rights Charter. Despite these efforts, in cooperation with other parliamentary groups, a number of issues remains to be tackled, requiring enhanced revision of the current draft LOPD before it is finalised, in respect of the protection of minors, the regulation of the Data Protection Officer, role the impediments to scientific and biomedical research, the scope of video-surveillance, the lack of a regime of sanctions for public administrations, the obligation to block as an interim measure and the lack of modernisation of the Spanish Data Protection Agency.

Drawing together the criticisms highlighted in this paper, the draft LOPD, in line with the current LOPD, does not contain open clauses according to article 85 GDPR. These are the grounds for derogation in matters of right to freedom of expression and information, which is known as the journalism exemption.

Ultimately, the introduction of regulatory changes currently pending before the Parliament might create a complex draft LOPD, producing legal uncertainty for organisations and citizens due to its inappropriate legislative technique. Therefore special attention should be given to the internal coherence of the new Spanish Act.