ARTÍCULOS

Cuadernos de **Gobierno y Administración Pública**
ISSN: e-2341-4839

https://dx.doi.org/10.5209/cgap.74053

EDICIONES COMPLUTENSE

Privacy and public authorities: Issues in the new digital administrative process

Juan Franciso Rodríguez Ayuso[1]

Recibido: 1/02/2021 / Aceptado: 10/05/2021

Abstract. The main objective of this research study is to offer a systematic analysis of consent in the processing of personal data of minors under the General Data Protection Regulation and the Organic Law on the Protection of Personal Data and the Guarantee of Digital Rights. This is the fundamental legal basis for dissecting the essential contours of the digital signature as the most suitable instrument for guaranteeing the provision of this consent, placing special emphasis on the singularities that this presents when those intervening as data controllers are Public Administrations under the new regulations on trust services.
Keywords: personal data, digital signature, consent, minors, public administrations, personal data, digital signature.

[es] Privacidad y autoridades públicas: Cuestiones propias de la nueva tramitación administrativa digital

Resumen. El objetivo principal del presente estudio de investigación consiste en ofrecer un análisis sistemático del consentimiento en aquellos tratamientos de datos personales de menores de edad al amparo del Reglamento general de protección de datos y en la Ley Orgánica de Protección de Datos Personales y de Garantía de Derechos Digitales. Y ello como base jurídica fundamental para diseccionar los contornos esenciales de la firma electrónica como instrumento más idóneo para garantizar la prestación de este consentimiento, haciendo especial énfasis en las singularidades que ello presenta cuando quienes intervienen como responsables del tratamiento son las Administraciones Públicas al amparo de la nueva normativa en materia de servicios de confianza.
Palabras clave: datos personales, firma electrónica, consentimiento, menores de edad, Administraciones Públicas

Cómo citar: Rodríguez Ayuso, J.F. (2022): Privacy and public authorities: Issues in the new digital administrative process, en *Cuadernos de Gobierno y Administración Pública* 9-1, 9-20.

1. Introduction

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC[2] (hereinafter General Data Protection Regulation or GDPR) regulates personal data relating to minors in a new way, since this issue was not specifically addressed in the previous legislation, which was largely based on the system provided for in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[3] (hereinafter, GDPR).

In turn, and with the aim of adapting the Spanish legal system to the General Data Protection Regulation and completing its provisions, the new Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights[4] (hereinafter, LOPDGDD), which, by virtue of its Single Repealing Provision, repeals Organic Law 15/1999, of 13 December, on personal data protection[5] (hereinafter, LOPD) and Royal Decree-Law 5/2018, of 27 July, on urgent measures for the adaptation of Spanish law to European Union regulations on data protection[6], in addition to any provisions of equal or lower rank that contradict, oppose or are in-

[1] Universidad Internacional de La Rioja
juanfrancisco.rodriguez@unir.net
[2] Official Journal of the European Union (hereinafter referred to as DOUE) L 119/1 of 04 May 2016.
[3] Official Journal of the European Communities (hereinafter referred to as DOCE) L 281/31 of 23 November 1995.
[4] Official State Gazette (hereinafter, BOE) no. 294, of 06 December 2018.
[5] BOE No. 298 of 14 December 1999.
[6] BOE no. 183 of 30 July 2018.

compatible with the provisions of the GDPR and the present LOPDGDD[7]. This new Organic Law will also make a specific and relevant pronouncement on the special processing of personal data relating to minors.

In accordance with the most relevant international instruments, when we speak of minors, we are referring to those natural persons under 18 years of age, given that they have not been emancipated from a legal point of view prior to that age (Andreu, 2013). Over the last few years, a large part of the doctrine (Hidalgo, 2017; Piñar, 2016) has opted to use the notion of children and adolescents to refer to persons under 18 years of age; however, throughout these pages, we will use the previous notions interchangeably, as well as the notions of minors or, simply, minors.

The Article 29 Working Group[8] also defines them as human beings in the exact sense of the word (who are also under 18 years of age) (Article 29 Working Group., 2017). Precisely for this reason, a minor should enjoy all the rights that correspond to a person, including, obviously, the fundamental right to the protection of his or her personal data (Durán, 2019).

In this sense, it is Article 8 GDPR that has included, for the first time in the Community regulatory framework, a specific reference to the protection of personal data of minors. In this regard, neither the repealed Directive nor Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the digital communications sector (Directive on privacy and digital communications)[9] included any specific mention of minors. Beyond this, in Spain, and on the basis of this provision of the GDPR, several others will be born that will come to explain the content, somewhat more generic, of the Community article; these will be, in essence, Articles 7, 84 and 92, in addition to the 19th Additional Provision, all of them, we repeat, of the new LOPDGDD.

In accordance with this Community precept, which explicitly regulates the Conditions applicable to the consent of the child in relation to information society services:

> "1. Where Article 6(1)(a) applies in relation to the direct offer to children of information society services, the processing of a child's personal data shall be considered lawful where the child is at least 16 years old. If the child is under 16 years of age, such processing shall only be lawful if and only to the extent that the consent was given or authorised by the holder of parental responsibility or guardianship over the child.
>
> Member States may provide by law for a lower age for such purposes, provided that such lower age is not less than 13 years.
>
> 2. The controller shall make reasonable efforts to verify in such cases that consent was given or authorised by the holder of parental responsibility or guardianship over the child, taking into account available technology.
> 3. Paragraph 1 shall not affect general provisions of contract law of the Member States, such as rules relating to the validity, formation or effects of contracts in relation to a child".

Although prior to the new rules on the protection of personal data there was no specific regulation on this issue, this does not allow us to state that, throughout this period of time, the processing of personal data of children has been in a situation of legal uncertainty, since minors have always had the right to privacy and to the protection of personal data in their immanent condition of natural persons, to whom the rules have always applied and will apply, without any distinction whatsoever (Durán, 2013; Gómez-Juárez, 2016; Guillén, 2015). Consequently, the general principles contemplated in the previous regulation have been applicable to all cases involving minors.

Irrespective of the above, it goes without saying that the new rules on the protection of personal data will apply to all minors, whether or not they are European nationals, regardless of their legal status within the European Union (Palma, 2018). In this sense, the first paragraph of Article 4 of the GDPR[10], when referring to the concept of data subject, does not establish any distinction or differentiation based on the nationality or situation of the natural person under analysis; this, in the specific case we are analysing now, is of specific importance if we consider the increasingly frequent situations of minors from non-EU territories, an aspect of great relevance, although it is beyond the scope of this study.

In any event, we will conclude by saying that, as we will have the opportunity to analyse, although both the GDPR and the new LOPDGDD include provisions related to the processing of personal data of minors, there are numerous references to children

---

7 In particular, Royal Decree 1720/2007, of 21 December, approving the Regulation implementing Organic Law 15/1999, of 13 December, on the protection of personal data (hereinafter, RDLOPD) (Official State Gazette no. 17, of 19 January 2008). However, this Royal Decree is not expressly repealed, so that, in everything that does not oppose or contradict the provisions of the national and Community regulations currently in force, it will continue to be fully applicable.

8 The Article 29 Working Party (Art. 29 WG) is the independent European working group that has been dealing with issues related to privacy and personal data protection until 25 May 2018 (entry into application of the GDPR).

9 DOCE L 201/37 of 31 July 2002.

10 According to this paragraph, data subject shall be:

"[...] an identified or identifiable natural person ("data subject"); an identifiable natural person shall be any person whose identity can be established, directly or indirectly, in particular by means of an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person". The data subject shall therefore be the owner of the personal data undergoing processing.

when analysing other matters. These allusions are justified by the fact that these provisions do not seek to fully regulate the processing of personal data relating to minors (which is why it is necessary to integrate the provisions of this article with the rest of the legislation on the protection of personal data), but only address an analysis of those conditions that apply to the consent of minors, provided that such consent is given in the specific field of information society services (De las Heras y De Verda, 2019).

2. Legitimacy of the process of minors

Article 8 GDPR regulates the conditions that apply to the consent of minors in relation to information society services as a legal basis for the processing of their personal data.

This provision stipulates that, where the consent relates to the making of a direct offer to minors of information society services, the processing of the child's personal data is lawful if the child is over 16 years of age. If the child is under this age, such processing shall only be considered lawful if and only to the extent that the consent on which it is based was given by the holder of parental authority or guardianship over the child and only to the extent that it was given or authorised. In any event, this does not affect the general provisions of the law governing contracts in the countries of the European Union, such as the rules relating to the validity, formation or effects of contracts in relation to minors.

This Article also gives the Member States the option of modifying this minimum age by means of an internal law, provided that it is not lower than 13 years of age. Under the protection of this provision, Article 7 of the new LOPDGDD (in addition to Articles 84 and 92, as well as the Nineteenth Additional Provision) is born, which alters this minimum age, in general terms, to 14 years of age[11] and does so in the following terms:

> "1. The processing of the personal data of a minor may only be based on his or her consent when he or she is over fourteen years of age. Exceptions are those cases in which the law requires the assistance of the holders of parental authority or guardianship for the conclusion of the legal act or business in the context of which consent to the processing is sought.
> 2. The processing of data of minors under fourteen years of age, based on consent, shall only be lawful if the consent of the holder of parental authority or guardianship is given, with the scope determined by the holders of parental authority or guardianship".

An important aspect is what is to be understood by information society services. Contrary to what might be thought, the regulatory text responsible for providing a definition of information society services is not the one that regulates their subject matter. Indeed, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular digital commerce, in the Internal Market (hereinafter referred to as the Directive on digital commerce or the DCE)[12], in Article 2. (a) refers to Article 1(2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations[13], as amended by Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations[14].

According to this provision, an information society service is defined as:

> "[...] any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

A service shall be deemed to be at a distance when it is provided without the simultaneous presence of the parties, i.e. without the synchronous physical presence of the person providing the information society services (information society service providers) and the recipient (recipients of information society services); by digital means, where it is sent from the source and received by the recipient of information society services by means of digital equipment for the processing (including digital compression) and storage of data and which is transmitted, conveyed and received in its entirety by wire, radio, optical or any other electromagnetic means (Plaza, 2013), and at the individual request of a recipient of services, where it is the recipient who requests that the service be provided to him. Finally, the information society service is for consideration when both parties involved obtain something reciprocally, i.e. when both the providers of information society services and the recipients of information society services provide something for the benefit of the other party (Alemán, 2006).

Notwithstanding the latter statement, it is worth bearing in mind the content of Recital 18 DCE, which clarifies that information society services do not only cover those services which give rise to online contracting, but, to the extent that they represent an economic activity, they will also extend to services which are not remunerated by their recipients. In the opinion of some authors, this onerous nature of the

[11] However, in the initial LOPDGDD Proposal, the minimum age foreseen was 13 years old.

[12] DOCE L 178/1 of 17 July 2000.

[13] DOCE L 204/37 of 21 July 1998.

[14] DOCE L 217/18 of 5 August 1998.

service is an essential note, since what is included is any activity carried out digitalally and which has an economic significance, regardless of whether or not it is the end user who has to pay for the service in question (Rodríguez, 2018).

Thus, all those who obtain economic income as a consequence of the service, either directly (as is the case of services paid for by their recipients) or indirectly (through the inclusion of advertising or as a consequence of the exploitation of personal data of users who register to access the service), will be understood to be included within the notion of information society service providers. On the other hand, all other cases in which a total absence of economic activity is to be considered, such as personal web pages or blogs, would be excluded from the specific legal regime for information society service providers.

In the domestic legal system and in practically identical terms, Law 34/2002, of 11 July, on information society services and digital commerce[15] (hereinafter, LSSICE) has also opted to include, in section a) of its annex, a definition of information society services. All these services, the Spanish legislator states, will be characterised by four essential aspects that must cumulatively concur: they must be provided at a distance, by digital means, at the individual request of the recipient of information society services and, at least usually, for consideration. And this is where, based on the Explanatory Memorandum, the third section includes, within the concept of information society services, digital commerce, which includes two fundamental activities that group together the rest: on the one hand, the sending of commercial communications prior to contracting, which groups together the supply of information by telematic means, and, on the other, digital contracting itself, which includes both the organisation and management of auctions by digital means or of virtual markets and shopping centres, and the management of purchases on the Internet by groups of people. The means through which this contracting can be channelled are, among others, e-mail, web page, videoconference or chat.

To these should be added, as we shall see, those information society intermediation services relating to the provision of access to the Internet (Internet service providers), those that allow the transmission of data over telecommunications networks (mere conduit or routing), those concerning the temporary copying of Internet pages requested by users (proxy caching or buffering), those enabling the hosting of information, services or applications provided by others on their own servers (hosting), those providing search tools or links to other Internet sites (searching and linking), those making possible, the creation, verification and validation of digital signatures, digital seals, digital time stamps, certified digital delivery services, certificates relating to these services and certificates for the authentication of websites, and the preservation of digital signatures, seals or certificates relating to these services (trust services) or any other service provided at the individual request of users (such as the downloading of files or audio), provided that they represent an economic activity for providers of intermediary information society services:

Thus, and returning to the consent of minors, the General Data Protection Regulation distinguishes between the following possible scenarios (Brito, 2017).

Firstly, in cases where the minor is under 18 and over 16 years of age, in which case he or she may give consent, so that, if he or she does so, the processing of his or her personal data by the controller will be lawful.

Secondly, in the case of minors under 16 years of age, they will not be able to give valid consent. In such cases, consent on their behalf must be given by the holder of parental authority or guardianship over the minor.

Thirdly, in the case of minors under the age of 16 and over the age of 13, who will be entitled to give their consent in a valid manner if so established by the Member States at the domestic level, as is the case in Spain, under the protection, we repeat, of Article 7 of the new LOPDGDD.

Finally, children under 13 years of age, who, under no circumstances, will be able to give their consent in a valid manner in accordance with the law for the processing of their personal data, not even in the event that the national law of a Member State of the European Union implements it, since this provision would be understood to be contrary to the provisions of the second paragraph of Article 8 of the GDPR.

Notwithstanding the above, we must always bear in mind that, in general, the best interests of the child shall prevail. This means that, in cases of conflict (for example, in those cases in which the holder of parental authority or guardianship over the minor gives consent on behalf of the child concerned for a processing of personal data that is clearly detrimental to the interests of the minor), those mechanisms provided for in each Member State will have to be enabled to protect the interests, we repeat, the best interests of the child (Escobar, 2017).

In any event, this Article 8 of the GDPR lacks any provision in relation to the consent given by the minor or by the holder of parental authority or guardianship over the child when we are not dealing with a case of an offer of an information society service, as Article 7 of the LOPDGDD does. In this case, it leaves the doubt as to whether or not the content of this provision could also be applied to these cases, and, in the latter case, what response could be given, whether analogous or not, to the provisions of Article 8 GDPR, a doubt that disappears with the entry into force of the LOPDGDD.

In any case, in the general opinion, it does not seem to be the intention of the Community legislator to leave out all those cases which may arise and which respond to a minor's consent, outside an offer of information society services (Rodríguez, 2019). It

[15] BOE no. 166, of 12 July 2002.

is true that it would have been highly advisable for the specific content of Article 8 GDPR to have stated this circumstance, although, as we said, by extension or by applying a rule of analogy to this content, we could understand Article 8 GDPR to be applicable to similar situations. In short, despite the fact that the new legislation on personal data protection refers specifically only to information society services, it would not be appropriate to understand that this would leave out of the regulatory framework many other cases, which are certainly similar and also in need of regulation.

Nor does it include the case that would allow us to know what happens to consent when it is given by the holder of parental authority or guardianship over the child at a time before the child reaches the age of majority, when the latter, immediately afterwards, reaches the age of majority. We do not know, unless we carry out interpretative work, what would happen with this consent, i.e. whether it would be necessary to seek consent again, this time directly from the minor, or whether it would be possible to extend the effects of the consent given by the holder of guardianship or parental authority over the then child. However, in the general view, it would be logical to seek the consent of the data subject again in order to continue processing his or her personal data (Brito, 2018).

3. Control of process of children

An issue that cannot go unnoticed if we analyse all the circumstances surrounding the processing of personal data relating to minors, as the special categories of data subjects that they are, is the way in which the controller seeks to verify the age of the child in order to corroborate the provision of consent, either by the child or by those exercising parental authority or guardianship. As can easily be seen, this situation poses serious difficulties in a context, such as the current one, strongly imbricated in the aforementioned information society, where the physical presence of the minor does not take place and, therefore, it is certainly difficult to verify his or her age.

In this regard, Article 8.2 GDPR, which we again endorse because of its importance for these purposes, establishes that:

> "[...] the controller shall make reasonable efforts to verify in such cases that consent was given or authorised by the holder of parental authority or guardianship over the child, taking into account available technology".

This indication seems to allude to minors under 16 years of age, being necessary, in these cases, that the consent be given or authorised by the person exercising parental authority or guardianship over the minor and only to the extent that this consent was given or authorised. Furthermore, the provision indicates that the effort made by the data controller must be reasonable, this being an indeterminate legal concept that may be qualified depending on the specific case.

In Spain, in 2010, the Spanish Data Protection Agency (hereinafter, AEPD) issued a report (Spanish Data Protection Agency, 2010) in which it established that the regulations then in force in Spain (LOPD/RDLOPD) did not establish a specific procedure to be followed by the data controller in order to verify the age of the child and the consequent authenticity of the consent given by the parents, guardians or legal representatives of the minor, granting the data controller the freedom to use the procedure it deems appropriate. In this sense, some authors (Cuadra, 2013; González, 2003) consider that this duty of the controller translates into an obligation to do and not into an obligation of result, so that, if the controller articulates the procedures it deems appropriate, documents them in a relevant manner and effectively verifies their compliance, it cannot be held responsible for any liability arising, for example, from the child having forged his or her National Identity Card or having photocopied that of the holder of parental authority or guardianship without the latter's consent (García, 2018). However, in order to comply more adequately and satisfactorily with the principle of proactive liability imposed by the GDPR, it is certainly favourable that the procedure established by data controllers be reasonable when verifying the identity of the minor, preferably requiring his or her digital signature.

Digital signatures, currently regulated, essentially and at Community level, in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on digital identification and trust services for digital transactions in the internal market and repealing Directive 1999/93/EC[16] (hereinafter, eIDAS Regulation or RIE-SCTE) , as well as, at national level, in Law 6/2020, of 11 November, regulating certain aspects of digital trust services[17]

---

[16] DOUE L 257/73 of 28 August 2014.

[17] BOE no. 298, of 12 November 2020. The purpose of this Act is to regulate certain aspects of digital trust services, as a complement to the eIDAS Regulation.
The purpose of this Act is to regulate certain aspects of digital trust services, as a complement to the eIDAS Regulation.
The entry into force of the LSEC implies the repeal, among others, of the LFE (which generated some problems of interpretation where it did not coincide with the RIE-SCTE), with the aim of adapting the legal system to the regulatory framework of the European Union, thus avoiding the existence of regulatory gaps that could give rise to situations of legal uncertainty in the provision of digital trust services. Likewise, article 25 of Law 34/2002, of 11 July, on information society services and digital commerce, referring to trusted third parties, is repealed, due to the fact that the services offered by this type of provider are subsumed in the types regulated by Regulation (EU) 910/2014, fundamentally in the services of certified digital delivery and the preservation of digital signatures and seals.
In view of the above, it is worth referring to the following most relevant measures incorporated by the LSEC: (a) it contemplates the regime envisaged for digital certificates, in which several provisions are introduced regarding the issuance and content of qualified certificates, whose maximum period of validity is maintained at five years; b) with regard to the identity and attributes of qualified certificates, those qualified certificates issued to natural persons shall in-

(hereinafter, LSCE) , which repeals Law 59/2003, of 19 December, on digital signatures[18] (LFE) , is a particularly suitable instrument to be able to accredit the consent we have been referring to. Next, we analyse digital signatures from a legal perspective (more specifically, digital signatures, a total of three, determining each of the three classes included in national and EU regulations), especially when the processing takes place in the sphere of Public Administrations, especially sensitised after the entry into force of the current Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations[19] (hereinafter, LPACAP) (Rodríguez, 2017).

3.1. Signature for general children's identification

Article 3(10) RIE-SCTE generally defines an digital signature as "[...] 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", or, in other words, any method or symbol based on digital means used or adopted by a party with the intention of signing, fulfilling all or some of the characteristic functions of a handwritten signature. The reference to its use with the intent to sign corresponds to the new regulation of other digital trust services that serve different purposes.

This definition shows the Community legislator's intention to regulate digital signatures in a broad sense, without prejudice to disciplining in more detail specific modalities to which, gradually, it attributes special legal effectiveness (in ascending order, as we shall see, advanced digital signatures and qualified digital signatures). It is also a technologically undefined concept (Martínez, 2004) (principle of technological neutrality), since it does not refer to any specific technology (cryptography, passwords, etc.) through which to sign, although it is true that it will be the asymmetric cryptography inherent to digital signatures that, in a veiled manner, presides over the rule as a whole. Moreover, the data making up the digital signature may form part of the digital document or be formally associated with it, appearing as an independent whole. However, whether digital signatures are integrated or separate will depend on the technical system selected and the practical applications of each type of digital signature.

According to this general notion, an digital signature could be, in contractual terms, any set of data based on digital means used by the signatory with the intention of signing, without specifying (in an attempt, I believe, to leave digital signatures open to as many purposes as successive technological developments will allow) the purpose of doing so. In this way, a kind of somewhat incomprehensible redundancy is created, which leads to defining the general digital signature as the one used by the signatory to sign.

On this point, the eIDAS Regulation departs from the definition contained in its predecessor, which, by providing a simple (Valero and Martínez, 2013) (non-general) concept of digital signature, limited the common purpose pursued by all digital signatures to serving as a means of authentication (Cruz, 2004)[20]. And this in a wording that is, in principle, debatable (Cruz, 2015; Alamillo, 2017) and confusing, since, as this authentication phase is subsequent to the identification phase proper, it would have been better to opt for the latter[21]. Nor is it made clear what is to be understood by authentication and identification, which places us before an indeterminate legal concept susceptible of generating radically different interpretations (Alamillo, 2017).

Be that as it may, the fact is that, with this new wording, the European standard generates a confusion

clude the ID card, NIE or NIF, except in cases where the holder lacks all of them, for which, exceptionally, the use of another identifying code or number is permitted, provided that it identifies the holder univocally and permanently over time, so that those issued to legal persons or entities without legal personality shall be identified by their company name and NIF; c) on the other hand, in application of the provisions of the eIDAS Regulation, the LSEC will mean that only natural persons will be authorised to sign digitalally.

The entry into force of the LSEC implies the repeal, among others, of the LFE (which generated some problems of interpretation where it did not coincide with the RIE-SCTE), with the aim of adapting the legal system to the regulatory framework of the European Union, thus avoiding the existence of regulatory gaps that could give rise to situations of legal uncertainty in the provision of digital trust services. Likewise, article 25 of Law 34/2002, of 11 July, on information society services and digital commerce, referring to trusted third parties, is repealed, due to the fact that the services offered by this type of provider are subsumed in the types regulated by Regulation (EU) 910/2014, fundamentally in the services of certified digital delivery and the preservation of digital signatures and seals.

In view of the above, it is worth referring to the following most relevant measures incorporated by the LSEC: (a) it contemplates the regime envisaged for digital certificates, in which several provisions are introduced regarding the issuance and content of qualified certificates, whose maximum period of validity is maintained at five years; b) with regard to the identity and attributes of qualified certificates, those qualified certificates issued to natural persons shall include the ID card, NIE or NIF, except in cases where the holder lacks all of them, for which, exceptionally, the use of another identifying code or number is permitted, provided that it identifies the holder univocally and permanently over time, so that those issued to legal persons or entities without legal personality shall be identified by their company name and NIF; c) on the other hand, in application of the provisions of the eIDAS Regulation, the LSEC will mean that only natural persons will be authorised to sign digitalally.

18 BOE no. 304, of 20 December 2003.

19 BOE no. 236 of 2 October 2015.

20 According to this provision, an digital signature is defined as "[...] data in digital form attached to or logically associated with other digital data and used as a means of authentication". The origin of the use of this term by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for digital signatures - OJEC L 13/12 of 19 January 2000 - (hereinafter DFE) refers directly to the Anglo-Saxon concept of authentication, conceived as the essence of the act of signing, the act of signing the document.

21 Article 3(1) RIE-SCTE defines digital identification as the process of using a person's identification data [i.e. the set of data that makes it possible to establish the identity of a natural or legal person, or of a natural person representing a legal person - Article 3(3)-] in digital form, being the data that uniquely represents a natural or legal person or a natural person representing a legal person.

that is by no means negligible. Indeed, while the previous regulation defined the minimum that an digital signature had to meet to be considered as such for legal purposes (identification of the signatory of a data message or authentication or accreditation of that identification), the RIE-SCTE, despite the plausible intention presumably pursued, makes it impossible for the legal practitioner to specify the element that, satisfied, would allow us to know when we are in the presence of an digital signature, however basic or elementary it may be. Consequently, this definition would include multiple signature procedures, some as complex as the digital signature based on asymmetric cryptography or the signature configured on the basis of biometric systems such as the iris, the palm of the hand or the fingerprint, and others as simple as the inclusion of the name or other identifying element at the end of an digital message, the digitalised handwritten signature or the existence of a question-answer and an access PIN (Buonomo and Merone, 2013; García, 2003; Escolano, 2005; Vattier, 2003). As a result of the foregoing, we are in a position to affirm that, if the aim pursued is to generate certainty in those who are subject to and directly or indirectly affected by the rule, it would be more appropriate to reformulate the current concept of general digital signature and redirect it, with nuances, to the traditional simple digital signature, in a sort of definition, at least somewhat more clarifying or complete, which could be as follows: the digital signature is the set of data in digital format, attached to other digital data or logically associated with them, which are used, at least, as a means of identification of the signatory.

3.2. Identification and integrity

Raising the quality and security requirements for digital signatures, Article 3(11) RIE-SCTE introduces the concept of advanced digital signature, which is understood as "[...] an digital signature that meets the requirements set out in Article 26".

These requirements, the latter provision adds, are as follows:

a. be uniquely linked to the signatory;
b. allow the digital identification of the signatory (González-Echenique, 2020) (minor or holder of parental authority for, in this case, giving consent to processing operations in which the controller is the Public Administration);
c. be created using digital signature creation data that can be used by the signatory for the creation of an digital signature, with a high level of confidence (Díaz, 2018)[22], under his exclusive control; and
d. linked to the data signed by it in such a way that any subsequent modification of the data is detectable.

It should be noted that the first three requirements (unique linkage to the signatory, identification of the signatory and creation by means under the signatory's exclusive control) are intended to ensure the authenticated identification of the author and to prevent the rejection of data messages at source, while the last requirement (linkage to the data so that any subsequent alteration can be detected) is intended to safeguard the integrity of digital documents.

3.3. Secure identification and integrity

Finally, Article 3(12) of the RIE-SCTE defines a qualified digital signature (introducing a new name at Community level for what, since Law 59/2003 of 19 December 2003 on digital signatures, has been known in Spain as a qualified digital signature) as an "[...] advanced digital signature that is created by means of a qualified digital signature creation device and is based on a qualified digital signature certificate".

Rather than a new form, the qualified digital signature constitutes a new type of advanced digital signature which, accompanied by certain elements that make it more secure (qualified digital signature creation device, on the one hand, and qualified digital signature certificate, on the other), will have "[...] a legal effect equivalent to that of a handwritten signature" (Article 25.2 RIE-SCTE). For this reason, it is invested with a new nomen iuris, with the aim of distinguishing it from that other signature which, because it has not been created by means of a qualified digital signature creation device or because it is not based on a qualified digital signature certificate (or because it does not meet either of these two requirements), will not have legal effects comparable, in terms of validity and effectiveness, to those of a handwritten signature, being integrated under the name of advanced digital signature. The latter, like the simple digital signature and the advanced digital signature based on a qualified digital certificate, will not be deprived of legal effects or admissibility as evidence in legal proceedings merely because it is in digital form or because it does not meet the requirements of the qualified digital signature (Article 25.1 RIE-SCTE), and it must be assessed, in any event, how effective it is, which can sometimes be complex and costly.

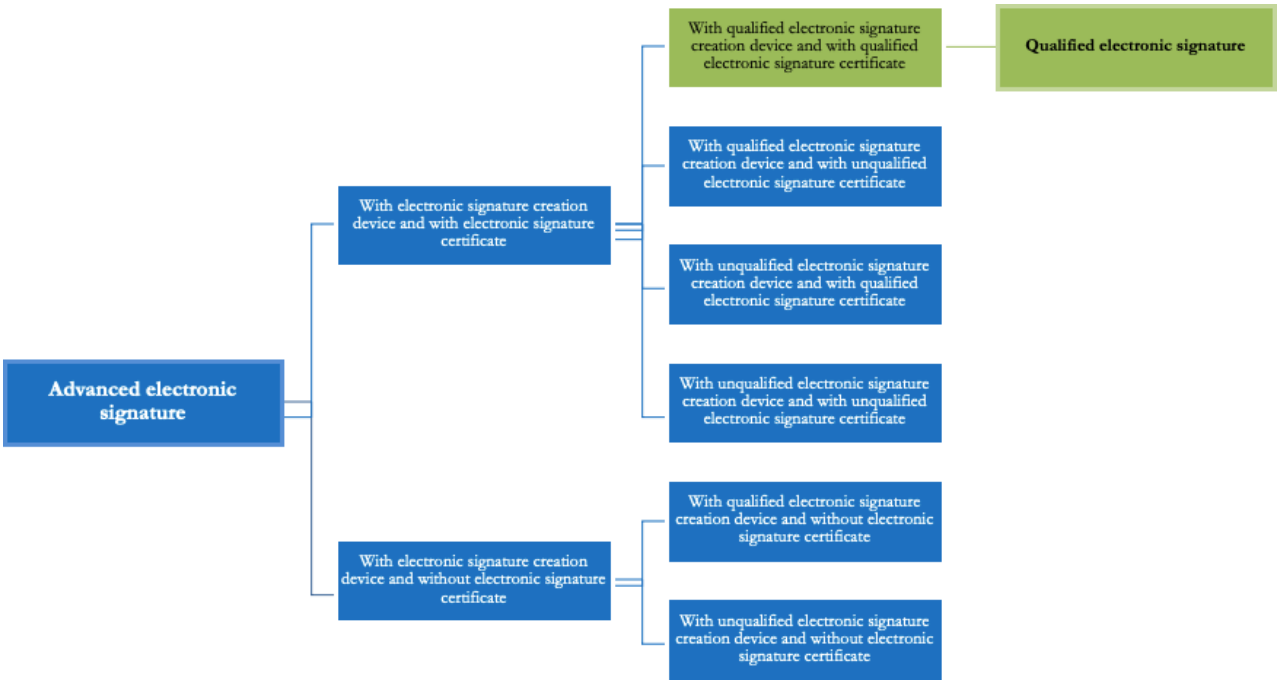
It is this greater legal certainty that justifies the fact that Article 10 LPACAP, among the signature systems admitted by the Public Administrations, considers qualified digital signatures to be preferential, so that, according to the second paragraph of this provision:

> "In the event that the interested parties opt to relate with the Public Administrations by digital means, the following shall be considered valid for signature purposes:

[22] With the expression "[...] can use, with a high level of confidence", the RIE-SCTE moves closer to the DFE and the LFE (and away from the RDLFE, which eliminates all probability in this respect), which we consider to be correct, since the link between the signature and the signatory is a probable link, conditional on the technical means.

(a) Qualified and advanced digital signature systems based on qualified digital certificates of digital signature issued by providers included in the ‘’Trusted List of Certification Service Providers”.

Finally, the regulation introduces certain substantial modifications with respect to the previous body, including the creation of a specific regulation for the use of digital signatures by legal persons; the explicit acceptance of the representation relationships that may underlie the use of digital signatures; the addition of a special regime for the issuance of digital certificates to entities without legal personality, for the sole purpose of their use in the tax sphere; the incorporation of the term qualified digital signature to refer to that which is legally equivalent to a handwritten signature; the incorporation into the ID card of identification and digital signature facilities, expressly providing for the existence of an digital ID card; the incorporation into the ID card of identification and digital signature facilities, expressly providing for the existence of an digital signature; the incorporation of the term qualified digital signature to refer to a signature that is legally equivalent to a handwritten signature; the incorporation of identification and digital signature facilities into the ID card, expressly providing for the existence of an digital ID card, which will be fully effective in terms of the integrity and authenticity of the digital communications carried out through it; increasing the importance of the private sector and self-regulation in the certification systems of information society service providers, thereby encouraging the development of voluntary accreditation systems; strengthening the inspection and control capacities of these certification service providers; the elimination of certain administrative aspects, such as the registration of PSSIic, which is replaced by a simple information dissemination service on these providers, on quality certifications and on the characteristics of the products and services they have for the development of their activity, or, finally, the clarification of the economic guarantees to be provided by trust service providers issuing recognized certificates (De Miguel, 2015).



4. References across the legislation

As indicated in previous pages, there are several references to minors throughout the new Community legislation on the protection of personal data. More specifically, these references are contained in Recitals 38, 58, 65 and 75, as well as in Articles 6(1)(f), 12(1), 40(2)(g) and 57(1)(b) of the General Data Protection Regulation. Aspects relating to minors will also be provided in Articles 84 and 92, as well as in Additional Provision 19, all of the new Organic Law on Data Protection.

In the first of these references, Recital 38 GDPR, we find, at the end, an exception to the consent given by the person exercising parental authority or guardianship over the child. According to this recital, the consent given by the holder of parental authority or guardianship should not be indispensable in the context of services of a preventive or advisory nature, proposed directly to minors.

For its part, connected in an immanent way to the principle of transparency of Article 5.1.a) GDPR (Troncoso, 2018), is Recital 58 GDPR, which, when analysing the set of circumstances that must be informed to data subjects, provides that, when this information covers processing operations involving minors, this information must be provided in clear and simple language that is accessible to the child.

Thirdly, Recital 65 of the GDPR, referring to the right of erasure, contemplates the case of consent, once given by the child, which is subsequently sought to be withdrawn by the child. In this context, the recital states that the data subject must be able to avail himself of this right even if, at the time of exercising the aforementioned right, he had already reached the age of 18.

A final analysis of the recitals of the Community legislation on data protection leads us to analyse Recital 75 of the GDPR. One of the new features of the GDPR is the risk perspective, by virtue of which it will be necessary to carry out a risk analysis prior to processing in order to determine the set of security measures appropriate to such processing. In this regard, the aforementioned recital establishes a series of aspects that may entail situations of risk in relation to the processing of the data subject's personal data, referring, among these specific situations or aspects, to those processing operations that affect particularly vulnerable persons, in particular minors. This is related to the provisions of Article 9 GDPR, which regulates the processing of special categories of personal data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data intended to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), where, despite the above, no reference is made to personal data relating to children, which leads us to affirm that the personal data of minors shall not be considered as special categories of personal data, regardless of the fact that this type of processing is subject to certain specificities that seek to protect with greater intensity the rights corresponding to this special category of data subjects. This would allow us to affirm that, in connection with Article 24 GDPR (which regulates the responsibility of the controller -in this case, the Public Administrations-, the adoption of appropriate technical and organisational measures will be necessary to protect, comply with and be able to demonstrate compliance with the processing carried out on the personal data of minors.

With regard to the articles, the first of these is Article 6 GDPR, whose letter f), located in its first paragraph, refers to the processing necessary to meet the legitimate interests pursued by the controller, being, in these cases, necessary that such legitimate interests never predominate over the interests or fundamental rights and freedoms of the data subject that require guaranteeing his personal data, especially in those cases in which we are in the presence of minors (Fernández and Fernández, 2019). In short, the controller may legitimise its processing of the data subject's personal data, even when the data subject is a child, on the basis of the legitimate interest pursued, provided that this legitimate interest never prevails over that of the data subject, in particular when the data subject is a particularly vulnerable person, such as a minor.

However, and as far as we are concerned here, this legal basis finds an exception in those cases where the processing is carried out by public authorities in the performance of their functions. In this case, it is understood that, even in the case of minors, the protection safeguard provided for in the final paragraph of Article 6(1)(f) of the GDPR may not apply, so that when the controller is a public authority and is performing its functions, the legitimate interest pursued by the authority will prevail over the legitimate interest of the data subject, in this case, the minor.

Secondly, there is the first paragraph of Article 12 GDPR, which regulates transparency in providing information about the circumstances surrounding the processing of personal data and the rights to which the data subject is entitled. This paragraph provides that the information to be provided to the data subject must be particularly concise, transparent, intelligible, easily accessible and in clear and simple language when the data subject is a minor.

Thirdly, letter g) of the second paragraph of Article 40 GDPR, connected with the previous point, establishes that the information to be provided to minors and the protection to be afforded to them, as well as the manner of obtaining the consent of those exercising parental authority or guardianship over the minor, constitute aspects that the General Data Protection Regulation seeks to incorporate in the codes of conduct which, in accordance with this provision, the different countries that make up the European Union, the supervisory authorities, the Committee and the Commission will have to promote.

Finally, letter b) of the first paragraph of Article 57 GDPR, when speaking of the functions corresponding to the supervisory authority, establishes that, regardless of any other functions attributed to them in other sections of the regulations on personal data protection, there shall be a total of 22, including a second, which makes special reference to the attention to be shown in those activities specifically aimed at minors in order to facilitate their better awareness and understanding of the risks, rules, guarantees and rights related to the processing of their personal data (Rodríguez, 2020).

For its part, in the domestic legal system, we find, in the first place, Article 84 LOPDGDD, which establishes that parents, guardians, curators or legal representatives shall ensure that minors make a balanced and responsible use of digital devices and information society services, with the aim of guaranteeing the appropriate development of their personality and preserving their dignity and fundamental rights. Similarly, the use or dissemination of images or personal information of minors on social networks and equivalent information society services that may imply an unlawful interference in their fundamental rights will determine the intervention of the Public Prosecutor's Office, which will request the precautionary and protective measures provided for in Organic Law 1/1996, of 15 January, on the Legal Protection of Minors,

partially amending the Civil Code and the Civil Procedure Act[23].

For its part, Article 92 LOPDGDD adds that:

> "Educational centres and any natural or legal persons carrying out activities involving minors shall guarantee the protection of the best interests of minors and their fundamental rights, especially the right to the protection of personal data, in the publication or dissemination of their personal data through information society services. When such publication or dissemination is to take place through social networking services or equivalent services, they must have the consent of the minor or their legal representatives, in accordance with the provisions of Article 7 of this Organic Law".

Finally, the nineteenth additional provision of the LOPDGDD concludes by stating that, within one year of the entry into force of this Organic Law, the Government shall submit to the Congress of Deputies a draft law specifically aimed at guaranteeing the rights of minors in the light of the impact of the Internet, in order to guarantee their security and combat the discrimination and violence exercised against them by means of the new technologies.

In short, as we have been able to observe in the previous lines, there are numerous allusions and references which, in order to protect the rights and freedoms of the data subject who is a minor, are established in the new regulations on the protection of personal data, granting and guaranteeing better conservation to this special category of data subjects.

It follows that the Community institutions need to protect the personal data of minors by applying a series of principles that must be in force when obtaining personal data relating to this group of data subjects:

a. Children may not provide personal information relating to other data subjects.
b. In order to transfer personal data relating to minors to third countries or international organisations, it will be necessary to obtain the explicit and demonstrable consent of those exercising parental authority or guardianship over the child, which, as we have seen, must be given by means of instruments that securely guarantee the provision of the consent, in particular, digital signatures.
c. It is prohibited to induce minors to provide information of a personal nature by obtaining prizes or similar inducements.
d. It will be necessary to temporarily limit the validity of the consent given by those exercising parental authority or guardianship over the child.

Otherwise, in the area of social networks, consent may be obtained by creating a user account. However, in the case of minors, ideally, as mentioned above, such platforms should be able to make use of electronic signature mechanisms, in order to ensure secure identification of the user and thus prevent minors from giving consent without their representatives being able to do so instead.

5. Conclusions

Throughout this paper we have been able to dissect the fundamental elements of consent as the quintessential and fundamental legal basis for the processing of personal data of minors in the context of Public Administrations. To this end, we have established the need for this consent to be provided by the holders of parental authority or guardianship over the child when, in accordance with the provisions established, firstly and at Community level, by the GDPR, and subsequently and at national level, the LOPDGDD, the child is under fourteen years of age.

Similarly, once the applicable legal basis has been verified as a matter of priority, it is necessary to analyse how to verify this consent virtually, remotely and in the different procedures to be carried out before the Public Administrations. In this respect, the existence and usefulness of the digital signature as a basic trust service, which is undergoing a new configuration under the protection of the European RIESCTE, recently embodied in Spain through the LSEC, has been confirmed; Specifically, the three modalities presented by this instrument in the new regulation have been described and the properties that can be guaranteed by each of them have been dissected, reaching the conclusion that it is only the qualified digital signature that, due to the greater legal-technical security it offers, should be used in relations with the Public Administrations, to the extent that it is the latter that have decidedly opted for this security mechanism, the only one which, for legal purposes, is equivalent to the traditional handwritten signature.

Finally, and to conclude by highlighting the importance of minors in current privacy regulations, as a result of the reinforcement sought of the position of the data subject as the owner of his or her personal data, the different references have been analysed, all of them fundamental, which determine the fulfilment of additional or reinforced obligations on the part of data controllers and data processors..

6. Bibliography

Alamillo Domingo, I. (2017). "Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos", Fernández Ramos, S., Valero Torrijos and Gamero Casado, J. E. (dirs.). *Tratado*

[23] BOE no. 15 of 17 January 1996.

de Procedimiento Administrativo Común y Régimen Jurídico Básico del sector público. Valencia: Tirant lo Blanch, pp. 675-768.

Alemán Monterreal, A. (2011). "La protección de datos de menores en el ámbito sanitario: ¿discriminación necesaria?", *Actualidad Civil*, 19: 551-575.

Andreu Martínez, B. (2013). *La protección de datos personales de los menores de edad*. Cizur Menor: Thomson Reuters Aranzadi.

Arias Pou, M. (2006): *Manual práctico de comercio electrónico*. Las Rozas: La Ley.

Brito Izquierdo, N. (2017). "Tratamiento de los datos personales de menores de edad: supuestos, límites, retos y desafíos", *La Ley Derecho de Familia: Revista Jurídica sobre Familia y Menores*, 14: 17-31.

Brito Izquierdo, N. (2018). "Tratamiento de los datos personales de menores de edad en la nueva normativa europea protectora de datos personales", *Actualidad civil*, 5.

Buonomo, G. and Merone, A. (2013). "La scrittura privata informatica: firme elettroniche, valore probatorio e disconoscimento in giudizio (alla luce delle modifiche introdotte dalla l. 221/2012)", *Judicium: il processo civile in Italia e in Europa*, 1: 12-22.

Cruz Rivero, D. (2004), "Las definiciones de firma electrónica en el Real Decreto-ley 14/1999, sobre firma electrónica, y el Proyecto de Ley de firma electrónica", DAVARA Rodríguez, M. Á. (coord.), *XVIII Encuentros sobre Informática y Derecho, 2003-2004*. Madrid: Universidad Pontificia de Comillas, pp. 127-136.

Cruz Rivero, D. (2015). *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de 19 de diciembre, de firma electrónica*. Madrid: Marcial Pons.

Cuadra Chiong, M. M. (2013). "La protección de datos personales de los menores de edad", *Anuario de justicia de menores*, 13: 515-516.

De Las Heras Vives, L. and De Verda Y Beamonte, J. R. (2019). "Consentimiento de los menores de edad", Arenas Ramiro, M. and Ortega Giménez, A. (dirs.), *Protección de datos: comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el GDPR)*. Madrid: Sepin Editorial Jurídica, pp. 73-77.

Díaz Moreno, A. (2017). "Concepto y eficacia de la firma electrónica en la Directiva 1999/93/CE, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica", *Revista de la Contratación Electrónica*, 2: 10-32.

De Miguel Asensio, P. A. (2015). *Contratación electrónica*: Cizur Menor: Aranzadi.

Durán Ruiz, F. J. (2013). "La necesaria intervención de las administraciones públicas para la preservación del derecho fundamental a la protección de datos de los menores de edad", Durán Ruiz, F. J. (coord.). *I Congreso sobre retos sociales y jurídicos para los menores y jóvenes del siglo XXI*. Granada: Comares.

Durán Ruiz, F. J. (2019). "El tratamiento de los datos personales de los menores de edad en la nueva normativa de protección de datos", Quesada Páez, A., Moreno Cordero, G., García Garnica, M. C. and Marchal Escalona, N. (dirs.). *Aproximación interdisciplinar a los retos actuales de protección de la infancia dentro y fuera de la familia*. Cizur Menor: Thomson Reuters Aranzadi, pp. 473-482.

Escobar Roca, G. (2017): *Informe 2016. Monographic issue: data protection of minors*, Madrid: Trama.

Fernández Samaniego, J. and Fernández Longoria, P. (2019). "El interés legítimo como principio para legitimar el tratamiento de datos", Rallo Lombarte, A. (coord.), *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales*. Valencia: Tirant lo Blanch, pp. 169-196.

García Herrera, V. (2018). "El válido consentimiento para el tratamiento de los datos personales de los menores de edad en Internet. Especial referencia al supuesto en que los representantes legales estén divorciados o separados", *La Ley Derecho de Familia: revista jurídica sobre familia y menores*, 20: 62-71.

García Más, F. J. (2005). "El documento público electrónico (1)", Escolano Navarro, J. J. (coord.), *Nuevas tecnologías en la contratación, sociedad nueva empresa e hipoteca electrónica: seminario organizado por el Consejo General del Notariado en la UIMP en julio de 2003*. Madrid: Civitas, pp. 113-132.

Gómez-Juárez Sidera, I. (2006). "Reflexiones sobre el derecho a la protección de datos de los menores de edad y la necesidad de su regulación específica en la legislación Española", in *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 11: 71-88.

González-Echenique Castellanos de Ubao, L. (2020). "Estudio de la Directiva y del Real Decreto-Ley de 17 de septiembre de 1999 sobre firma electrónica", Mateu de Ros Cerezo, R. and Cendoya Méndez De Vigo, J. M. (coords.), *Derecho de Internet: la contratación electrónica y firma digital*. Cizur Menor: Thomson Reuters Aranzadi, pp. 207-260.

González Madrid, C. (2003). "Los datos de menores en el ámbito de la educación", Datospersonales.org: *la Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, 2: 1-16.

Guillén Catalán, R. (2015). "Los retos de la sociedad ante la protección de datos de los menores", *Revista Boliviana de Derecho*, 20: 324-343.

Article 29 Working Group (2017). *Guidelines on transparency under Regulation (EU)* 2016/679, 17/ES, WP260 rev.01, 29 November.

Hidalgo Cerezo, A. (2017). "La protección de datos de los menores de edad. Especial referencia a sus excepciones en materia sanitaria y de educación", *La Ley Derecho de Familia: Revista Jurídica sobre Familia y Menores*, 15.

Martínez Nadal, A. (2004). *Comentarios a la Ley 59/2003 de firma electrónica*. Madrid: Civitas.

Palma Ortigosa, A. (2018). "Ámbito de aplicación y definiciones del GDPR", Murga Fernández, J. P., Fernández Scagliusi, M. Á., and Espejo Lerdo De Tejada, M. (dirs.), *Protección de datos, responsabilidad activa técnicas de garantía*. Madrid: Reus, pp. 25-38.

Piñar Real, A. (2016). "Tratamiento de datos de menores de edad", Piñar Mañas, J. L. (dir), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Reus, pp. 187-204.

Plaza Penadés, J. (2013). "La Ley de servicios de la sociedad de la información y comercio electrónico", Plaza Penadés, J., Vázquez De Castro, E., Guillén Catalán, R. and Carbajo Cascón, F. (coords.), *Derecho y nuevas tecnologías de la información y la comunicación*. Cizur Menor (Navarra): Thomson Reuters Aranzadi, pp. 43-102.

Rodríguez Ayuso, J. F. (2017). "Servicios de confianza en materia de transacciones electrónicas: el nuevo Reglamento europeo 910/2014", Pérez Gallardo, L., *Contratación electrónica y protección de los consumidores: una visión panorámica*. Madrid: Reus, pp. 133-162.

Rodríguez Ayuso, J. F. (2018). *Ámbito contractual de la firma electrónica*. Barcelona: Bosch.

Rodríguez Ayuso, J. F. (2019). *Figuras y responsabilidades en el tratamiento de datos personales*. Barcelona: Bosch.

Rodríguez Ayuso, J. F. (2020). *Control externo de los obligados por el tratamiento de datos personales*. Barcelona: Bosch.

Troncoso Reigada, A. (2008). "Transparencia administrativa y protección de datos personales", Troncoso Reigada, A. (coord.), *Transparencia administrativa y protección de datos personales: V Encuentro entre Agencias Autonómicas de Protección de Datos Personales: celebrado el día 28 de octubre de 2008 en la Real Casa de Correos de Madrid.* Madrid: Agencia de Protección de Datos de la Comunidad de Madrid, pp. 123-188.

Valero Torrijos, J. and Martínez Gutiérrez, R. (2013). "Las bases jurídicas de la modernización tecnológica en las Administraciones públicas", Plaza Penadés, J. (coord.), *Derecho y nuevas tecnologías de la información y la comunicación*. Cizur Menor: Aranzadi, pp. 479-544.

Vattier Fuenzalida, C. (2003). "De nuevo sobre el régimen legal de la firma electrónica: estudio del Anteproyecto de 26 de junio de 2002", *Actualidad civil*, 1: 137- 152.

Juan Franciso Rodríguez Ayuso. Licenciado en Derecho y en Administración y Dirección de Empresas desde el año 2011, ambas por la Universidad de Córdoba. Doctor en Derecho digital por la Universidad de Bolonia (Italia). Profesor Ayudante Doctor y docente en las asignaturas "Nuevas Tecnologías y Derecho", dentro del Máster de Propiedad Intelectual y Derecho de las Nuevas Tecnologías; "Derechos del Ciudadano y Obligaciones del Responsable (I) y (II)", dentro del Máster en Protección de Datos; "Derecho de Internet", dentro del Grado en Derecho, y "Derechos Humanos, Nuevas Tecnologías y Bioderecho", dentro del Máster en Derechos Humanos. Todas ellas son impartidas en la Universidad Internacional de La Rioja.