Revista Digital de Derecho Administrativo
ISSN: 2145-2946
Universidad Externado de Colombia

Rodríguez Ayuso, Juan Francisco

The Provision by Public Authorities of Safe Environments for Particularly Sensitive Citizen Interaction: The Situation at the European Level

Revista Digital de Derecho Administrativo, núm. 26, 2021, Julio-Diciembre, pp. 285-310
Universidad Externado de Colombia

DOI: https://doi.org/10.18601/21452946.n26.10

The Provision by Public Authorities of Safe Environments for Particularly Sensitive Citizen Interaction: The Situation at the European Level

Juan Francisco Rodríguez Ayuso[1]

ABSTRACT

The main objective of this research study is to offer a systematic analysis of consent in minors and the processing of personal data under the General Data Protection Regulation and the Organic Law on the Protection of Personal Data and the Guarantee of Digital Rights. Specifically, besides studying consent in depth, as a fundamental legal basis, we dissect the essential contours of the e-signature as the most suitable instrument for guaranteeing the provision of this consent, focusing on the special features that this presents when those who intervene as controllers are Public Administrations.

1 Doctor en Derecho Administrativo acreditado por ANECA y coordinador académico del Máster en Protección de Datos de la Universidad Internacional de La Rioja (UNIR), La Rioja, España. Correo-e: juanfrancisco.rodriguez@unir.net. Enlace ORCID: https://orcid.org/0000-0003-4721-1465. Fecha de recepción: 10 de febrero de 2021. Fecha de modificación: 10 de abril de 2021. Fecha de aceptación: 10 de mayo de 2021. Para citar el artículo: Rodríguez Ayuso, Juan Francisco, "The Provision by Public Authorities of Safe Environments for Particularly Sensitive Citizen Interaction: The Situation at the European Level", *Revista digital de Derecho Administrativo*, Universidad Externado de Colombia, n.º 26, 2021, pp. 285-310. DOI: https://doi.org/10.18601/21452946.n26.10.

Keywords: General Data Protection Regulation, Processing, Personal data, Minors, Public Administrations.

Habilitación por organismos públicos de entornos seguros de interacción ciudadana especialmente sensible: estado de la cuestión a nivel europeo

RESUMEN

El objetivo principal del presente estudio de investigación es ofrecer un análisis sistemático del consentimiento en el tratamiento 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. En concreto, además de profundizar en el consentimiento como base jurídica fundamental, se diseccionan los contornos esenciales de la firma electrónica como un 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.

Palabras clave: Reglamento General de Protección de Datos, tratamiento datos personales, menores de edad, Administraciones públicas.

STATEMENT OF THE ISSUE

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. This repealed Directive 95/46/EC[2] (hereinafter General Data Protection Regulation or GDPR) regulating personal data relating to minors in a new way, since this issue was not specifically addressed in previous legislation, largely based on the system provided by the Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995. This being the directive previously

2 Official Journal of the European Union (hereinafter referred to as DOUE) L 119/1 of 04 May 2016.

applied to the protection of individuals, with regard to the processing of personal data and on the free movement of such data[3] (hereinafter, GDPR).

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, on the Protection of Personal Data and Guarantee of Digital Rights[4] (hereinafter, LOPDGDD) came into force. This regulation included, by virtue of its Single Repealing Provision, the repeal of Organic Law 15/1999 on personal data protection[5] (hereinafter, LOPD) and The Royal Decree-Law 5/2018, of 27 July. This included 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 contradicted, opposed or were subsequently deemed incompatible with the provisions of the GDPR and the present LOPDGDD[7]. This new Organic Law will also make a specific and relevant concluding statement on the special processing of personal data relating to minors.

In accordance with the most relevant international indicators, when minors are mentioned, it is 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[8]. Over the last few years, a large part of the doctrine[9] 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 a variation of the previous interchangeably, as well the notions of minors.

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) n.º 294, of 06 December 2018.

5 BOE, n.º 298 of 14 December 1999.

6 BOE, n.º 183 of 30 July 2018.

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*, n.º 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 BELÉN ANDREU MARTÍNEZ, *La protección de datos personales de los menores de edad*, Cizur Menor: Thomson Reuters Aranzadi, 2013, p. 37.

9 Among others, ALBERTO HIDALGO CEREZO, "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*, n.º 15, 2017; ALICIA PIÑAR REAL, "Tratamiento de datos de menores de edad", in José Luis Piñar Mañas (dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Madrid: Reus, 2016, pp. 190-191.

The Article 29 Working Group[10] also defines them as human beings in the exact sense of the word (who are also under 18 years of age)[11]. Precisely for this reason, a minor should enjoy all the rights that correspond to a person, including, the fundamental right to the protection of their personal data[12].

In this sense, Article 8 GDPhas included, for the first time in the Community regulatory framework specific references 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 electronic communications sector (Directive on privacy and electronic communications)[13] included any specific mention of minors. Beyond this, in Spain and on the basis of this provision of the GDPR, several other articles come to explain somewhat more generic Community related content these will be, in essence, Articles 7, 84 and 92, in addition to the 19th Additional Provision, all of them, without exception, apply, the new LOPDGDD.

In accordance with this Community precept, a number of conditions were established which explicitly regulate the Conditions that are applicable to the child consent, 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 authorized 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 authorized by the holder of parental responsibility or guardianship over the child, taking into account available technology.

10 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).

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

12 Francisco Javier Durán Ruiz, "El tratamiento de los datos personales de los menores de edad en la nueva normativa de protección de datos", in Abigail Quesada Páez, Gisela Moreno Cordero, María del Carmen García Garnica y Nuria Marchal Escalona (dirs.), *Aproximación interdisciplinar a los retos actuales de protección de la infancia dentro y fuera de la familia*, Cizur Menor: Thomson Reuters Aranzadi, 2019, p. 480.

13 DOCE L 201/37 of 31 July 2002.

> 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, it cannot necessarily be stated that, throughout this period of time, the processing of personal data of children had been in a situation of legal uncertainty. The fact being that minors have always had the right to privacy and 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[14]. 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 and regardless of their legal status within the European Union[15]. In this sense, the first paragraph of Article 4 of the GDPR[16], when referring to the concept of the data subject, does not establish any distinction or differentiation based on the nationality or situation of the natural person under analysis. Minors coming from non-EU territories are becoming increasingly more common and their data more important, which is also of great relevance. Despite this, that particular area is in fact, beyond the scope of this study. To conclude, there will be an opportunity to analyze, although both the GDPR and the new LOPDGDD their inclusion of provisions

14 On this issue, *vid*. Francisco Javier Durán Ruiz, "La necesaria intervención de las administraciones públicas para la preservación del derecho fundamental a la protección de datos de los menores de edad", in Francisco Javier Durán Ruiz (coord.), *I Congreso sobre Retos Sociales y Jurídicos para los Menores y Jóvenes del siglo XXI,* Granada: Comares, 2013; Isidro Gómez-Juárez Sidera, "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", *Revista Aranzadi de Derecho y Nuevas tecnologías*, n.º 11, 2006, pp. 71-88; Raquel Guillén Catalán, "Los retos de la sociedad ante la protección de datos de los menores", *Revista Boliviana de Derecho*, n.º 20, 2015, pp. 324-343.

15 Adrián Palma Ortigosa, "Ámbito de aplicación y definiciones del GDPR", in Juan Pablo Murga Fernández, María de los Ángeles Fernández Scagliusi and Manuel Espejo Lerdo de Tejada (dirs.), *Protección de datos, responsabilidad activa técnicas de garantía*, Madrid: Reus, 2018, p. 27.

16 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.

related to the processing of the personal data of minors and their numerous references to children, 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 to complete 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[17].

1. LEGAL ISSUES TO CONSIDER IN VIEW OF THE NECESSARY LEGAL JUSTIFICATION FOR THE PROCESSING OF DATA OF MINORS: CONSENT AS A TRADITIONAL PRIVACY AND PUBLIC INTERACTION ENABLING

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 authorized. 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) was created, which alters this minimum age, in general terms, to 14 years of age[18] and does so in the following terms:

17 Luis de las Heras Vives and José Ramón de Verda y Beamonte, "Consentimiento de los menores de edad", in Mónica Arenas Ramiro and Alfonso Ortega Giménez (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, 2019, p. 74.

18 However, in the initial LOPDGDD Proposal, the minimum age foreseen was 13 years old.

> 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 in this, is what can be understood as 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 electronic commerce, in the Internal Market (hereinafter referred to as the Directive on electronic commerce or the DCE)[19], 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[20], 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[21].

According to this provision, an information society service is defined as: "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). It is conducted by electronic means, where it is sent from the source and received by the recipient of information society services by means of electronic equipment for the processing (including digital compression) and storage of data. This data is transmitted, conveyed

19 DOCE L 178/1 of 17 July 2000.

20 DOCE L 204/37 of 21 July 1998.

21 DOCE L 217/18 of 5 August 1998.

and received in its entirety by wire, radio, optical or any other electromagnetic means[22], 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 are involved and 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[23].

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, however, because they also represent 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 service is of essential note, since what is included is any activity carried out electronically 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[24].

Thus, all those who receive economic remuneration 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.

Our domestic legal system has applied in practically identical terms, Law 34/2002, of 11 July, on information society services and electronic commerce[25] (hereinafter, LSSICE), which 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 characterized by four essential aspects

22 As pointed out by Javier Plaza Penadés, "La Ley de servicios de la sociedad de la información y comercio electrónico", in Javier Plaza Penadés, Eduardo Vázquez de Castro, Raquel Guillén Catalán and Fernando Carbajo Cascón (coords.), *Derecho y nuevas tecnologías de la información y la comunicación,* Cizur Menor: Thomson Reuters Aranzadi 2013, p. 46, what they want to make clear is that the ISS in question must be provided through a communication network, regardless of how the access to the network takes place, whether by mobile phone, television or computer.

23 Ana Alemán Monterreal, "La protección de datos de menores en el ámbito sanitario: ¿discriminación necesaria?", *Actualidad Civil,* n.º 19, 2011; María Arias Pou, *Manual práctico de comercio electrónico,* Las Rozas: La Ley, 2006, p. 60.

24 On this issue, *vid.* Juan Francisco Rodríguez Ayuso, Ámbito contractual de la firma electrónica, Barcelona: Bosch, 2018, pp. 33-34.

25 BOE, n.º 166, of 12 July 2002.

that must cumulatively concur: they must be provided at a distance, by electronic means, at the individual request of the recipient of information society services and, at least usually, for consideration. Based on the Explanatory Memorandum, within the concept of information society services, the third section includes, electronic commerce, which, in turn, includes two fundamental activities that group together the rest. On one hand, the sending of commercial communications prior to contracting, which groups together the supply of information by telematic means, and, on the other, electronic contracting itself, which includes both the organization and management of auctions by electronic means or of virtual markets and shopping centers, and the management of purchases on the Internet by groups of people. The means through which this contracting can be channeled are, among others, e-mail, web page, videoconference, or chat.

To the above be added, as those information society intermediation services that relate to the provision of access to the Internet (Internet service providers). In particular those services allowing the transmission of data over telecommunications networks (via conduit or routing), concerning the temporary copying of Internet pages requested by users (proxy caching or buffering), the hosting of information, services or applications provided by others on their own servers, providing search tools or links to other Internet sites (searching and linking), enabling the creation, verification and validation of electronic signatures, electronic seals, electronic time stamps, certified electronic delivery services, certificates relating to these services and certificates for the authentication of websites, and the preservation of electronic signatures, seals or certificates relating to these services (trust services) and/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.

Returning to the consent of minors, the General Data Protection Regulation clearly distinguishes between the following possible scenarios[26]:

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

26 Noemí Brito Izquierdo, "Tratamiento de los datos personales de menores de edad: supuestos, límites, retos y desafíos", *La Ley Derecho de Familia*, n.º 14, 2017, pp. 18-20.

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 are paramount. 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 best interests of the child in every case[27].

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 sates. In this case, it leaves 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, 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[28]. It is true that it would have been highly advisable for the specific content of Article 8 GDPR to have stated this circumstance, although, as previously mentioned 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 to information society services only, it would not be appropriate to infer that this would leave out the regulatory framework of 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,

27 Guillermo Escobar Roca, *Informe 2016. Monographic issue: data protection of minors*, Madrid: Trama, 2017.

28 Juan Francisco Rodríguez Ayuso, *Figuras y responsabilidades en el tratamiento de datos personales*, Barcelona: Bosch, 2019.

when the latter, immediately afterwards, reaches the age of majority. It isn't yet known, unless the appropriate interpretative work is carried out, what would happen with this consent. Various questions arise here. Would it be necessary to seek consent again, this time directly from the minor? Could it be possible to extend the effects of the consent given by the holder of guardianship or parental authority over the then child? However, it is clear that it would be logical and preferable to seek the consent of the data subject again, in order to continue processing his or her personal data[29].

2. INSTRUMENTS FOR VERIFYING THE AGE OF MINORS IN ORDER TO ENSURE A SAFE ENVIRONMENT FOR RELATIONS WITH PUBLIC BODIES: SPECIAL FEATURES OF ELECTRONIC SIGNATURES AS A TRUST SERVICE PAR EXCELLENCE

An issue that cannot go unnoticed if we analyze all the circumstances surrounding the processing of personal data relating to minors, due to the special category of data subjects that they are, is the way in which the controller seeks to verify the age of the child. This is 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 their age.

In this regard, Article 8.2 GDPR, which is strongly endorsed, 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 authorized by the holder of parental authority or guardianship over the child, taking into account available technology". This indication seems to allude to the fact that in cases when these individuals are minors under 16 years of age, in the consent being given or authorized is carried out by the person exercising parental authority or guardianship over the minor, and only to the extent that this consent was given or authorized. Furthermore, the provision indicates that the effort made by the data controller must be reasonable, this being an indeterminate legal concept that may qualify depending on the details of the specific case.

29 In the same sense, NOEMÍ BRITO IZQUIERDO, "Tratamiento de los datos personales de menores de edad en la nueva normativa europea protectora de datos personales", *Actualidad Civil*, n.º 5, 2018.

In Colombia, 2010, the Spanish Data Protection Agency (hereinafter, AEPD) issued a report[30] 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, thus granting the data controller the freedom to use the procedure it deems appropriate. In this sense, some authors[31] consider that this duty of the controller translates into an obligation to do and not into an obligation of result. Meaning 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 from a child having forged their National Identity Card, or having photocopied that of the holder of parental authority or guardianship without the latter's consent[32]. However, in order to comply more adequately and satisfactorily with the principle of proactive liability imposed by the GDPR, it is certainly favorable that the procedure established by data controllers be reasonable when verifying the identity of the minor, preferably requiring their electronic signature.

Electronic signatures, currently regulated, essentially and at Community level, in Regulation (EU) n.º 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC[33] (hereinafter, eIDAS Regulation or RIE-SCTE) , as well as, at national level, in Law 6/2020, regulating certain aspects of electronic trust services[34] (hereinafter, LSCE) , which repeals Law 59/2003, of 19 December,

30 Spanish Data Protection Agency, Report 0046/2010.

31 María Milagros Cuadra Chiong, "La protección de datos personales de los menores de edad", *Anuario de justicia de menores*, n.º 13, 2013, pp. 515-516; Carmen González Madrid, "Los datos de menores en el ámbito de la educación", *Datospersonales.org*, n.º 2, 2003, pp. 1-16.

32 Vanessa García Herrera, "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*, n.º 20, 2018, pp. 62-71.

33 DOUE L 257/73 of 28 August 2014.

34 BOE, n.º 298, of 12 November 2020. The purpose of this Act is to regulate certain aspects of electronic trust services, as a complement to the eIDAS Regulation. The purpose of this Act is to regulate certain aspects of electronic 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 our 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 electronic trust services. Likewise, article 25 of Law 34/2002, of 11 July, on information society services and

on electronic signatures[35] (LFE) , is a particularly suitable instrument to be able to accredit the consent we have been referring to. Next, we analyze electronic signatures from a legal perspective (more specifically, electronic 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, particularly sensitized after the current Law 39/2015, came into force as of 1 October, on the Common Administrative Procedure of Public Administrations[36] (hereinafter, LPACAP)[37].

electronic 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 electronic delivery and the preservation of electronic 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 electronic 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 DNI, 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 electronically. 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 our 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 electronic trust services. Likewise, article 25 of Law 34/2002, of 11 July, on information society services and electronic 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 electronic delivery and the preservation of electronic 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 electronic 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 DNI, 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 authorized to sign electronically.

35 BOE, n.º 304, of 20 December 2003.

36 BOE, n.º 236 of 2 October 2015.

37 On this issue, *vid*. Juan Francisco Rodríguez Ayuso, "Servicios de confianza en

2.1. Basic Electronic Signature

Article 3(10) RIE-SCTE generally defines an electronic signature as "data in electronic form attached to or logically associated with other electronic data used by the signatory to sign" or, in other words, any method or symbol based on electronic 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 electronic trust services that serve different purposes.

This definition shows the Community legislator's intention to regulate electronic 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 electronic signatures and qualified electronic signatures). It is also a technologically undefined concept[38] (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 electronic signature may form part of the electronic document or be formally associated with it, appearing as an independent whole. However, whether electronic signatures are integrated or separate, will depend on the technical system selected and the practical applications of each type of electronic signature.

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

On this issue, the eIDAS Regulation departs from the original definition contained in its predecessor, which, by providing a simple[39] (non-general) concept of electronic signature, limited the common purpose pursued by

materia de transacciones electrónicas: el nuevo Reglamento europeo 910/2014", in Leonardo Pérez Gallardo (coord.), *Contratación electrónica y protección de los consumidores: una visión panorámica*, Madrid: Reus, 2017, pp. 133-162.

38 Apolonia Martínez Nadal, *Comentarios a la Ley 59/2003 de firma electrónica*, Madrid: Civitas, 2004, p. 74.

39 Julián Valero Torrijos and Rubén Martínez Gutiérrez, "Las bases jurídicas de la modernización tecnológica en las Administraciones públicas", in Javier Plaza Penadés

all electronic signatures to serving as a means of authentication[40]. And this in a wording that is, in principle, debatable[41] and confusing, since, as this authentication phase is subsequent to the identification phase proper, it would have been better to opt for the latter[42]. Nor is it made clear what is to be inferred as authentication and identification, which places us before an indeterminate legal concept susceptible of possibly generating radically different interpretations[43].

Be that as it may, with this altered lexis, the European standard could generate confusion that is by no means negligible. Indeed, while the previous regulation defined minimum specifications that an electronic 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,

(coord.), *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor: Aranzadi, 2013, p. 531.

40 According to this provision, an electronic signature is defined as "data in electronic form attached to or logically associated with other electronic 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 electronic 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. DIEGO CRUZ RIVERO, "Las definiciones de firma electrónica en el Real Decreto-ley 14/1999, sobre firma electrónica, y el Proyecto de Ley de firma electrónica", in Miguel Ángel Davara Rodríguez (coord.), *XVIII Encuentros sobre Informática y Derecho, 2003-2004*, Madrid: Universidad Pontificia de Comillas, 2004, pp. 127-136.

41 In contrast, DIEGO CRUZ RIVERO, *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, Madrid: Marcial Pons, 2015, p. 41, argues that, unlike identification, the use of the term authentication denotes a conscious act of signing a declaration. IGNACIO ALAMILLO DOMINGO, "Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos", in Severiano Fernández Ramos, Julián Valero Torrijos and Eduardo Gamero Casado (dirs.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público*, Valencia: Tirant lo Blanch, 2017, p. 723, concludes, in a broad interpretation of both precepts (Community and national), that, in general, the DFE and the LFE "allow the use, as an electronic signature system, of any identification/authentication mechanisms, provided that they are appropriate for the context of the operation in question, and that only those systems technically designed to be anonymous could be considered excluded from the legal definition".

42 Article 3(1) RIE-SCTE defines electronic 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 electronic form, being the data that uniquely represents a natural or legal person or a natural person representing a legal person.

43 IGNACIO ALAMILLO DOMINGO, "Identity and electronic signature. Nociones técnicas y marco jurídico general. Identification and authentication of citizens", p. 720.

makes it impossible for the legal practitioner to specify the requirements, would allow us to know when we are in the presence of an electronic 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. This would also include others that could be as simple as the inclusion of the name or other identifying element at the end of an electronic message, the digitized handwritten signature, or the existence of a question-answer and an access PIN[44]. As a result of the foregoing, it can be affirmed 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 electronic signature and redirect it, with nuances, to the traditional simple electronic signature. In this case the definition is, at least somewhat more clarifying or complete, which could be as follows: the electronic signature is the set of data in an electronic format, attached to other electronic data or logically associated with them, which can be used as a means of identification of the signatory.

2.2. Advanced Electronic Signature

Raising the quality and security requirements for electronic signatures, Article 3(11) RIE-SCTE introduces the concept of advanced electronic signature, which is understood as "an electronic 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 electronic identification of the signatory[45] (minor or holder of parental authority for, in this case, giving consent to processing operations in which the controller is the Public Administration);

44 Giovanni Buonomo and Andrea Merone, "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*, n.º 1, 2013, p. 15; Francisco Javier García Más, "El documento público electrónico (1)", in José Javier Escolano Navarro (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, 2005, p. 127; Carlos Vattier Fuenzalida, "De nuevo sobre el régimen legal de la firma electrónica: estudio del Anteproyecto de 26 de junio de 2002", *Actualidad Civil*, n.º 1, 2003, p. 140.

45 The question arises as to whether this allusion adds some distinctive nuance to the advanced electronic signature with respect to the simple electronic signature, which, as we know, also allows the signatory to be identified. In favour of this thesis, Leopoldo

(c) be created using electronic signature creation data that can be used by the signatory for the creation of an electronic signature, with a high level of confidence[46], 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 electronic documents.

3. QUALIFIED ELECTRONIC SIGNATURE

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

Rather than a new form, the qualified electronic signature constitutes a new type of advanced electronic signature which, accompanied by certain elements that make it more secure (qualified electronic signature creation

González-Echenique Castellanos de Ubao, "Estudio de la Directiva y del Real Decreto-Ley de 17 de septiembre de 1999 sobre firma electrónica", in Rafael Mateu de Ros Cerezo and Juan Manuel Cendoya Méndez de Vigo (coords.), *Derecho de Internet: la contratación electrónica y firma digital*, Cizur Menor: Thomson Reuters Aranzadi, 2000, pp. 215-216.

46 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. Also, Alberto Díaz Moreno, "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", in *Revista de la Contratación Electrónica*, n.º 2, p. 25, who understands this requirement as meaning that the signatory must be able to provide an electronic signature in order to be able to sign the contract. 25, which understands this requirement as meaning that "there must be guarantees – in terms of probability – that, in the absence of fraud or other improper conduct, two persons cannot produce the same signature".

device, on the one hand, and qualified electronic 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, a new '*nomen iuris*' is in place, with the aim of distinguishing it from that other signature which, because it has not been created by means of a qualified electronic signature creation device, or because it is not based on a qualified electronic 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 electronic signature. The latter, like the simple electronic signature and the advanced electronic signature based on a qualified electronic certificate, will not be deprived of legal effects or admissibility as evidence in legal proceedings, merely because it is in electronic form or because it does not meet the requirements of the qualified electronic signature (Article 25.1 RIE-SCTE), and it must be assessed, in any event, how effective it is, which can 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 electronic signatures to be preferential, according to the second paragraph of this provision:

> In the event that the interested parties opt to relate with the Public Administrations by electronic means, the following shall be considered valid for signature purposes:
>
> (a) Qualified and advanced electronic signature systems based on qualified electronic certificates of electronic signature issued by providers included in the Trusted List of Certification Service Providers.

4. REFERENCES TO THESE PARTICULARLY VULNERABLE SUBJECTS IN CURRENT EUROPEAN UNION 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, towards the end, an exception to the consent given by the person exercising parental authority or guardianship over the child can be found. 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, when applied directly to minors.

For its part, connected in an immanent way to the principle of transparency of Article 5.1.a) GDPR[47], 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 in reference to the right of erasure, contemplates the case of consent given by the child, which is subsequently sought to be self-withdrawn by the minor. 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, they had already reached the age of 18.

A final analysis of the recitals of the Community legislation on data protection, leads us to analyze 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 processes. 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, plus the processing of genetic and 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 in particular to personal data relating to children, which leads us to affirm that the personal data of minors shall not be considered as a special category of personal data, regardless of the fact that this type of processing is subject to certain specifications 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

47 In this regard, *vid*. ANTONIO TRONCOSO REIGADA, "Transparencia administrativa y protección de datos personales", in Antonio Troncoso Reigada (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, 2008, pp. 23-188.

–in this case, Public Administrations–, the adoption of appropriate technical and organizational 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, letter f), located in its first paragraph, which 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[48]. In short, the controller may legitimize 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 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, in all the different countries that make up the European

48 On legitimate interest as a legal basis for processing, *vid*. Javier Fernández Samaniego and Paula Fernández Longoria, "El interés legítimo como principio para legitimar el tratamiento de datos", in Artemi Rallo Lombarte (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, 2019, pp. 169-196.

Union, the supervisory authorities, the Committee and the Commission will have to promote unilaterally.

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[49].

For its part, In the Colombian domestic legal system, Article 84 LOPDGDD can be found, 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, would require the intervention of the Public Prosecutor's Office, requesting 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 be applied[50].

For its part, Article 92 LOPDGDD adds that:

> Educational centers 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. This being put in place in order to guarantee their security

49 For a complete study of data protection supervisory authorities, see JUAN FRANCISCO RODRÍGUEZ AYUSO, *Control externo de los obligados por el tratamiento de datos personales*, Barcelona: Bosch, 2020.

50 BOE, n.º 15 of 17 January 1996.

and combat the discrimination and violence exercised against them by means of modern technologies.

In short, as has been previously observed, there are numerous allusions to and references being made that in order to protect the rights and freedoms of the data subject who are a minors, are effectively established in the new regulations on the protection of personal data, granting and guaranteeing better conservation of rights 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 organizations, 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, electronic signatures.
c. It is prohibited to encourage 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.

CONCLUSIONS

Throughout this paper 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 has been dissected. To this end, 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 at Community level, by the GDPR, and subsequently and at national level and the LOPDGDD has been established and the child must be under fourteen years of age.

Similarly, once the applicable legal basis has been verified as a matter of priority, it is necessary to analyze 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 electronic signature as a basic trust service, is undergoing a new configuration under the protection of the European RIE-SCTE, recently brought into force in Spain, through the LSEC, is 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 electronic signature that, due to the greater legal-technical security it offers, should be used in relations with the Public Administrations. This is due to the fact that these public administration entities have decidedly opted for this security mechanism, the only one which, for legal purposes, has the same validity as the traditional handwritten signature.

To conclude this study it cannot be stated how important the rights of minors are in relation to current privacy regulations. As a result of the reinforcement and clarity sought position of these particular data subjects as the owners of their own personal data. Numerous sources and references have been analyzed, all of them fundamental, which has subsequently meant fulfilment of additional or reinforced obligations and responsibilities on the part of data controllers and processors to ensure the correct treatment of this sensitive data relating to minors.

BIBLIOGRAPHY

Alamillo Domingo, Ignacio. "Identity and electronic signature. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos". In Severiano Fernández Ramos, Julián Valero Torrijos and Eduardo Gamero Casado (dirs.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público*. Valencia: Tirant lo Blanch, 2017.

Alemán Monterreal, Ana. "La protección de datos de menores en el ámbito sanitario: ¿discriminación necesaria?". *Actualidad Civil,* n.º 19, 2011

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

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

Brito Izquierdo, Noemí. "Tratamiento de los datos personales de menores de edad: supuestos, límites, retos y desafíos". *La Ley Derecho de Familia,* n.º 14, 2017.

Brito Izquierdo, Noemí. "Tratamiento de los datos personales de menores de edad en la nueva normativa europea protectora de datos personales". *Actualidad Civil,* n.º 5, 2018.

Buonomo, Giovanni, and Andrea Merone. "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*, n.º 1, 2013.

Cruz Rivero, Diego. "Las definiciones de firma electrónica en el Real Decreto-ley 14/1999, sobre firma electrónica, y el Proyecto de Ley de firma electrónica". In Miguel Ángel Davara Rodríguez (coord.), *XVIII Encuentros sobre Informática y Derecho, 2003-2004*. Madrid: Universidad Pontificia de Comillas, 2004.

Cruz Rivero, Diego. *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, 2015.

Cuadra Chiong, María Milagros. "La protección de datos personales de los menores de edad". *Anuario de Justicia de Menores*, n.º 13, 2013.

De las Heras Vives, Luis, and José Ramón de Verda y Beamonte. "Consentimiento de los menores de edad". In Mónica Arenas Ramiro and Alfonso Ortega Giménez (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, 2019.

Díaz Moreno, Alberto. "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*, n.º 2, 2000.

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

Durán Ruiz, Francisco Javier. "El tratamiento de los datos personales de los menores de edad en la nueva normativa de protección de datos". In Abigail Quesada Páez, Gisela Moreno Cordero, María del Carmen García Garnica and Nuria Marchal Escalona (dirs.), *Aproximación interdisciplinar a los retos actuales de protección de la infancia dentro y fuera de la familia*. Cizur Menor: Thomson Reuters Aranzadi, 2019.

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

Fernández Samaniego, Javier, and Paula Fernández Longoria. "El interés legítimo como principio para legitimar el tratamiento de datos". In Artemi Rallo Lombarte (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, 2019.

García Herrera, Vanessa. "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*, n.º 20, 2018.

García Más, Francisco Javier. "El documento público electrónico (1)". In José Javier Escolano Navarro (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, 2005.

Gómez-Juárez Sidera, Isidro. "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". *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n.º 11, 2006.

González-Echenique Castellanos de Ubao, Leopoldo. "Estudio de la Directiva y del Real Decreto-Ley de 17 de septiembre de 1999 sobre firma electrónica". In Rafael Mateu de Ros Cerezo and Juan Manuel Cendoya Méndez de Vigo (coords.), *Derecho de Internet: La contratación electrónica y firma digital*. Cizur Menor: Thomson Reuters Aranzadi, 2000.

González Madrid, Carmen. "Los datos de menores en el ámbito de la educación". *Datospersonales.org*, n.º 2, 2003.

Guillén Catalán, Raquel. "Los retos de la sociedad ante la protección de datos de los menores". *Revista Boliviana de Derecho*, n.º 20, 2015.

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

Hidalgo Cerezo, Alberto. "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*, n.º 15, 2017.

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

Palma Ortigosa, Adrián. "Ámbito de aplicación y definiciones del GDPR". In Juan Pablo Murga Fernández, María de los Ángeles Fernández Scagliusi y Manuel Espejo Lerdo de Tejada (dirs.), *Protección de datos, responsabilidad activa técnicas de garantía*. Madrid: Reus, 2018.

Piñar Real, Alicia. "Tratamiento de datos de menores de edad". In José Luis Piñar Mañas (dir), *Reglamento general de protección de datos: Hacia un nuevo modelo europeo de privacidad*. Madrid: Reus, 2016.

Plaza Penadés, Javier. "La Ley de servicios de la sociedad de la información y comercio electrónico". In Javier Plaza Penadés, Eduardo Vázquez de Castro, Raquel Guillén Catalán and Fernando Carbajo Cascón (coords.), *Derecho y*

nuevas tecnologías de la información y la comunicación. Cizur Menor: Thomson Reuters Aranzadi, 2013.

Rodríguez Ayuso, Juan Francisco. "Servicios de confianza en materia de transacciones electrónicas: el nuevo Reglamento europeo 910/2014". In Leonardo Pérez Gallardo (coord.), *Contratación electrónica y protección de los consumidores: Una visión panorámica*. Madrid: Reus, 2017.

Rodríguez Ayuso, Juan Francisco. Ámbito contractual de la firma electrónica. Barcelona: Bosch, 2018.

Rodríguez Ayuso, Juan Francisco. *Figuras y responsabilidades en el tratamiento de datos personales*. Barcelona: Bosch, 2019.

Rodríguez Ayuso, Juan Francisco. *Control externo de los obligados por el tratamiento de datos personales*. Barcelona: Bosch, 2020.

Troncoso Reigada, Antonio. "Transparencia administrativa y protección de datos personales". In Antonio Troncoso Reigada (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, 2008.

Valero Torrijos, Julián, and Rubén Martínez Gutiérrez. "Las bases jurídicas de la modernización tecnológica en las Administraciones públicas". In Javier Plaza Penadés (coord.), *Derecho y nuevas tecnologías de la información y la comunicación*. Cizur Menor: Aranzadi, 2013.

Vattier Fuenzalida, Carlos. "De nuevo sobre el régimen legal de la firma electrónica: estudio del Anteproyecto de 26 de junio de 2002". *Actualidad Civil*, n.º 1, 2003.