

PROTECTION OF CHILDREN'S PERSONAL DATA. A CRITICAL OVERVIEW FOLLOWING THE ENTRY INTO FORCE OF THE EUROPEAN UNION REGULATION ON PERSONAL DATA PROTECTION

Marta Ortega Gómez*

Abstract

This article examines the rules introduced by Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation, GDPR) for the purpose of protecting children's personal data. The Preamble of the GDPR refers to children as vulnerable beings requiring specific protection in the field of personal data protection, and states that the GDPR is mainly aimed at providing a strong system of data protection based on fundamental rights for all individuals. Moreover, the GDPR's provisions deal with consent to the processing of children's personal data (Art. 8) and to the requirement of special clarity that is imposed on data processors and controllers when they interact with children (Art. 12). However, the fact that just two of these provisions (out of a total of ninety-nine) refer to children is evidence that the regime provided under Regulation (EU) 2016/679 is essentially 'age blind'. The study of these references and provisions is aimed at assessing whether the protection provided by the GDPR for the benefit of children can actually be considered a "strong protection for children", as the same Preamble proclaims. Considering the aforementioned, this article intends to highlight possible weaknesses of the GDPR in the area of study.


Keywords: General Data Protection Regulation; children's personal data; Charter of Fundamental Rights of the European Union; children's consent to data processing.

PROTECCIÓ DE DADES PERSONALS DELS NENS. UNA VISIÓ CRÍTICA DESPRÉS DE L'ENTRADA EN VIGOR DEL REGLAMENT DE LA UNIÓ EUROPEA SOBRE PROTECCIÓ DE DADES PERSONALS

Resum

Aquest article examina la normativa introduïda pel Reglament (UE) 2016/679 en relació amb la protecció de persones físiques pel que fa al processament de dades personals (Reglament general de protecció de dades, GDPR) i se centra en la protecció de les dades personals dels nens. El preàmbul de l'RGPD es refereix als nens com a persones vulnerables que necessiten protecció específica en l'àmbit del processament de dades personals. Afirmar, també, que l'objectiu principal de l'RGPD és proporcionar a tothom un marc sòlid de protecció de dades basat en els drets fonamentals. A més, l'RGPD regula les condicions aplicables al consentiment per al processament de les dades personals dels nens (art. 8) i també explicita que els responsables del processament d'aquestes dades han de ser clars, en particular, amb la informació adreçada als nens (art. 12). Tanmateix, el fet que només 2 de les 99 disposicions es refereixin als nens demostra que el Reglament (UE) 2016/679 pràcticament no té en compte l'edat en les seves disposicions. L'estudi d'aquestes referències i disposicions es proposa valorar si l'RGPD es pot considerar realment un "marc sòlid per a la protecció de les dades" dels nens, tal com s'afirma en el seu preàmbul. Tenint això en compte, aquest article es proposa fer paleses les possibles deficiències de l'RGPD en el camp de l'estudi.

Paraules clau: Reglament general de protecció de dades; dades personals dels nens; Carta de Drets Fonamentals de la Unió Europea; consentiment per al processament de dades dels nens.

* Marta Ortega Gómez, associate professor of Public International Law-European Community Law and director of the postgraduate course on European Data Protection Law at the University of Barcelona. Faculty of Law, Av. Diagonal, 684, 08028 Barcelona. martaortega@ub.edu.  0000-0003-4254-3989.

Article received 20.11.2021. Blind review: 15.12.2021 and 22.12.2021. Final version accepted: 28.02.2022.

Recommended citation: Ortega Gómez, Marta. (2022). Protection of children's personal data. A critical overview following the entry into force of the European Union Regulation on Personal Data Protection. *Revista Catalana de Dret Públic*, 64, 158-173. <https://doi.org/10.2436/rcdp.i64.2022.3754>

Contents

1 Introduction

2 The Preamble of the GDPR affirms that children are data subjects that require specific legal protection, but the Regulation is blind to age

3 The rights of children to the protection of their personal data: the fundamental rights approach

3.1 The human rights approach in the GDPR. General considerations

3.2 The rights of children and the right to the protection of personal data in the Charter of Fundamental Rights of the European Union

4 The issue of child empowerment in the field of data protection

5 Children's consent to data processing under Article 8 of the GDPR

5.1 Definition of children for the purpose of the GDPR and the issue of age

5.2 The scope of application of Article 8 of the GDPR: children's consent in relation to ISS

5.3 Age verification

6 Article 12 of the GDPR and the requirement of the data controller to provide clear, transparent, intelligible information and communication to the data subject

6.1 Scope of the obligation of transparency

6.2 The obligation of the controller to facilitate the exercise of data subject rights

7 Final considerations

References

“As Baby Bear exclaims to a concerned Mother Bear and Father Bear,
‘And someone has stolen my identity’”

Edith Ramirez

[CARU Annual Conference 2012](#)

1 Introduction

European Union Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data¹ (the General Data Protection Regulation, or GDPR), in force since 25 May 2018, introduced a general regime on personal data protection which applies to all natural persons (Valpuesta Gastaminza & Hernández Peña, 2021).²

One of the most remarkable novelties introduced by the GDPR was the inclusion of express references to children. Two of these references appear in recitals 38 and 58 of the Preamble, and another two are provisions of articles 8 and 12. The present study examines these references and articles. Recitals 38 and 58 of the Preamble remark on the fact that children need specific legal protection with respect to data protection, while Article 8 refers to the issue of children's consent to the release of their data to data controllers and processors. Meanwhile, Article 12 deals with the obligation of the data processor to inform the data subject, with transparency and clarity, about the exercise of their individual rights, conferred by articles 15 to 22: right to object, right to erasure (right to be forgotten), right to restrict processing, and the right to object to automated decision-making and personal profiling.

Through thorough examination, this paper intends to show the way in which the GDPR takes into consideration the processing of children's personal data. In advance of this analysis, it must be remarked that the GDPR basically introduces age-blind rules (Art. 8 and 12 are the sole exceptions). Strictly speaking, this means that adults and children deserve virtually the same consideration by data controllers and processors. However, small children cannot perceive the risks associated with the release of their personal data for data processing

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, pp. 1–88. Regulation 2016/679/EU constitutes a rather comprehensive legal instrument in the field of personal data protection. It is more ambitious, complete and rigorous than Directive 95/46/EC on the protection of individuals with regard to the processing of personal data, which it replaced (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, OJ L 281, 23.11.1995, pp. 31–50). For a retrospective analysis of Directive 95/46/EC: Hustinx (2017); Kasneci (2010); Robinson et al. (2009).

This paper is not concerned with other normative acts of the EU that make reference to data protection in specific areas. Hence, the following acts are outside the scope of this study: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ EU L 119, 4.5.2016, pp. 89–131; 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), OJ L 201, 31.7.2002, pp. 37–47. Directive 2002/58 was amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ L 337 de 18.12.2009, pp. 11–36. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, pp. 132–149; Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by EU institutions, bodies, offices and agencies and on the free movement of such data, repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, pp. 39–98.

2 For a general approach to the system of data protection in the EU, see also Troncoso Reigada (2021); Rallo Lombarte and García Mahamut (2015); Council of Europe, European Court of Human Rights, European Data Protection Supervisor and European Union Agency for Fundamental Rights (2019); Conde Ortiz (2008); Delgado (2008); López Álvarez (2016); Piñar Mañas (2016).

purposes.³ They do not have the skills or the knowledge to perceive themselves as data subjects who are the holders of the fundamental right to the protection of their personal data.⁴

2 The Preamble of the GDPR affirms that children are data subjects that require specific legal protection, but the Regulation is blind to age

The Preamble of the GDPR (in recitals 38 and 58) affirms that children are persons whose data require specific protection, “as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data”.⁵ According to this statement, and following on from remarks made in the previous section, children should be considered vulnerable subjects (Mangas Martín, 2008, p. 444)⁶ by data controllers and data processors.

Article 8 of the GDPR defines 13 years as the age below which children are especially vulnerable subjects with regard to data processing operations. Thus, children below the age of 13 must be considered vulnerable children who require specific legal protection in all situations involving the right to the protection of personal data. Article 8 of the GDPR, on the issue of the child's consent,⁷ supports this interpretation by stating that any minor of 14 and above must be represented by a parent or guardian when consent to data processing is given or authorised.

After recognising that children need specific protection, Recital 38 of the Preamble continues:

Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. (GDPR, Recital 38)

Despite the clarity and rotundity of the wording of Recital 38, the provisions of the GDPR actually pay little attention to it. In effect, the only issue expressly regulated, in Article 8 of the GDPR, is the issue of children's consent in relation to the collection of their personal data when using services directly offered to them. The other two issues – children's personal data for marketing and personal profiling⁸ – are completely absent from the provisions of the GDPR, despite their objective importance.

³ Children are accustomed to nonchalantly releasing their personal data to information society services (ISS), defined as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services”: Article 1.1b of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, pp. 1–15). In practice, children usually access ISS and give their permission to the processing of their data without any sort of parental supervision or control. This is quite commonplace in our times; even very young children lie about their real age and opt to proportion personal data to data processors and controllers for processing within the framework of an ISS relationship or scheme.

It is also a fact that children have easy access to most websites. When this occurs, it is common for them to bring personal data (which may evidence their personal profile, including personal choices and commercial preferences, interests, psychological profile, social stat, etc.) to the websites, ignoring privacy alerts. All this usually happens without the supervision of their parents.

At the same time, parents are rarely aware of the precise contents of their children's digital activity in either of the two contexts referred to above. There is also evidence that personal data controllers and processors are not in the habit of making serious checks on the age of users, as will be presented in detail later (in section 5 of this work).

⁴ The Committee of Ministers of the Council of Europe has repeatedly insisted on the opportunities and risks for children in the digital environment. This appears in the [Council of Europe Strategy for the Rights of the Child \(2016–2021\)](#), last accessed on 8 October 2021. The strategy identifies the rights of children in the digital environment as one of its priority areas. In 2021, the Council of Ministers remarked on the risks in terms of privacy for children, highlighting the privacy risks for children who suffer COVID-19 and the data exposure of children whilst confined: [Declaration by the Committee of Ministers on the need to protect children's privacy in the digital environment](#), adopted by the Committee of Ministers on 28 April 2021 at the 1402nd meeting of the Ministers' Deputies, last accessed on 21 October 2021.

⁵ Recital 38. Recital 58 affirms that such specific protection implies that all communications addressed to children shall be expressed in plain, clear language.

⁶ The following studies also refer to the issue under examination: Lievens and Verdoodt (2018); Livingstone et al. (2016); Lenhart and Madden (2007).

⁷ Section 7 below deals with this issue.

⁸ Data processing shall be fair, according to Article 8 of the CFREU. The authors of this work maintain that they are contrary to aggressive practices with regard to profiling and that the negative effects of profiling should be neutralised as they become unfair consumer practices: Laux et al. (2021). Remarkably, data controllers and processors of children's data may have an undue and

The obligations imposed by the GDPR on data processors and controllers give rise to a comprehensive system of individual rights and guarantees. The rights of the data subject have already been cited (in section 1). With regard to legal and institutional guarantees, it must be highlighted that data processors and controllers are subject to the supervision of data protection officers and to authorities of control; they must comply with registry and auditory rules; on specific occasions, they are bound to obtain a data impact assessment within the terms of the Regulation; international data transfers are subject to principles regarding the “adequacy of the level of protection afforded”,⁹ and infringements may be the object of sanctions.¹⁰

However, the whole construction fails to make a legal differentiation between children and adults that could be considered adequate to procure effective protection for children in the field of study, as this article intends to put in evidence.

3 The rights of children to the protection of their personal data: the fundamental rights approach

The consideration of the right to data protection as a fundamental right for all natural persons (González Fuster & Gellert, 2012) lies at the heart of the GDPR regime. In effect, the whole system of provisions of the GDPR is conceived and orientated towards providing a high level of protection for personal data in accordance with the Lisbon Treaty and the Charter of Fundamental Rights of the European Union (CFREU).¹¹ Yet this system of legal protection has not incorporated children as it should have done.

3.1 The human rights approach in the GDPR. General considerations

The Preamble of the GDPR starts by affirming that the individual right to data protection is a fundamental right according to Article 8 of the CFREU. The first indents of the Preamble provide further specification in this regard. Recital 2 of the Preamble affirms that the right to data protection protects all natural persons, regardless of nationality or residence. And Recital 4 of the Preamble recognises that the right to data protection is not an absolute right and therefore must be interpreted in conjunction with other fundamental rights.

Remarkably, the jurisprudence of the Court of Justice of the European Union (CJEU) provides strong support to the fundamental rights approach of the GDPR. Essentially, the Court has procured a high level of protection in the field of data protection through its rulings, which have decisively contributed to the determination of the scope, limits and substance of the fundamental right to data protection. This appears to be evident in relevant judgments such as the *Bodil Lindqvist* ruling (2003),¹² the *Costeja v Google Spain* ruling (2014), as well as the ruling in the *Facebook Ireland and others* case (2021).¹³

abusive influence on the behaviour of children who are targeted by direct or indirect (subliminal) publicity messages from services providers. Federation of European Direct Marketing (FEDMA) (2003); Ghose and Yang (2009); Brkan, Maja (2019).

9 GDPR: articles 30 (records of processing activities), 35 (data protection impact assessment), 37–39 (data protection officer), and 44 (general principle for transfers). Article 25 of Directive 95/46/EC already dealt with international data transfer and the adequacy criteria, which means that data transfers will require the same level of data protection in the jurisdiction of a third country where the processing is going to take place. The CJEU has been strict on this point. It invalidates the so-called *privacy shield* between the US and the EU in the Schrems case (CJEU Judgement of 16 July 2020, in Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, ECLI:EU:C:2020:59). In 2015, the CJEU had stated in the *Schrems I* case (CJEU Judgment of 6 October 2015, *Maximilian Schrems*, C-362/14 ECLI:EU:C:2015:650) that the supervisory authority of a Member State has the competence to verify the effectiveness of the adequacy criteria applicable to international data transfers. See the discussion of the *Schrems I* case by Uría Gavilán (2016). On 25 March 2022, the US and the EU announce a new agreement on data transfer from the EU to the US with the intention to comply with the requirements of the CJEU, a new Data Transfer Privacy Framework.

10 Article 82 of the GDPR regulates the right to be compensated by the processor or controller if the data subject suffers harm due to the infraction of the rules of the GDPR.

11 In order to illustrate this idea, reference must be made to Article 9 of the GDPR, which introduces a specific category of very sensitive data that make reference to race, religion, political opinion, etc., and are intrinsically connected with essential fundamental rights. Article 32 of the GDPR on data security can also be cited as an example. This provision recognises that data processing implies “the risk of varying likelihood and severity for the rights and freedoms of natural persons”. Both provisions provide reinforced protection of the fundamental rights and values that the GDPR aims to protect.

12 CJEU Judgment of 6 November 2003, *Bodil Lindqvist*, C-101/01, ECLI:EU:C:2003:596.

13 According to the CJEU (*Facebook Ireland and others* case), national data protection authorities have the right to sue; articles 7, 8

Moreover, when the CJEU has been asked to interpret Article 8 of the CFREU in conjunction with other fundamental rights recognised by the CFREU (rights which could have the effect of limiting the right to data protection, such as the right to information and the right to freedom of expression), the right to data protection has prevailed (Docksey, 2016) in all the cases which have been examined. For instance, in Case 136/17, ruled in 2019, the CJEU affirmed that the data subject's fundamental rights guaranteed by articles 7, respect for private and family life (Martín y Pérez de Nanclares, 2008, pp. 213–215)¹⁴, and 8, right to the protection of personal data (Martín y Pérez de Nanclares, 2008, p. 223–243), of the CFREU override the rights of potentially interested internet users protected by Article 11 of the Charter (freedom of expression and information).¹⁵

In this context, it must also be highlighted that, at the time of writing, there are no CJEU rulings dealing specifically with the issue of the fundamental right of children to data protection.

3.2 The rights of children and the right to the protection of personal data in the Charter of Fundamental Rights of the European Union

One of many positive contributions made by the CFREU is the recognition of the fundamental right of individuals to personal data protection. Article 8 of the CFREU recognises the right to protection of their personal data in the following terms: “Everyone has the right to the protection of personal data concerning him or her.” This provision requires the data holder's consent to data collection, processing and fair use¹⁶ for specified uses by the controller and processor. The right to data protection is guaranteed by both the method of requiring consent and by the obligation of the collector or the processor to make fair use of the data in the context of data processing.

Additionally, Article 8 recognises the right of everyone to have access to collected data concerning him or her, and the right to have these data rectified or erased. This provision applies to the activity of both private and public sectors.

As can be observed, Article 8 of the CFREU applies indistinctly to adults and children. Despite the lack of nuance, where children's rights to privacy are at stake, Article 8 should be read and interpreted in connection with Article 24 (CFREU), which refers to the “rights of the child”. Article 24.1 states that “children shall have the right to such protection and care as is necessary for their well-being”, going on to affirm that “children may express their views freely [...] on matters which concern them in accordance with their age and maturity.” Article 24.2 continues: “In all actions relating to children, [...] the child's best interests must be a primary consideration.”

and 47 of the CFREU are involved in the ruling, CJEU Judgement of 15 June 2021, *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, C-645/19, ECLI:EU:C:2021:483. In the *Digital Rights Ltd v Ireland* case, the CJEU considers that Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, amending Directive 2002/58/EC, is invalid as it does not sufficiently comply with security requirements and contradicts articles 7 and 8 of the CFREU: CJEU Judgement of 8 April 2014, *Digital Rights Ireland and others*, C293/12 and C594/12, ECLI:EU:C:2014:238.

Another example of protective jurisprudence is CJEU Judgement of 1 October 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH*, Case C-673/17, ECLI:EU:C:2019:801.

The construction of a privacy shield is another expression of the will of the CJEU to guarantee a high level of protection of the right to data protection: CJEU Judgement of 30 May 2006, *Parliament v Commission and Council*, C-317/04 and C-318/04, ECLI:EU:C:2006:346.

However, the CJEU refused to qualify the right to data protection as a fundamental right in the Judgement of 16 December 2008, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, Case C-73/07, ECLI:EU:C:2008:72.

¹⁴ The right to data protection and the right to privacy are closely linked but not identical; while their core content overlaps in some aspects, they also differ, as Kokott and Sobotta (2013, pp. 222–228) point out. In effect, the right to privacy refers to the privacy of the individual, which may be questioned in the relation between the holder of the right and the possible invader of the right; whereas the right to the protection of personal data encompasses a concrete area of the right to privacy, that which refers to the individual's personal data (Hijmans, 2016, p. 6). See also Warren and Brandeis (1890, pp. 193–220); González Fuster (2014).

¹⁵ CJEU Judgement of 24 September 2019, *GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17, ECLI:EU:C:2019:773.

¹⁶ The expression of “fair use” implies considerations of ethics, legitimacy, legality, and even public morality.

Reading the two provisions conjointly leads one to understand, in the first place, that both private institutions and public authorities must guarantee data protection with regard to children. And second, that the minimum standard of protection for children shall comprise the following aspects:

- a) Children's data shall be fairly processed for specified purposes.
- b) Use of children's data must be consented to by the children or their parents or guardians, in accordance with their age and maturity.
- c) Children's well-being with respect to the protection of their personal data shall be guaranteed.
- d) Children's right to freedom of expression shall also be guaranteed in accordance with their age and maturity. There are two other fundamental rights closely connected with the right to privacy:¹⁷ the right to dignity, and the right to education, which is highly relevant in relation to children in the digital arena (Rallo Lombarte, 2018, p. 151).¹⁸

In accordance with Article 24 of the CFREU, the best interests and well-being of children – the core contents of the rights of children – should constitute prevailing values to which other fundamental rights must be subjected.

Finally, it can be considered that a high level of safeguarding should be given to children's right to data protection. It is a right that should be respected and guaranteed by all actors associated with data processing, including data processors and controllers, search engines, information society services (ISS), the public administration, data protection agencies, data protection officers and authorities, and the judiciary. As expounded in the previous section, the CJEU seems clearly inclined to procure such a high level of legal protection with respect to the right to the protection of personal data.

4 The issue of child empowerment in the field of data protection

As is well known, Directive 95/46/EU was the first EU legislation to address personal data protection. It was adopted with one primary objective: to prevent national legislation on the protection of data privacy from hampering the free flow of personal data between the Member States of the European Community.¹⁹ Accordingly, Directive 95/46/EC was primarily and essentially framed to protect the internal market; the Directive²⁰ did not pay much attention to data protection in the dimension of individual rights. Nonetheless, the CJEU did provide early protection to the right of all natural persons to data protection on the basis of the Directive²¹ and the fundamental right to privacy.

17 In Case C-82/16, CJEU Judgment of the Court (Grand Chamber) of 8 May 2018, *K.A. and Others v Belgische Staat*. ECLI:EU:C:2018:308, the CJEU reads Article 7 in connection with Article 24 to refuse automatic denial of a residence permit on the basis of Directive 2008/115/EC.

18 The Declaration of the Committee of Ministers of the Council of Europe on "protecting the dignity, security and privacy of children on the Internet" adopted on 20 February 2008 remarks on the connection between "Dignity, security and privacy of children on the Internet". The Declaration recalls the right of children to the dignity, special protection and care necessary for their well-being.

19 In 1980, the Organisation for Economic Co-operation and Development (OECD) passed a code of guidelines concerning data privacy intended to provide a response to the "danger that disparities in national legislations could hamper the free flow of personal data across frontiers". The source of inspiration for the [OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data](#) (1980) regarding the need for privacy legislation is the same as that found in the European Union. At the European level, the Council of Europe adopted Convention No. 108 in 1981: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, in force since 1 October 1985. Last amendment of Convention 108+ took place in 2018 when the Council of Ministers adopted the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, in Denmark on 18 May 2018, CM (2018) 2 final.

20 Directive 95/46/EC leaves unregulated issues that are regulated by the GDPR. For instance, Article 24 of Directive 95/46/EC authorised the Member States to decide the amount of the sanctions to be imposed on companies in case of infringement; Regulation 2016/679/EU provides more specificity in this area by introducing fines for personal data breaches (PDB) and for administrative breaches. Both penalty types are between 2 and 5% of the previous year's annual turnover.

21 CJEU Judgment of 6 November 2003, *Bodil Lindqvist*, C-101/01, ECLI:EU:C:2003:596 was a relevant and significant start. See Brkan (2019, p. 883) on this point.

The Directive was mainly designed to establish common standards for data privacy protection among the Member States of the European Community, and to harmonise Member State legislations on data protection. The enactment of the Directive was intended to put an end to a situation in which “some Member States applied strict limitations and procedures, whereas other Member States had no rules at all” (Robinson et al., 2009) in the field of personal data protection, and this obstructed the free flow of personal data in the EU.

Directive 95/46/EC made no mention of children and, given its primary objective (stated above), this is understandable. The absence of references to children could also be due to the lack of awareness of the problems associated with children's privacy in the digital environment that existed at that time.

Also worthy of consideration is the fact that, when the Directive was passed, the EU legislator was not charged with the mission of developing an extended regime of the individual right to data protection as a fundamental right. In the nineties, the EU legislator had no express responsibility to protect the fundamental rights of children either. Directive 95/46/EC preceded the CFREU (adopted in 2000) and the Lisbon Treaty (LT) of 2007, both of which came into force on the same date, 1 December 2009.²² The CFREU had the virtue of transforming the legal scenario in the EU with regard to children's fundamental rights in the EU, children's well-being,²³ and the right of individuals to data protection. In addition, the LT introduced the individual right to data protection (Art. 16 of the Treaty on the European Union)²⁴ and required the EU institutions to legislate in this field. The CFREU also recognised the fundamental rights of children (Art. 24), the fundamental right to data protection (Art. 8), and the right to the protection of private life (Art. 7). Hence, it seems understandable that Directive 95/46/EC remained silent on children's data protection; at the time when the Directive was adopted, the treaties did not mention the issue either.²⁵ In addition, children's exposure to the digital environment at that time is not comparable with the current level of exposure, as there were no social media networks and the internet had only existed for four years.

Despite all this, while the EU remained conspicuous by its absence in this field, the United States adopted a federal law, the Children's Online Privacy Protection Act (COPPA), enacted in 1998²⁶ and amended in 2013.²⁷ This legislation is dedicated exclusively to children's personal data protection. In fact, it deals with one single issue regarding children's data protection: children's consent to release their personal data to data controllers and processors. COPPA requires parental consent on behalf of children under 13 years of age. Infringement of COPPA has resulted in heavy sanctions against the perpetrators. However, some commentators have described it as inadequate, as it appears that its application does not prevent the infringement of basic data protection rules.²⁸ The reported fragility of the COPPA regime is due to the fact that operators are not obliged to ask the

22 The Treaty of Lisbon (LT), amending the Treaty of the European Union (TEU) and the Treaty establishing the European Community, signed in Lisbon, 13 December 2007, OJ C 306, 17.12.2007, pp. 1–271.

23 The LT also sets “children's well-being” as an objective of the EU according to Article 3.3 of the TEU.

24 [Article 286](#) of the EC Treaty, adopted in 1997 as part of the Treaty of Amsterdam, provided that “Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty.”

25 However, the CJEU has provided a high level of protection when asked to interpret Directive 95/46/EC. Constant jurisprudence: CJEU Judgment of 6 October 2015, *Maximilian Schrems*, C-362/14 ECLI:EU:C:2015:650. In the ruling on the *Google Spain* case, the CJEU had to consider the link provided by the search engine Google and the right to be forgotten as a component of the right to privacy. The Court affirmed that “processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet – information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty”. CJEU Judgment of 13 May 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C131/12, EU:C:2014:317, paragraph 80.

26 The Children's Online Privacy Protection Act of 1998, 15 USC, 6501–6505 entered into force on 21 April 2000; its amendment entered into force on 1 July 2013.

27 As regards COPPA compliance, see Federal Trade Commission (2002): [Protecting children's privacy under COPPA: a survey on compliance](#), last accessed on 15 November 2021.

28 According to the report published by the Computer Science Institute of Berkeley, 57% of Google Play applications for children would infringe COPPA. On many occasions, geolocation data are collected and behavioural advertising also takes place: 19% of apps available through Android collect identifiers or other personally identifiable information, without parental consent (Irwin et al., 2018, p. 63).

age of users the requirement regarding parental consent is only triggered if the operator happens to determine that a user is a child under the age of 13. Another weakness of COPPA stems from the age threshold, as teens between 13 and 16 are not afforded any consideration, as they are under the GDPR.

Putting aside its possible shortcomings, the US legislation was nevertheless a pioneer in today's world. COPPA was the only specific legislation on the matter in question, on a world-wide scale, for over twenty years, until the Information Commissioner's Office (ICO) of the United Kingdom adopted [Age appropriate design: a code of practice for online services](#), also known as the Children's Code.²⁹ The UK code is a complementary normative instrument to the UK Data Protection Act (2018), which implemented the GDPR into UK law. The Children's Code came into force on 2 September 2020, allowing organisations a transition period of twelve months to be in compliance with it by 2 September 2021.³⁰ The code is a comprehensive and exhaustive legal instrument of nearly one hundred pages. It introduced detailed rules on transparency, parental consent, accountability, data minimisation, sharing and profiling, among other relevant issues with regard to the processing of children's personal data.

It is obvious that the EU legislator has not aspired to follow either the legal strategy of either the UK or the US in this area (Macenaite & Kosta, 2017, p. 146).³¹ Once the LT had come into force, the EU had already acquired the competence to produce a specific legislation on the protection of children's personal data, but it has not followed the Anglo-Saxon pathway. Instead, the EU has traditionally taken a rather passive position and shown limited interest in the issue. When the GDPR was negotiated and passed, it could have been followed by an executive or delegated EU regulation on children's personal data;³² alternatively, the EU legislator could have adopted a separate regulation to deal with children's personal data protection. None of this has occurred. It could be supposed that this is because the EU legislator is working on the assumption that child autonomy and children's education could be a good substitute for a more detailed system of protection.³³ Another very possible explanation is that the EU has found it difficult to legislate for this particular issue, due to the Member States' different views on the necessity of creating a comprehensive common system of personal data protection for children.

5 Children's consent to data processing under Article 8 of the GDPR

As highlighted previously, the GDPR provides specific legal protection for children with respect to the expression of consent to data release with a data processing purpose.

5.1 Definition of children for the purpose of the GDPR and the issue of age

The United Nations Convention on the Rights of the Child (UNCRC) establishes the age of legal majority at 18 years, hence a child is anybody under the age of 18.³⁴ Despite this universal definition, the GDPR recognises that children over 16 do not need the specific protection of a parent or guardian with regards to the expression of consent to the processing of their data by a controller or processor (GDPR, Art. 8).

²⁹ Data Protection Act (2018), chapter 12.

³⁰ The Secretary of State laid the Children's Code to Parliament under section 125(1)(b) of the Data Protection Act 2018 on 11 June 2020. The ICO issued the code on 12 August 2020 and it came into force on 2 September 2020 with a twelve-month transition period.

³¹ The authors find some coincidences between the EU GDPR and the COPPA regime. Interestingly, both regulations concur on the self-information criteria implicitly imposed on children and their representatives; the authors also believe that a regulatory instrument appears to be necessary to address this issue specifically.

³² Executive and delegated regulations are introduced by articles 290 and 291 of the Treaty of the Functioning of the European Union (TFEU).

³³ In fact, the thesis of empowerment of the data holder has been expressly assumed by the European Commission in a Communication from the Commission to the European Parliament and the Council: "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation" {SWD(2020) 115 final}, Brussels, 24.6.2020 COM(2020) 264 final, p. 17.

³⁴ According to Article 1 of the United Nations Convention on the Rights of the Child, adopted on 20 November 1989, in force since 2 September 1990.

The GDPR also concedes that the Member States (MS) of the EU may consider that children over 14 years of age can have the same consideration as children over 16 years under national implementing legislation. This is because Article 8 of the GDPR does not establish whether children aged between 14 and, at least, 16 years of age (or children under 16)³⁵ shall be represented by parents or guardians, leaving the issue to be decided by the individual MS. Hence, MS are free to decide whether express parental or legal guardians' consent is required at all over the age of 14. It appears to be evident that, at the time that the GDPR was being negotiated, not all the MS had the same sensitivity regarding the necessity to provide specific protection to children aged between 14 and 16.

Furthermore, Article 8 affirms that special protection is required for all children under 14. The protection which the Regulation provides for these children consists of representation by a parent or guardian, which is required for giving consent to a data processor or controller when a child is *offered* an ISS (and by extension, in practice, *targeted*) by an information service operator.

Although the GDPR does not expressly affirm so, it follows that children aged 16 and over are considered equal to adults over 18 years old, if the law of the MS concerned admits this, which is in fact the case in all the MS of the EU.

As can be observed, the Regulation does not pretend to create a uniform system to determine the age below which representation by an adult is required. The lack of uniformity thereof leads to legal divergence between MS. And this is far from being a minor issue, as the system of protection varies widely in the different MS. Presumably, the immediate consequence of this is that the data protection system is not as strong as the same Regulation proclaims (in Recital 17 of the Preamble).³⁶ Furthermore, this divergence among the MS can be considered an important obstacle to the effective harmonisation of EU law in this field. It opens the door to different standards of protection and different obligations for data processors and controllers in the different states of the EU. Effective harmonisation regarding the issue of age appears to be necessary to provide a strong and coherent data protection legal framework within the Union.

As a result of the ambiguity of Article 8, the age threshold varies significantly in the different Member States. Parental consent for children under the age of 16 is required in Croatia, Germany, Luxembourg, Ireland, Poland, Romania, Netherlands, Hungary, Slovakia. France, Check Republic, Greece and Slovenia do not require parental consent over the age of 15. Austria, Bulgaria, Cyprus, Italy, Lithuania and Spain do not require parental consent for children over 14. And Belgium, Malta, Portugal, Sweden, Estonia, Finland, Latvia, Denmark do not require parental consent above the age of 13.³⁷

5.2 The scope of application of Article 8 of the GDPR: children's consent in relation to ISS

As indicated, Article 8.1 of the GDPR applies to ISS directly offered to a child and to the giving of consent to a data controller or processor who may be the service provider. The notion of ISS derives by way of reference from Directive 2015/1535/EU,³⁸ which covers both remunerated and non-remunerated ISS, as it refers to services "normally remunerated". In practice, the most commonly used ISS are social media networks which are not remunerated for their use, and the social media networks habitually used by minors do not incur any charge for use (e.g., Facebook, Instagram, TikTok³⁹ and Hangouts, among many other social and communication networks and games).

35 According to the wording of Article 8 of the GDPR, children who have passed their 16th birthday are considered adults in the field of data protection.

36 According to Recital 17 of the Preamble, the GDPR was conceived to provide "a strong and coherent data protection framework in the Union" for all natural persons. Obviously, in order to become strong, this strong system of protection should include children, taking into account their specific vulnerabilities.

37 Source [euConsent](#).

38 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17.9.2015, pp. 1-15.

39 Some apps are remunerated for their use: transport services apps, education services apps and some social media networks are frequently remunerated by users.

Article 8 refers to a scenario in which a service provider “offers” ISS to a child. The use of the term “offer” indicates a situation in which the child is targeted by the service provider; however, most children search for and access ISS without waiting to be offered them. In consequence, it should be considered that the term “offer” should be broadly understood (to obtain a broader protection for children) as also covering scenarios in which the child approaches the information service operator on their own initiative.⁴⁰

Then, following prior considerations, Article 8.1 of the GDPR envisages three types of legal scenarios involving data processing and minors of under 18 years of age.

In the first place, the processing of the personal data of a minor of under 18 years of age is always lawful provided that, according to national law, the child is at least 16 and gives their express consent to the processor (the same rule that applies to adults). Then, from 16 years old, all individuals shall have absolute freedom to release and control their own personal data and offer them to ISS providers for processing purposes.

Secondly, where the child is aged between 14 and at least 16 years of age, such processing is subject to parental authorisation only if the law of the Member State requires it, and to the extent that express consent is given by parents or guardians.

In the third place, Article 8 requires parental consent in all cases for children aged 13 and under.

5.3 Age verification

The GDPR is far from strict with respect to the issue of age verification by data controllers or processors. In effect, Article 8.2 of the Regulation merely requires them to “make reasonable efforts to verify” that the consent is truly in line with the law, “taking into consideration available technology.”⁴¹ At the present moment, there are no effective technological means to verify the identity and the age of internet service users. However, some websites do use age checks (Nash et al., 2014).

Accordingly, the consent expressed by a child aged 13 and under in all cases, or by a child aged between 14 and 16 (where parental consent is required) without a parent’s or guardian’s express authorisation, is not valid. Notwithstanding, the Regulation does not impose a rigorous obligation upon the data controller or processor to find out the real age of the data subject. As explained above, it is commonplace for minors of 13 to introduce a false age in order to participate in social media networks, websites and digital gaming without parental control; this is followed by the release of their personal data (preferences, geolocation, address, social status and so on). In January 2021, Italy ordered the social media network TikTok to block the accounts of any users whose age it could not determine, after a 10-year-old child died trying to imitate a challenge accessible through this social media platform (see [The Guardian](#), January 23 2021).

As can be observed, Article 8.2 is framed in such a way that, even if available technology to verify age existed, the data controller would merely have to make a *reasonable effort* to verify the age and identity of a user. Consequently, Article 8.2 is excessively lenient in addressing the issue of age falsification of users of social media networks and digital gaming. Cancellable biometrics control appears to be a possible effective solution to control the age of users (Balla, 2013, pp. 1–11). Biometrics itself implies control of the child’s physiognomy and represents another invasion of privacy. However, if used adequately, it may function as a preventive and dissuasive tool for the benefit of children.

The United Kingdom became the first country to pass a law containing a legal mandate for certain data controllers and processors to verify the age of users. According to the chapter 30 of the Digital Economy Act of 2017, websites that published pornography on a commercial basis were required to implement a “robust” age verification system to prevent minors from accessing their sites. The UK government had to abandon this

40 In the UK, section 123 of the Data Protection Act 2018 more accurately refers to “relevant information society services which are likely to be accessed by children.” The vast majority of online services are accessed by children (not offered to them) and are clearly covered by the UK DPA Information Commissioner’s Office’s Children’s Code.

41 Article 8.2 GDPR affirms that a reasonable effort must be made, taking into consideration the available technology, to verify that the consent is lawfully given. This means that the company or organisation must implement age verification measures (for example, control questions, actions on the website, etc.).

requirement in 2019, however, after it was considered that a robust system of age verification would create added privacy risks for users of pornography.⁴²

6 Article 12 of the GDPR and the requirement of the data controller to provide clear, transparent, intelligible information and communication to the data subject

Children should be well informed about their rights by the data controller, according to Article 12 of the GDPR.

Under the heading “Transparent information, communication and modalities for the exercise of the rights of the data subject”, Article 12.1 of the GDPR affirms that information and communications from the data controller to the data subject shall be “concise, transparent, intelligible, and easily accessible [...], using clear and plain language, in particular for any information addressed specifically to a child.”

6.1 Scope of the obligation of transparency

The wording of Article 12 of the GDPR is excessively broad insofar as it does not stipulate the age of the children it refers to; considering this imprecision, the differentiation between children according to age made by Article 8 of the GDPR could be useful in this context. If it is assumed that the age criteria of Article 8 applies with regard to the obligation of transparent and clear information, it does not make much sense for Article 12 to apply to children who need to be represented by a parent or guardian, as (theoretically) they are already represented by a parent or guardian and do not need special attention from the data controller or processor. Therefore, it could be concluded that Article 12 refers to *the other children* between 14 and 16 years of age, as these children are not required to be represented to express consent, according to national law. These *unrepresented* children in particular require clear information with respect to their rights and how to exercise them.

Against the extrapolation of Article 8 of the GDPR with respect to the obligation of transparency, *Article 29 Working Party – Guidelines on transparency under Regulation 2016/679* (WP29) considers that there is no room for doubt in the wording of Article 12.⁴³ WP29 affirms that Article 12 refers to children, not their representatives, using the following terms to express this idea:

Article 8 does not provide for transparency measures to be directed at the holder of parental responsibility who gives such consent. [...] WP29's position is that transparency is a free-standing right which applies as much to children as it does to adults. (WP29, 2017, p. 10).

However, the same WP29 continues by affirming the following:

WP29 recognises that with very young or pre-literate children, transparency measures may also be addressed to holders of parental responsibility given that such children will, in most cases, be unlikely to understand even the most basic written or non-written messages concerning transparency. (WP29, 2017, p. 11).

Hence, WP29 states one thing, only to go on to state practically the opposite. It first affirms that Article 8 has no connection with Article 12 of the GDPR; then goes on to recognise that parents should be the addressees of the information addressed to their children only if they are very young or pre-literate. Using the criterion of pre-literacy, WP29 appears to exclude that Article 8 may be extrapolated with respect to transparency on the basis of freedom of expression. This solution introduces a criterion (pre-literacy) which does not appear anywhere in the wording of the GDPR and, consequently, appears alien to the GDPR.

42 Finally, Part III of the Digital Economy Act 2017 was not applied. Statement by Nicky Morgan, Secretary of State for Digital, Culture, Media and Sport. Written statement made on 16 October 2019, [Statement UIN HCWS13](#), accessed on 10 September 2021.

43 Article 29 Data Protection Working Party [Guidelines on transparency under Regulation 2016/679](#). Adopted on 29 November 2017. As last Revised and Adopted on 11 April 2018, 17/EN WP260 rev. 01, p. 10.

6.2 The obligation of the controller to facilitate the exercise of data subject rights

Article 12.2 of the GDPR requires the data controller to facilitate the exercise of data subject rights, under articles 15 to 22. To be precise, this obligation of the controller applies to the following rights conferred on to the interested person: the right of access (Art. 15), the right to rectification (Art. 16), the right to erasure, including the right to be forgotten (Art. 17; Di Pizzo Chiacchio, 2018),⁴⁴ the right to restrict processing (Art. 18), the right to be notified by the processor of the rectification or erasure of data (Art. 19); the right to portability (Art. 20); the right to oppose to the data's processing, including profiling, and the regulation on individual automated decision-making (ADM, Article 22).

Further on, Article 12.3 of the GDPR requires the data controller to provide the information requested under articles 15 to 22 "without undue delay and in any event within one month of receipt of the request". That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension. The data subject has the possibility to complain before the authority if the data controller does not comply with this obligation and seek a judicial remedy (Art.12.4).

In general, and regardless of their age, individuals that do not have a specific knowledge in the area of study are unaware of the existence of these rights and, consequently, how to exercise them. In addition, the complexity of the exercise of these rights may make it impracticable for a child alone to perform. Again, children (regardless of their age) who are not represented by their parents or tutors may find themselves totally at a loss when they have given their consent to data processing and would like to rectify this.

7 Final considerations

As expounded in the previous pages, the GDPR requires the intervention of parents or guardians to express consent for data processing purposes on behalf of all minors of 14 years and under. But beyond this requirement, the rules, rights and obligations that the GDPR introduces to protect the individual before data processors and controllers, apply to children and adults in equal terms. Consequently, and contrary to the rotund wording of Recital 38 of the Preamble, children do not merit specific protection under the rules of the GDPR, with the exception of the issue of expression of consent. In this legal scenario, it appears particularly serious and concerning that the GDPR fails to exclude children's profiling, as well as the fact that the GDPR does not require parents or guardians of minors to exercise the rights conferred by articles 15 to 22 of the GDPR on behalf of children.

To conclude, it appears to be clear that the GDPR is inadequate to protect children's privacy and their right to the protection of their personal data. Essentially, the GDPR offers an age-blind legal construction. This is far from being a casual circumstance: it is the expression of the absence of intention of the European legislator to procure a coherent and rigorous system that guarantees children's fundamental right to data protection in an effective manner. Finally, the omission of the European legislator in the field of study proves that the principle of children's empowerment in the sphere of personal data protection (with all its actual and potential implications) is deliberately (and silently) being imposed by the EU legislator on the European society.

⁴⁴ See also Simón Castellano (2012).

References

- Balla, Joseph. (2013). Applying biometric data for personal identification. *Biztonságpolitika.hu*, 1–11.
- Brkan, Maja. (2019). The essence of the fundamental rights to privacy and data protection: Finding the way through the maze of the CJEU's constitutional reasoning. *German Law Journal*, 20(6), 864–883. <https://doi.org/10.1017/glj.2019.66>
- Conde Ortiz, Elena. (2008). *La protección de datos personales*. Dykinson.
- Delgado, Lucrecio. (2008). *Vida privada y protección de datos en la Unión Europea*. Dykinson.
- Council of Europe, European Court of Human Rights, European Data Protection Supervisor, & European Union Agency for Fundamental Rights. (2019). *Handbook on European data protection law: 2018 edition*. Publications Office. <https://data.europa.eu/doi/10.2811/58814>
- Danish Consumer Ombudsman. (2014). [*The Consumer Ombudsman's guidance on children, young people and marketing*](#).
- De Pauw, Pieter, De Wolf, Ralf, Hudders, Liselot, & Cauberghe, Veroline. (2018). From persuasive messages to tactics: Exploring children's knowledge and judgement of new advertising formats. *New Media & Society*, 20(7), 2604–2628. <https://doi.org/10.1177/1461444817728425>
- Di Pizzo Chiacchio, Adrián. (2018). *Expansión del derecho al olvido digital. Efectos de "Google Spain" y el big data e implicaciones del nuevo Reglamento Europeo de Protección de Datos Personales*. Atelier.
- Docksey, Christopher. (2016). Four fundamental rights: Finding the balance. *International Data Privacy Law*, 6(3), 195–209.
- Federation of European Direct Marketing (FEDMA). (2003). [*European Code of Practice for the Use of Personal Data in Direct Marketing*](#).
- Finocchiaro, Giusella, Rallo Lombarte, Artemi, García Mahamut, Rosario, Hustinx, Peter, López Aguilar, Juan Fernando, Abrams, Martin, Lattanzi, Roberto, Tene, Omer, Vladeck, David, Agustina Sanllehi, José R., Dirk Blumenberg, Axel, Álvarez Rigaudias, Cecilia, Arenas Ramiro, Mónica, Bonfiglio, Salvatore, de Hert, Paul, Stefanatou, Dimitra, Fernández Samaniego, Javier, Fernández Longoria, Paula, González Fuster, Gloria, ... Puyol, Javier. (2015). *Hacia un nuevo derecho europeo de protección de datos*. Tirant lo Blanch.
- Ghose, Anindya, & Yang, Sha. (2009). An empirical analysis of search engine advertising: Sponsored search in electronic markets. *Management Science*, 55(10), 1605–1622. <https://doi.org/10.1287/mnsc.1090.1054>
- González Fuster, Gloria, & Gellert, Raphael. (2012). The fundamental right of data protection in the European Union: In search of an uncharted right. *International Review of Law, Computers & Technology*, 26(1), 73–82.
- González Fuster, Gloria. (2014). *The emergence of personal data protection as a fundamental right in the EU*. Springer.
- Hijmans, Hielke. (2016). *The European Union as a constitutional guardian of internet privacy and data protection*. University of Amsterdam.
- Hustinx, Peter. (2017). [*EU data protection law: The review of Directive 95/46/EC and the proposed General Data Protection Regulation*](#). In Marise Cremona (Ed.), *New Technologies and EU Law*. Oxford University Press.
- Kasneji, Dede. (2010). [*Data protection law: Recent developments*](#) [Unpublished doctoral dissertation]. Università degli Studi di Trieste.

- Kokott, Julianne, & Sobotta, Cristoph. (2013). The distinction between privacy and data protection in the case law of the CJEU and the ECHR. *International Data Privacy Law*, 3(4), 222–228.
- Laux, Johann, Wachter, Sandra, & Mittelstadt, Brent. (2021). Neutralizing online behavioural advertising: algorithmic targeting with market power as an unfair commercial practice. *Common Market Law Review*, 58(3), 719–750.
- Leandro Nuñez García, José, Piñar Real, Alicia, Uriarte Landa, Iñaki, Álvarez Caro, María, Duaso Calés, Rosario, Piñar Mañas, José Luis, Troncoso Reigada, Antonio, Alonso Martínez, Carlos, Díaz-Romeral Gómez, Alberto, Irurzun Montoro, Fernando, Nieto Garrido, Eva, Torregrosa Vázquez, José, Adsuara Varela, Borja, Corral Sastre, Alejandro, Hernández Corchete, Juan Antonio, Muñoz-Machado Cañas, Julia, Tejerina Rodríguez, Ofelia, Cervera Navas, Leonardo, García Mexía, Pablo, ... Fernández Conte, Julen. (2017). *Reglamento General de Protección de Datos*. Reus Editorial.
- Lenhart, Amanda, & Madden, Mary. (2007). *Teens, privacy and online social networks*. Pew Research Center.
- Lievens, Eva. (2010). *Protecting children in the digital era: The use of alternative regulatory instruments*. Brill.
- Lievens, Eva, & Verdoodt, Valerie. (2018). Looking for needles in a haystack: Key children's rights issues in the General Data Protection Regulation. *Computer Law & Security Review*, 34(2), 269–278.
- Livingstone, Sonia, Carr, John, & Byrne, Jasmina. (2016). One in three: Internet governance and children's rights. *Innocenti Discussion Papers*, 1.
- López Álvarez, Luis Felipe. (2016). *Protección de datos personales: adaptaciones necesarias al nuevo reglamento europeo*. Ediciones Lefebvre.
- Macenaite, Milda, & Kosta, Eleni. (2017). Consent for processing children's personal data in the EU: Following in US footsteps? *Information & Communications Technology Law*, 26(2), 146–197. <https://doi.org/10.1080/13600834.2017.1321096>
- Mangas Martín, Araceli. (2008). Artículo 24. Derechos del niño. In Araceli Mangas Martín (Ed.), *Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo* (pp. 441–453). Fundación BBVA.
- Martín y Pérez de Nanclares, José. (2008). Artículo 7. Respeto de la vida privada i familiar. In Araceli Mangas Martín (Ed.), *Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo* (pp. 213–215). Fundación BBVA.
- Martín y Pérez de Nanclares, José. (2008). Artículo 8. Protección de datos de carácter personal. In Araceli Mangas Martín (Ed.), *Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo* (pp. 223–243). Fundación BBVA.
- Nash, Victoria, O'Connell, Rachel, Zevenbergen, Bendert, & Mishkin, Allison. (2014). *Effective age verification techniques: Lessons to be learnt from the online gambling industry. Final report*. Oxford Internet Institute.
- Piñar Mañas, José Luis (dir.). (2016). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de protección de datos*. Reus.
- Rallo Lombarte, Artemi. (2018). Privacy and freedom. *European Data Protection Law Review (EDPL)*, 2, 150-151.
- Rallo Lombarte, Artemi, & García Mahamut, Rosario. (2015). *Hacia un nuevo derecho europeo de protección de datos*. Tirant lo Blanch.
- Reyes, Irwin, Wijesekera, Primal, Reardon, Joel, Elazari, Amit, Razaghpanah, Abbas, Vallina-Rodriguez, Narseo, & Egelman, Serge. (2018). "Won't Somebody Think of the Children?" Examining COPPA

- Compliance at Scale. *Proceedings on Privacy Enhancing Technologies*, 3, 63–83. <https://doi.org/10.1515/popets-2018-0021>
- Robinson, Neil, Graux, Hans, Botterman, Maarten, & Valeri, Lorenzo. (2009). *Review of the European Data Protection Directive*. RAND Corporation.
- Schober, Karl. (2015, September 9). [Global privacy sweep finds privacy issues in children's apps](#). *JD Supra*.
- Simón Castellano, Pere. (2012). *El reconocimiento del derecho al olvido digital en España y en la UE: Efectos tras la sentencia del TJUE*. Editorial Bosch.
- Troncoso Reigada, Antonio (Ed.). (2021). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales*. Civitas.
- Uría Gavilán, Elisa. (2016). Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems. *Revista de Derecho Comunitario Europeo*, 53, 261-282.
- Valpuesta Gastaminza, Eduardo, & Hernández Peña, Juan Carlos (coords.). (2021). *Tratado de Derecho digital*. Wolters Kluwers.
- Warren, Samuel D., & Brandeis, Louis D. (1890). [The right to privacy](#). *Harvard Law Review*, 4(5), 193–220.