

FACULTAD
DE CIENCIAS
JURÍDICAS



ZIENTZIA
JURIDIKOEN
FAKULTATEA

TRABAJO FIN DE ESTUDIOS

**DOBLE GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS Y
EN DERECHO**

**PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL:
ESPECIAL REFERENCIA AL MENOR DE EDAD EN EL
MARCO DE LAS REDES SOCIALES**

TANIA SESMA GOÑI

DIRECTORA

MARÍA ÁNGELES EGUSQUIZA BALMASEDA

Pamplona

16 de enero de 2018

RESUMEN

La rápida evolución tecnológica y el uso creciente de Internet, especialmente de las redes sociales, han traído consigo una intromisión en la esfera más personal e íntima de las personas. Cada vez más compartimos infinidad de aspectos relativos a nuestra vida, aspectos que fácilmente quedan en manos de terceros, ocasionando que nuestro derecho a la intimidad y por ende nuestro derecho a la protección de datos pueda quedar gravemente lesionado. En el presente trabajo abordamos precisamente el estudio de éste último derecho, partiendo de su configuración constitucional y continuando con su desarrollo actual en el ámbito comunitario y en la legislación española. El nuevo Reglamento Europeo de protección de datos que se aplicará a partir de mayo de 2018, replantea los perfiles de este derecho en el ordenamiento jurídico español, lo cual obliga a revisar las soluciones dadas a la problemática que plantea la protección de datos del menor de edad en el marco de las redes sociales, que es el objeto último de este trabajo.

PALABRAS CLAVE: derecho a la intimidad, protección de datos, menor de edad, redes sociales.

ABSTRACT

Rapid technological developments and the increasing use of Internet, especially of social networks, have brought about an intrusion into the most personal and intimate sphere of people. Increasingly, we share infinity aspects of our lives, aspects that can easily remain in the hands of third parties, causing our right to privacy and therefore our right to data protection to be seriously injured. In the present work we deal precisely with the study of this last right, starting from its constitutional configuration and continuing with its current development in the Community area and in Spanish legislation. The new European Data Protection Regulation that will be applied from May 2018, rethinks the characteristics of this right in the Spanish legal system, which forces us to review the solutions given to the issue of the protection of minors' data in the framework of social networks, which is the ultimate goal of this work.

KEY WORDS: right to privacy, data protection, minor, social networks.

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
Art. (arts.)	Artículo (artículos)
CC	Código Civil
CE	Constitución Española
LO	Ley Orgánica
LOPD	Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal
LOPJM	Ley Orgánica 1/1996, de 15 de enero, de protección jurídica del menor, de modificación del Código Civil y de la Ley de Enjuiciamiento Civil.
LORTAD	Ley Orgánica 5/1992 Reguladora del Tratamiento Automatizado de los Datos de Carácter Personal
LSSICE	Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico
RDLOPD	Reglamento de Desarrollo de la LOPD
RGPD	Reglamento UE 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de esos datos
S. (SS.)	Sentencia (Sentencias)
STC	Sentencia del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TCFA	Tribunal Constitucional Federal Alemán
TEDH	Tribunal Europeo de Derechos Humanos
TS	Tribunal Supremo

ÍNDICE

I. INTRODUCCIÓN	6
II. EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA.....	8
II.1. El origen: la protección del derecho a la intimidad.	8
II.1.1. <i>The right to be let alone</i>	8
II.1.2. <i>Protección del derecho a la intimidad en España</i>	10
II.2. La construcción del derecho a la autodeterminación informativa en España a partir de los instrumentos internacionales.	12
II.3. La configuración del derecho a la autodeterminación informativa como derecho fundamental en España. SSTC 290/2000 y 292/2000.	14
II.3.1. <i>Contenido del derecho a la autodeterminación informativa</i>	17
II.3.2. <i>Ámbito de protección del derecho a la autodeterminación informativa</i>	20
II.3.3. <i>Límites al ejercicio del derecho a la autodeterminación informativa</i>	21
III.RÉGIMEN JURÍDICO DEL DERECHO A LA PROTECCIÓN DE DATOS.22	
III.1 Ámbito jurídico hasta el momento presente.	23
III.1.1 <i>Directiva 95/46/CE</i>	23
III.1.2 <i>La actual LOPD</i>	25
III.2. Futuro ámbito jurídico en la protección de datos; la incidencia en el caso de los menores de edad.....	28
III.2.1. <i>Reglamento UE 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de esos datos</i>	28
III.2.2. <i>Proyecto de la LOPD</i>	33
IV. LA PROTECCIÓN DE DATOS EN SU PROYECCIÓN AL MENOR DE EDAD Y EN EL MARCO DE LAS REDES SOCIALES.....	35
IV.1. El menor de edad como sujeto especialmente protegido.....	35
IV.2. Peculiaridades en materia de protección de datos respecto al menor de edad	36
IV.2.1 <i>Consentimiento para el tratamiento de sus datos</i>	36
IV.2.2 <i>Ejercicio de los derechos ARCO</i>	39
IV.3. Menores de edad en el uso de las redes sociales: falta de control por parte de los proveedores del servicio en el cumplimiento de los requisitos de la normativa de protección de datos.....	40
IV.3.1 <i>Aspectos generales</i>	40

IV.3.2. <i>Consecuencias de la falta de control por parte de los proveedores del servicio en el cumplimiento de la normativa de protección de datos.</i>	42
IV.4. Papel de los padres frente al menor de edad en el uso de las redes sociales.	45
IV.4.1 <i>Conflicto entre el ejercicio de la patria potestad de los padres frente al derecho a la intimidad del menor.</i>	45
IV.4.2. <i>Problemática en el tratamiento de datos de un menor de edad por parte de padres separados.</i>	48
V. CONCLUSIONES.	50
VI. BIBLIOGRAFÍA.	52
VII. JURISPRUDENCIA CONSULTADA.	54

I. INTRODUCCIÓN

Vivimos en un mundo donde las tecnologías de la información y la comunicación forman parte de nuestra sociedad, pudiendo incluso llegar a decir que son ella misma. Nos encontramos en la era de la “Sociedad de la Información”, donde la exposición de nuestra vida íntima es cada vez más intensa y más cotidiana, y donde nuestros aspectos más íntimos de la personalidad quedan fácilmente en manos de terceros, convirtiéndonos en sujetos perfectamente identificados o cuanto menos identificables.

La Sociedad de la Información, el impacto de las Tecnologías y las Comunicaciones, así como la necesidad de proteger el derecho a la Intimidad frente a las amenazas actuales de la informática, han dado origen al reconocimiento del derecho a la protección de datos y la progresiva creación de lo que se ha denominado “cultura de protección de datos”, que consiste en una creciente sensibilización hacia el valor que tienen nuestros datos personales; sensibilización que ha ido de la mano de un mayor conocimiento de los derechos y medios de protección que el ordenamiento jurídico nos ofrece en este sentido.

Ante esta necesidad constatada de proteger nuestros datos personales, y por consiguiente nuestra intimidad, es de destacar el objetivo de la previsión contenida en el art. 18.4 CE., en virtud del cual: “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”. No se trata de acabar con el uso de la informática, sino de compatibilizar ese uso, en ocasiones abusivo, con el respeto a los derechos fundamentales de las personas susceptibles de ser lesionados.

El interés del tema objeto de este trabajo nace de la propia realidad a la que nos enfrentamos, una realidad marcada por la “Revolución Tecnológica” que, si bien ha traído consigo importantes ventajas, también ha supuesto una mayor intromisión en la intimidad, hasta el punto de que el afectado llega incluso a perder el control sobre sus propios datos personales, sin ser consciente de los riesgos que ello implica.

El principal propósito de nuestro trabajo será, por un lado, plantear los aspectos centrales del Reglamento UE 2016/679 de protección de datos que comenzará a aplicarse a partir del 28 de mayo de 2018, y el proyecto de nueva LOPD, con objeto de visualizar los cambios a los que se enfrenta la normativa actual. Y, por otro lado,

abordar el estudio del menor de edad como titular del derecho a la protección de datos dentro del marco de las redes sociales, como sujeto especialmente vulnerable. Una atención especial dedicaremos al conflicto que suscita la protección de la intimidad y otros derechos del menor frente al ejercicio de la patria potestad por parte de los padres, y al problema relativo al consentimiento del menor de edad para el tratamiento de sus datos. Para ello, analizaremos el art. 13 del RDLOPD, en el cual se reconoce capacidad suficiente a los mayores de catorce años para otorgar por sí mismos el consentimiento para el tratamiento de sus datos personales, pero no así a los menores de dicha edad, los cuales necesitarán la representación legal de sus padres o tutores.

En definitiva, a lo largo del trabajo iremos profundizando paulatinamente en el estudio del derecho a la protección de datos personales, para ahondar finalmente en la protección del menor de edad, y en el marco de las redes sociales. Para ello se hace necesario realizar el recorrido seguido en nuestro país desde la protección de la intimidad frente al uso de la informática, hasta la protección de datos personales en su construcción y configuración final como un derecho fundamental de “tercera generación”, autónomo y diferenciado respecto del derecho a la intimidad.

II. EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA.

II.1. El origen: la protección del derecho a la intimidad.

El derecho a la autodeterminación informativa se construye a partir de la noción de intimidad¹ y se encamina, fundamentalmente, a dotar a las personas de cobertura jurídica frente al peligro que supone la informatización de sus datos personales. En el mundo actual en el que vivimos, en que las tecnologías de la información y la comunicación se están haciendo con el control, éste derecho cobra gran relevancia.

Conviene, por consiguiente, estudiar en qué consiste el derecho a la intimidad, antes de aproximarnos al derecho a la autodeterminación informativa.

II.1.1. *The right to be let alone.*

Los orígenes de la intimidad se remontan a finales del siglo XIX, concretamente a Estados Unidos, gracias al trabajo de dos visionarios del mundo del derecho, Samuel Warren y Louis Brandeis, los cuales empiezan a concebir la idea de que toda persona tiene que tener una esfera privada, fuera del conocimiento público.

Éstos decidieron escribir un artículo titulado «The Right to Privacy», y lo publicaron en la Harvard Law Review el 15 diciembre de 1890. En él se definía el “derecho a ser dejados en paz”, un nuevo derecho descrito en los siguientes términos:

“Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society [...] Now the right to life has come to mean the right to enjoy life, - the right to be let alone”². Gracias a su trabajo, WARREN y BRANDEIS³ sientan las bases de un verdadero derecho a la intimidad, un derecho autónomo, con un contenido intangible y

¹ Hablamos de derecho a la autodeterminación informativa como podríamos hablar de derecho a la protección de datos, pero esa primera denominación obedece a que así fue acuñado en su origen por la Jurisprudencia. LUCAS MURILLO DE LA CUEVA, P. *El derecho a la autodeterminación informativa*. Tecnos, Madrid, 1990, pág 25.

² “Los cambios políticos, sociales y económicos entrañan el reconocimiento de nuevos derechos y el derecho común, en su eterna juventud, se amplía para satisfacer nuevas demandas de la sociedad (...), ahora, el derecho a la vida ha evolucionado hasta significar el derecho a disfrutar de la vida, el derecho a ser dejado en paz”.

³ En 1916, Brandeis es Juez del TS, y entronca este derecho a la intimidad con la IV enmienda de la Constitución.

completamente necesario para el normal desarrollo de la vida de toda persona, que protege su círculo más íntimo y personal.

Podemos decir que son los padres de ese derecho a la intimidad, caracterizado por el rechazo de toda intromisión no consentida en la vida privada⁴, pero tuvieron un predecesor en el que se inspiraron, el juez COOLEY⁵. Éste ya se planteó con anterioridad a ellos que cada uno es libre para poder tener una vida privada que el resto de la sociedad no tiene por qué conocer, incluso aunque se trate de personas con cierta notoriedad pública.

En definitiva, el resultado de su trabajo y esfuerzo supuso un gran avance y un paso importante para la sociedad, pues hasta el momento, cuando se hablaba del concepto de intimidad, se relacionaba con el derecho a la propiedad. No se concebía la idea de que pudiera existir un derecho sin un contenido tangible que proteger.

De esta manera, el derecho a la intimidad sufrirá una importante evolución, desligándose de una concepción exclusivamente iusprivatista, propia del liberalismo, para comenzar a considerarse como un atributo de la personalidad del individuo, quedando enmarcado en lo que se denomina “derechos o bienes de la personalidad”⁶. Así, el fundamento del derecho a la intimidad no estaría en el derecho de propiedad, sino en la inviolabilidad y dignidad del ser humano.

En el ámbito del derecho continental europeo, este derecho a la intimidad, como derecho inherente a la persona, se introdujo en diversas constituciones, configurando una estructura sólida de lo que hoy podemos llamar “intimidad”. La Constitución portuguesa de 1976 fue la primera que se hizo eco de él en su art. 26.1, siguiéndole la española de 1978, que insertó este derecho en su art. 18. Fuera de estos dos casos y, al margen de diversas Constituciones americanas, las cuales configuraron este derecho a través de la jurisprudencia, solamente quedaban las grandes declaraciones internacionales de derechos⁷ que reconocían este derecho a la intimidad.

⁴ LUCAS MURILLO DE LA CUEVA, P. *El derecho a la autodeterminación informativa*. Ob.cit., pág.60.

⁵ El juez Cooley escribió el artículo The Law of Torts en 1879, donde defendía el derecho de las personas a ser dejadas en paz.

⁶ VELÁZQUEZ BAUTISTA R, *Protección jurídica de datos personalizados automatizados*. Colex, 1993, pág 40.

⁷ Art 12 Declaración Universal de 1948, establece que “nadie será objeto de injerencias en su vida privada, su familia, su domicilio o correspondencia...” Art. 17.1 Pacto Internacional de Derechos Civiles y Políticos de 1966, establece el mismo contenido que el citado per aludiendo también a la vida privada

II.1.2. *Protección del derecho a la intimidad en España.*

El derecho a la intimidad en nuestro país encuentra su acomodo en el art. 18 CE. En concreto, su apartado primero reconoce el derecho a la intimidad personal y familiar como derecho fundamental y lo garantiza a través de la limitación del uso de la informática. Además, el art. 20.4 erige a la intimidad en límite de los derechos en él reconocidos, como son la libertad de expresión e información y por último, el art. 105.b), al demandar de la ley la regulación del acceso de los ciudadanos a los archivos y registros administrativos, excluye del público el conocimiento de “lo que afecte a la intimidad de las personas”.

Por lo demás, la inviolabilidad del domicilio y el secreto de las comunicaciones, consideradas tradicionales formas de proteger la vida privada, integran los otros dos apartados del art. 18.

Se deduce pues, tal y como afirma LUCAS MURILLO⁸, que el derecho a la intimidad contiene una faceta negativa que rechaza la publicidad; y, por otra parte, en cuanto derecho de libertad, implica una presunción erga omnes, jurídicamente tutelada, de su titular a desenvolverse sin limitación alguna dentro de su ámbito privado. En este sentido, debemos hacer mención a las dos manifestaciones del derecho a la intimidad⁹ que aparecen reflejadas en el art. 18.1 CE. Por un lado, la intimidad personal; y, por otro, la intimidad familiar, que van a albergar el ámbito privado de toda persona.

En cuanto a la intimidad personal, la podemos definir como aquella que está referida de forma concreta al individuo, a un espacio psíquico y físico relativo a la persona individualmente considerada. Refleja la necesidad de que la persona disponga de un espacio íntimo en el que no quepan injerencias como presupuesto indispensable de una vida digna. En palabras del TC: “El derecho a la intimidad personal consagrado en el art. 18.1 aparece configurado como un derecho fundamental, estrictamente vinculado a la propia personalidad y que deriva, sin duda, de la dignidad de la persona humana que el art. 10.1 CE reconoce. Entrañando la intimidad personal constitucionalmente garantizada la existencia de un ámbito propio y reservado frente a

en el art. 14.1. Y Art. 8.1 Convención Europea para la protección de los Derechos Humanos y de las Libertades Fundamentales señala que “toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”.

⁸ LUCAS MURILLO DE LA CUEVA, P. *El derecho a la autodeterminación informativa*. Ob. cit., pág 90.

⁹ REBOLLO DELGADO, L. *Derechos fundamentales y protección de datos*. Dykinson, Madrid, 2004, págs. 41 y 42.

la acción y el conocimiento de los demás, necesario-según las pautas de nuestra cultura- para mantener una calidad mínima de vida humana” (STC 231/1988, de 2 de diciembre, FJ 4º y STC 57/1994 de 28 de febrero, FJ 5º).

Respecto a la intimidad familiar, se dice que es una singularidad del derecho a la intimidad personal. Tiene su fundamento en que protege, además de la vida propia y personal, un conjunto de circunstancias relativas a la vida de otras personas con las que se guarda una vinculación, como es la familiar. De nuevo, citando al TC, podemos señalar lo siguiente: “El derecho a la intimidad personal y familiar se extiende no sólo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar, aspectos que, por la relación o vínculo existente en ellas, inciden en la propia esfera de la personalidad del individuo que los derechos del art. 18.1 protegen”.

En este contexto, siguiendo con el contenido que alberga la intimidad, conviene preguntarnos si el derecho a la intimidad protege nuestra información personal frente a todos los peligros que entraña el desarrollo de la informática, y por ende el uso irrestrictivo y desordenado de las tecnologías de la información y comunicación, o por el contrario es preciso crear otro soporte jurídico para conseguir dicho objetivo.

Cuando se aprobó la LO 1/1982 , de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, se pensó que era suficiente aplicar las medidas y procedimientos en ella previstos para hacer frente a las intromisiones ilegítimas en la intimidad personal y familiar que pudiera producir la informática¹⁰. No obstante, con el paso del tiempo, y como acertadamente señala LUCAS MURILLO¹¹, se puso de manifiesto su insuficiencia. Éste señala que “La LO 1/1982, únicamente protege lo que podríamos llamar el ámbito más estricto de la intimidad, pero no es útil para impedir la captación, el acopio, la relación y transmisión de informaciones personales que no necesariamente pertenecieran a ese reducto último de la vida privada”. Asimismo, tampoco es útil para ofrecer medios al afectado que le permitan conocer qué datos relativos a su persona utilizan terceros, para rectificar aquellos que

¹⁰ Su exposición de motivos decía lo siguiente:” En tanto no se promulgue la normativa prevista en el art. 18 apartado 4 de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente Ley”.

¹¹ LUCAS MURILLO DE LA CUEVA, P. *Informática y protección de datos personales*. Centro de Estudios Constitucionales. Madrid, 1993, pág. 17.

puedan ser inexactos, o cancelar los que carezcan de relevancia o incluso puedan ser falsos.

En definitiva, era necesario el reconocimiento de un nuevo derecho que ofreciera una respuesta jurídica frente al fenómeno de la Sociedad de la Información, para frenar toda amenaza que el desarrollo tecnológico pudiera representar para los derechos y libertades de las personas.

II.2. La construcción del derecho a la autodeterminación informativa en España a partir de los instrumentos internacionales.

El derecho a la autodeterminación informativa surge como un derecho nuevo. No está previsto expresamente en nuestro ordenamiento jurídico, basta con su lectura para apreciarlo a simple vista, pero ha sido extraído por el TC concretamente del art. 18.4 CE “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos, y el pleno ejercicio de sus derechos “, que encontraba su desarrollo en la LORTAD de 1992.

A la hora de identificarlo, el TC se sirvió de los instrumentos con los que el art.10.2¹² de la Constitución quiere que se interpreten las normas sobre derechos fundamentales y libertades que contiene. En particular, el TC utilizó especialmente el Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, sobre la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, en el cual se define el marco de protección de la privacidad en relación con las tecnologías de la información y la comunicación. Dicho convenio surgió con objeto de desarrollar la protección de los derechos fundamentales de las personas en relación con el uso de la informática, y fijar las bases para una legislación internacional que permitiera compatibilizar el flujo internacional de datos con la privacidad del individuo¹³.

Asimismo, junto al Convenio del Consejo de Europa n.º108, que tendrá su plasmación en la Directiva 95/46 que posteriormente estudiaremos, se sumaron una

¹² De acuerdo con el art. 10.2 CE, las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

¹³ALVAREZ HERNANDO, J. Y CAZURRO BARAHONA, V. *Practicum Protección de datos*. Aranzadi, 2015, pág. 36.

serie de elementos que ayudaron en la construcción de este derecho¹⁴. En este sentido, hay que hacer referencia al reconocimiento por la Unión Europea en el año 2000 con la Carta de los Derechos Fundamentales de la autonomía del derecho a la protección de datos de carácter personal¹⁵ y la jurisprudencia del TEDH que, a partir del derecho a la vida privada reconocido por el art. 8 de la Convención, dotó de autonomía a la protección de datos de carácter personal.

Finalmente, debemos destacar la inspiración en nuestro país de la jurisprudencia constitucional alemana, concretamente la sentencia del TCFA sobre la Ley del Censo de Población de 15 de diciembre de 1983, la cual constituye un hito fundamental en la afirmación del derecho a la autodeterminación informativa, como respuesta a la posibilidad del tratamiento masivo de datos. En dicha sentencia, el TC configura, a partir del derecho general de la personalidad que garantiza el art. 2.1 de la Ley Fundamental de Bonn, la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la vida privada.

El TCFA afirma en la sentencia que el derecho general de la personalidad comporta la atribución al individuo de la capacidad de decidir, en el ejercicio de su autodeterminación, qué extremos desea revelar de su propia vida y señala lo siguiente:

“La autodeterminación del individuo presupone –también en las condiciones de las técnicas modernas de tratamiento de la información– que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso, a omitir, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada...”

Esta libertad de decisión, de control, supone además que el individuo tenga la posibilidad de acceder a sus datos personales, que pueda, no sólo tener conocimiento de que otros procesan informaciones relativas a su persona, sino también someter el uso de éstas a un control, ya que, de lo contrario, se limitará su libertad de decidir por autodeterminación”.

¹⁴ LUCAS MURILLO DE LA CUEVA, P. “Perspectivas del derecho a la autodeterminación informativa”, *Revista de Internet, Derecho y Política*, núm 5, 2007, pág 21.

¹⁵ Art. 7 CDFUE “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones”. Art 8 CDFUE “Toda persona tiene el derecho a la protección de los datos de carácter personal que la conciernan”.

En definitiva, el TCFA extrae del derecho al libre desarrollo de la personalidad la facultad de cada individuo de disponer sobre la revelación y el uso de sus datos, entendiendo el derecho a la autodeterminación informativa como la facultad general de disponer de los datos propios, frente a su uso informatizado.

II.3. La configuración del derecho a la autodeterminación informativa como derecho fundamental en España. SSTC 290/2000 y 292/2000.

En nuestro país el derecho a la autodeterminación informativa se aceptará también como un derecho de configuración autónoma, cuya causa mediata es la informatización de la sociedad, y el rápido avance y desarrollo de las tecnologías de la información y comunicación. Se dice que integra una de las últimas generaciones de derechos, la que se conoce como “derechos de tercera generación”, que surgen para tratar de dar respuesta a los retos y dificultades de la sociedad de nuestros días, esto es, el progreso tecnológico; principalmente, el derivado de los avances que resultan de la combinación de las virtualidades de la informática y de las telecomunicaciones, que pueden suponer un peligro para la dignidad y los derechos de la persona.

La configuración de este derecho será fruto de un largo proceso evolutivo, donde la doctrina, la legislación (nacional y europea) y la jurisprudencia jugarán un papel central. Pero será esta última, la que tras más de 20 años desde la entrada en vigor de la CE en diciembre de 1978 consolide definitivamente este derecho, a través de dos célebres sentencias: STC 290/2000 y STC 292/2000, ambas de 30 de noviembre.

Para llegar a esa configuración última y definitiva del derecho a la protección de datos, como derecho autónomo y fundamental, diferente del derecho a la intimidad, la jurisprudencia española recorrió un largo proceso. En este sentido, resulta crucial hacer mención a la STC 254/1993 de 20 de julio, como primera sentencia en que el TC se pronunció acerca de este derecho y que vino a concretar, aunque con cierta confusión, lo que en la doctrina y la jurisprudencia comparada se conocía como “derecho a la autodeterminación informativa”.

Lo interesante de la sentencia se encuentra en su fundamento jurídico sexto, que viene a decir lo siguiente: “De este modo nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no

muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática»¹⁶.

Se puede apreciar cómo el TC es consciente de que tras el art. 18.4 de la Constitución subyace algo que no es exactamente igual al derecho a la intimidad, viniendo a consagrar un derecho fundamental diferente del derecho a la intimidad, pero manteniendo una cierta ambigüedad, declaración que no es del todo contundente, y que ya caracterizaba la exposición de motivos de la LORTAD.

Serán las SSTC 290/2000 y 292/2000 de 30 de noviembre, las que darán un paso más, y vendrán a configurar sobre la base de la LORTAD el derecho a la protección de datos tal y como hoy lo conocemos, como un derecho fundamental, autónomo y con entidad propia respecto al derecho a la intimidad. Todo tipo de dudas o ambigüedades planteadas en la Sentencia 254/1993 quedaron despejadas a través de ellas, especialmente gracias a la STC 292/2000, pues en ella se vino a concretar detalladamente tanto el contenido como la función de este nuevo derecho.

En primer lugar, se establece rotundamente que lo que ya el TC había considerado anteriormente como “un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos” constituye, también, “un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática”¹⁷.

En segundo lugar, el TC procede a manifestar que ambos derechos difieren en cuanto a su función, y por ende en cuanto a su objeto y contenido. Mientras que el derecho fundamental a la intimidad del art. 18.1 tiene como finalidad proteger frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar que la persona desee excluir del conocimiento ajeno y de las intromisiones de terceros en

¹⁶ STC 254/1993, de 20 de julio, fundamento jurídico 6º.

¹⁷ STC 292/2000, de 30 de noviembre, fundamento jurídico 5º.

contra de su voluntad, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.¹⁸

En definitiva, con estas sentencias se da el paso definitivo al reconocimiento de un verdadero derecho fundamental a la protección de datos, autónomo e independiente del derecho a la intimidad, etiquetado como un “derecho fundamental de creación jurisprudencial”. Tal y como explica DÍAZ REVORIO¹⁹: “Lo que hoy denominamos derecho fundamental a la protección de datos personales, libertad informática o autodeterminación informativa, es en el sistema español un derecho fundamental de creación jurisprudencial, pues el art. 18.4 de la Constitución, que le sirve de sustento principal, establece en puridad un mandato al legislador (“La ley limitará el uso de la informática...”) y no un derecho fundamental en sentido propio. El TC, siguiendo la estela del TCFA [que en 1983 había establecido la existencia de un derecho de autodeterminación informativa, derivado del derecho general a la personalidad del art. 2 de la Ley Fundamental (...)]”.

No obstante, no ha sido una cuestión pacífica la necesidad y oportunidad jurídica del reconocimiento de un nuevo derecho fundamental a la protección de datos personales. La forma concreta en que el TC ha llevado a cabo el reconocimiento y protección de este nuevo derecho fundamental fue objeto de críticas doctrinales. Diversos autores han rechazado la consideración del derecho a la autodeterminación informativa como derecho fundamental, y han apostado por una reformulación del derecho a la intimidad como garantía individual ante el avance informático. Entre ellos podemos destacar a REBOLLO DELGADO²⁰ y RUIZ MIGUEL²¹, según el cual “el derecho a la autodeterminación informativa no sería un nuevo derecho, sino que se trataría del mismo derecho a la intimidad auxiliado de nuevas técnicas y aplicado a un objeto nuevo, la informática”

¹⁸ STC 292/2000, de 30 de noviembre, fundamento jurídico 5º.

¹⁹ DÍAZ REVORIO, F.J. “Principios de la protección de datos: derecho de la información en la recogida de datos. Una perspectiva constitucional”, en TRONCOSO REIGADA, A. *Comentario a la ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, Civitas, 2010, págs. 433 y ss.

²⁰ REBOLLO DELGADO, L. Ob. cit., pág. 135. Más ampliamente, sobre este debate, HERRÁN ORTIZ, M.I. *El derecho a la intimidad en la nueva Ley Orgánica de protección de datos personales*, Dykinson, Madrid, 2002, pág.77-87.

²¹ RUIZ MIGUEL, C. “En torno a la protección de los datos personales automatizados”, *Revista de Estudios Políticos (Nueva Época)*, núm. 84, abril – junio, 1994, págs 241 y 242.

Por el contrario, autores como PÉREZ LUÑO²² y LUCAS MURILLO²³ llevaron a cabo pronunciamientos doctrinales apostando por el reconocimiento de este nuevo derecho. De hecho, la construcción doctrinal más relevante en España fue formulada por ellos. Para el profesor LUCAS MURILLO, la autodeterminación informativa pretende satisfacer la necesidad que tenemos actualmente de proteger y preservar nuestra identidad, controlando la revelación y el manejo de los datos que nos conciernen, así como de protegernos frente a la capacidad ilimitada de archivarlos, relacionarlos y transmitirlos, propia de la informática, y de los peligros que esto puede suponer²⁴.

Asimismo, en una obra posterior, LUCAS MURILLO definió la autodeterminación informativa como el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, preservando de este modo nuestra propia identidad, dignidad y libertad. Su formulación como derecho, “implica necesariamente poderes que permitan a su titular definir los aspectos de su vida que no sean públicos, que desea que no se conozcan, así como facultades que le aseguren que los datos que de su persona manejan terceros informáticamente son exactos, completos y actuales, y que se han obtenido de modo leal y lícito”²⁵.

II.3.1. *Contenido del derecho a la autodeterminación informativa.*

Una clara respuesta al contenido del derecho a la autodeterminación informativa la encontramos en el fundamento jurídico séptimo de la Sentencia 292/2000, la cual señala lo siguiente: “El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o

²² PÉREZ LUÑO plantea la necesidad, en la era informática, de la existencia de un habeas data que se erija, del mismo modo que en su día hizo el habeas corpus, en cauce procesal que salvaguarde la libertad de la personas en la esfera de la informática. El autor identifica este concepto con el de «libertad informática» que define como «un nuevo derecho de autotutela de la propia identidad informática: o sea, el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en un programa electrónico». PÉREZ LUÑO, A.E. *Manual de informática y derecho*. Ariel, Barcelona, 1996, pág. 43.

²³ LUCAS MURILLO DE LA CUEVA, P. *El derecho a la autodeterminación informativa*. Ob. cit.

²⁴ LUCAS MURILLO DE LA CUEVA, P. *El derecho a la autodeterminación informativa*. Ob. cit., págs. 173-174.

²⁵ LUCAS MURILLO DE LA CUEVA, P. *El derecho a la autodeterminación informativa*. Ob. cit., págs. 173 y 174.

uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.”

En este sentido, LUCAS MURILLO DE LA CUEVA²⁶ señala lo siguiente: “Este derecho sirve para poner en manos de cada uno de nosotros los instrumentos para definir qué aspectos de nuestra vida deseamos -o no nos importa en determinadas ocasiones- que manejen otros. Es decir, para controlar el acceso a nuestros datos personales, a las informaciones de cualquier tipo que nos identifiquen directa o indirectamente, y su uso por terceros, ya sean estos sujetos públicos o privados”.

Queda claro que el principio de consentimiento es uno de los principios esenciales que configuran el derecho a la protección de datos personales. Es decir, la necesidad de obtener el consentimiento del interesado para efectuar la recogida y posterior tratamiento de sus datos de carácter personal constituye la regla general en materia de protección de datos. Ello quedaba expresamente consagrado en el art. 6 de la LORTAD, según el cual: “El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa”.

A este respecto, resulta interesante conocer que en materia de protección de datos se entiende por consentimiento la manifestación de voluntad del interesado por la cual consiente el tratamiento de datos que le conciernen de forma libre, inequívoca, específica e informada, sin la intervención de vicio alguno, en los términos regulados por el art. 1265 del CC (es decir, ausencia de violencia, intimidación, error y dolo)²⁷.

Por otra parte, la STC 292/2000 también hace alusión a una serie de derechos o facultades que forman parte del contenido esencial del derecho a la protección de datos

²⁶ LUCAS MURILLO DE LA CUEVA, P. Texto de la conferencia que tuvo lugar el 24 de octubre de 2005 en la sede de la Agencia Catalana de Protección de Datos [En línea]. Disponible en: www.apd.cat [2011, 10 de enero].

²⁷ ALVAREZ HERNANDO, J. Y CAZURRO BARAHONA, V. *Practicum Protección de datos*. Ob.cit., pág. 55.

y que permiten hacer efectivo ese poder de control y disposición sobre los datos personales con que cuenta el titular de los mismos. Hablamos de los denominados derechos ARCO, esto es, derechos de acceso, rectificación, cancelación u oposición. Se trata de derechos personalísimos, de forma que únicamente cabe su ejercicio por parte del interesado, o su representante legal, en los casos de incapacidad o minoría de edad. Estos derechos, salvo el derecho de oposición, estaban contenidos expresamente dentro de los derechos de titularidad de las personas que recogía la LORTAD, en su título III

En cuanto al derecho de acceso, podemos decir que es la facultad que tiene el interesado de solicitar y obtener gratuitamente información de sus datos de carácter personal, en concreto, sobre si estos están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos. En palabras de LUCAS MURILLO, es el derecho que concede al interesado “la posibilidad de comprobar si se dispone de información sobre uno mismo y conocer el origen del que procede la existente y la finalidad con que se conserva. Del mismo modo el derecho de acceso conlleva la facultad de exigir y obtener una comunicación escrita en la que consten los anteriores extremos”²⁸. La definición de LUCAS MURILLO recoge con acierto todos los aspectos incluidos en el derecho de acceso; esto es, engloba una facultad de conocimiento de la información que se almacena en un fichero, su origen y su finalidad, y, al mismo tiempo, su comunicación.

La consecuencia de acceder a los datos y tener conocimiento de su estado puede condicionar el paso siguiente. Puede ser que el estado de los datos sea correcto, en cuyo caso y, hecho efectivo el derecho de acceso, el interesado habrá ejercitado su derecho a la protección de datos, conociendo y controlando sus informaciones personales y el uso que de las mismas se hace. Pero puede suceder, por el contrario, que el conocimiento de los datos tras el acceso revele alguna inexactitud o carencia. Aquí es donde entrarán en juego los derechos de rectificación y cancelación, en virtud de los cuales el titular de los datos quedará facultado para modificar aquellos que resulten inexactos o incompletos, o bien suprimir los que sean inadecuados o excesivos.

Por último, el titular de los datos cuenta con el derecho de oposición, el cual ha

²⁸ REBOLLO DELGADO, L. Y SERRANO PÉREZ, MM. *Introducción a la protección de datos*. Dykinson, Madrid, 2006, pág. 194.

sido definido como el derecho del interesado a negarse, por motivos legítimos, a que sus datos personales sean objeto de tratamiento en los siguientes casos²⁹:

- Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.
- Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos.

En definitiva, el derecho fundamental a la protección de datos se sustenta sobre dos pilares fundamentales³⁰, que constituyen su contenido esencial: por un lado, el consentimiento de la persona y por otro lado, el conjunto de derechos que lo hacen practicable y que garantizan el control de los datos en todo momento. El primero de ellos se manifiesta como autodeterminación del individuo, y conforma el espacio de libertad y dignidad de la persona, junto con el resto de derechos fundamentales. El segundo de ellos, los denominados derechos ARCO, determinan las facultades que posibilitan el ejercicio del derecho fundamental y garantizan su protección.

II.3.2. *Ámbito de protección del derecho a la autodeterminación informativa.*

El objeto de protección del derecho fundamental a la autodeterminación informativa lo podemos extraer del fundamento jurídico sexto de la Sentencia 292/2000, en virtud del cual el objeto de protección de este derecho no se reduce sólo a los datos íntimos de la persona, “sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales”.

Por consiguiente, podemos decir, tal y como queda expresamente señalado en la Sentencia, que su objeto de protección no es sólo la intimidad individual, pues para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. En la propia LORTAD, ya se hablaba de datos de carácter personal y no de datos íntimos. Concretamente, su art. 2, señalaba que la presente ley sería de aplicación a “los datos de carácter personal que figurasen en ficheros automatizados de los sectores público y

²⁹ REBOLLO DELGADO, L. Y SERRANO PEREZ, M.M. *Manual de protección de datos*, Dykinson, Madrid, 2017, págs. 207-210.

³⁰ SERRANO PÉREZ, M.M. “El derecho fundamental a la Protección de Datos. Su contenido esencial”, *Revista Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, 2005, pág. 255.

privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado”

Esto significa que la protección del derecho a la protección de datos personales se extenderá incluso a los datos públicos que, aun siendo accesibles al conocimiento de cualquiera, “no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos”.

En definitiva, el elemento u objeto merecedor de la protección jurídica es el “dato de carácter personal”, entendiéndose por ello no sólo los datos relativos a la vida privada o íntima de la persona, sino todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Basta, por tanto, que el dato permita identificar a una persona para que estemos hablando de dato de carácter personal y entre en juego la protección que ofrece el ordenamiento jurídico.

Por otro lado, es importante conocer frente a qué tipo de operaciones quedan protegidos nuestros datos personales, diferenciando a este respecto entre tratamiento de datos y cesión de los mismos.³¹ En el primer caso diremos que se produce cuando hay una recogida, grabación, captación, conservación, almacenamiento, elaboración, modificación, bloqueo o cancelación de datos, sin existir una revelación o comunicación de datos a otra persona distinta del interesado, mientras que en el segundo caso, esa comunicación o revelación si se da.

II.3.3. *Límites al ejercicio del derecho a la autodeterminación informativa.*

En lo que respecta a los límites del ejercicio del derecho a la autodeterminación informativa, también la STC 292/2000 se pronuncia, al igual que lo hace con el contenido y objeto de protección.

Lo hace señalando lo siguiente: “En cuanto a los límites de este derecho fundamental no estará de más recordar que la Constitución menciona en el art. 105.b) que la ley regulará el acceso a los archivos y registros administrativos "salvo en lo que

³¹ ENÉRIZ OLAECHEA, FJ. Y BELTRÁN AGUIRRE, JL. *La protección de los datos de carácter personal*. Pamplona, 2012, pág. 38.

afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas" (en relación con el art. 8.1 y 18.1 y 4 CE.), y en numerosas ocasiones este Tribunal ha dicho que la persecución y castigo del delito constituye, asimismo, un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana.”. Los datos relativos a estas materias mencionadas serán objeto de un desarrollo normativo específico y tendrán un régimen singular. En este sentido, encontramos por ejemplo el Real Decreto 1110/2015, de 11 de diciembre, por el que se regula el Registro Central de Delincuentes Sexuales, cuyo objeto no es otro que objeto crear y regular la organización y funcionamiento del Registro Central de Delincuentes Sexuales, así como el régimen de inscripción, consulta, certificación y cancelación de los datos contenidos en aquél. (art.1). Asimismo, se pretende facilitar la investigación e identificación de los autores de los delitos contra la libertad e indemnidad sexuales, así como de trata de seres humanos con fines de explotación sexual.

De esta forma, los límites al ejercicio del derecho a la protección de datos habrán de encontrarse en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos. Dichos límites serán los indispensables para mantener una convivencia en una sociedad democrática, deberán cumplir los requisitos de proporcionalidad y finalidad, y deberán venir regulados por la ley.

III. RÉGIMEN JURÍDICO DEL DERECHO A LA PROTECCIÓN DE DATOS.

La concreción normativa en España de este derecho plasmada en la LORTAD, será modificada por la LOPD, que supuso la trasposición a nuestro ordenamiento jurídico de la Directiva 95/46/CE, Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta directiva pronto será desplazada por el Reglamento Europeo de protección de datos, que entró en vigor el 25 de mayo de 2016 y comenzará a aplicarse en España el 25 mayo de 2018.

III.1 Ámbito jurídico hasta el momento presente.

III.1.1 Directiva 95/46/CE.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, inspirada en el Convenio 108 del Consejo de Europa, ha constituido el texto europeo de referencia en materia de protección de datos. Fue aprobada el 24 de octubre de 1995 y entró en vigor el 13 de diciembre de 1995.

La razón de ser dictada fue la necesidad de unificar el régimen relativo al tratamiento de datos en Europa. Tal y como queda establecido en su Considerando 8, el nivel de protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos debe ser equivalente en todos los Estados miembros, y ello no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia. Era necesario que la Comunidad interviniera para aproximar las legislaciones, y en consecuencia, se dictó esta Directiva 95/46/CE.

Se trata de una disposición de carácter vinculante, en virtud de la cual se establecen los principios en materia de protección de datos que han de regir en el ordenamiento interno de cada uno de los Estados Miembros, y que nace con el objetivo de garantizar “la protección de las libertades y los derechos fundamentales de las personas físicas, en particular, el derecho a la intimidad, en lo relacionado con el tratamiento de datos personales” (Art.1 Directiva 95/46/CE)

La Directiva fijó aquellos principios que han venido haciendo referencia especialmente a la calidad de los datos, y a la legitimación en su tratamiento. Sus arts. 6 y 7 los consagraron. Respecto a los primeros, se establece lo siguiente:

- Los datos han de ser tratados de manera leal y lícita.
- Los fines a que obedece la recogida de datos habrán de ser determinados, explícitos y legítimos.
- Los datos han de ser adecuados, pertinentes y no excesivos en relación a los fines para los cuales son recabados. También habrán de ser exactos, y en su caso cuando sea necesario actualizados, con posibilidad de cancelar o rectificar aquellos que resulten inexactos o incompletos.

- Los datos han de ser conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten posteriormente.

En cuanto a los principios relacionados con la legitimación del tratamiento de datos, el art.7 de la Directiva ha venido estableciendo lo siguiente:

- El interesado ha de prestar su consentimiento de forma inequívoca.
- Únicamente cabe el tratamiento de datos si es necesario para la ejecución de un contrato en que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado.
- También puede efectuarse el tratamiento de datos si es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
- Si es necesario, para proteger el interés vital del interesado, o
- Para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos.
- Por último, es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del art. 1 de la presente Directiva.

La aplicación de esta Directiva ha conseguido alcanzar dos objetivos fundamentales. Por un lado, garantizar un alto nivel de protección de los datos de carácter personal, y por otro, eliminar cuantos obstáculos pudiesen plantearle a la libre circulación de esos datos³². No obstante, parece ser que no ha resultado del todo suficiente, ya que en mayo de 2018 será de aplicación el Reglamento Europeo de Protección de datos, que supondrá su desplazamiento.

Finalmente, en el ámbito de la Unión Europea es preciso destacar que el derecho fundamental a la protección de datos personales se encuentra expresamente reconocido

³² ALVAREZ HERNANDO, J. Y CAZURRO BARAHONA, V. *Practicum protección de datos*. Ob. cit., pág. 37.

en el art. octavo de la Carta de Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000. En él se viene a decir de forma resumida que toda persona tendrá derecho a la protección de los datos personales que le conciernen, y que los mismos serán tratados de modo leal, para fines concretos, y sobre la base del consentimiento de la persona afectada.

III.1.2 *La actual LOPD.*

El marco jurídico vigente sobre el derecho a la protección de datos en España queda recogido en la LOPD, que vino a sustituir a la LORTAD a fin de trasponer a nuestro derecho la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En consecuencia, la LOPD sigue los principios establecidos por la Directiva 95/46/CE, relativos a la legitimación y calidad de los datos.

Esta LOPD ha sido desarrollada reglamentariamente por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el RDLOPD, que desarrolla con más detalle el régimen de la LOPD en el sistema.

En primer lugar, resulta interesante conocer qué protege exactamente la LOPD, a quién protege, y frente a qué tipo de operaciones.

Para ello acudimos a su art.1, en el cual queda perfectamente definido su objeto de protección. En virtud del mismo, sabemos que la LOPD tiene como objeto garantizar la protección de cualesquiera derechos fundamentales y libertades públicas de las personas físicas, especialmente su honor e intimidad personal, frente al tratamiento automatizado de sus datos de carácter personal.

Sin embargo, no todos los datos concernientes a las personas serán objeto del mismo nivel de protección. Los hay más o menos protegidos en función de su naturaleza. Así por ejemplo, aquellos datos relativos a la salud, ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual, gozarán de un mayor nivel de protección³³. La ley establece algunas condiciones en relación a los mismos, como la prohibición expresa de crear o almacenar ficheros que contengan exclusivamente este tipo de datos.

³³ Hablamos de lo que la LOPD conoce como datos especialmente protegidos, o datos sensibles, regulados en su art. 7, los cuales tienen un tratamiento diferente al resto de datos.

Tal y como se aprecia en el objeto o finalidad de la LOPD, se regula el derecho a la protección de las personas físicas, sin hacer expresa mención a las personas jurídicas.

Esto hace pensar y así es, que la protección de la privacidad conferida por la LOPD a las personas físicas no es aplicable a las personas jurídicas, pues no gozan de las garantías establecidas en la Ley Orgánica, sin perjuicio de que los Tribunales puedan atender las reclamaciones de responsabilidad que pudieran plantearse en supuestos de realización de un uso perjudicial de información relativa a empresas³⁴.

Además, por si ello no fuera suficiente, el RDLPD elimina cualquier tipo de incertidumbre, al indicar expresamente en su ámbito de aplicación que “Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas”.

Por consiguiente, queda definido el titular del derecho a la protección de datos, que será en todo caso una persona física, debiendo excluir a las personas fallecidas. Esto es así debido a que la muerte provoca la extinción de la personalidad de las personas³⁵, y con ello el ejercicio de determinados derechos como es el derecho a la protección de datos, es decir, el poder controlar nuestros datos y decidir y consentir sobre la posibilidad de que un tercero pueda conocer y tratar nuestra información.

No obstante, si bien es evidente que los tratamientos de datos de personas fallecidas no pueden quedar comprendidos dentro del ámbito de aplicación de LOPD, nada obsta a que las personas vinculadas al fallecido, por razones familiares o análogas, puedan dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste, con la finalidad de notificar la muerte, aportando acreditación suficiente del mismo y solicitando cuando se estime oportuno la cancelación de los mismos.

De esta forma, el sujeto interesado o afectado ante una posible vulneración de su derecho a la protección de datos será en todo caso una persona física, a la cual la LOPD le otorgará en ese caso su debida protección, reconociéndole derechos tales como el derecho de consulta al Registro General de Protección de datos, el derecho de impugnación de valores y los denominados derechos ARCO.

En cuanto al derecho de impugnación de valores, hay que entenderlo como aquel que legitima al sujeto afectado a proteger su privacidad frente a la posibilidad de que

³⁴ ECIJA ABOGADOS. *Protección de datos personales*. Aranzadi, 2010, pág. 67.

³⁵ Queda expresamente recogido en el art. 32 CC, el cual dispone que “la personalidad civil se extingue por la muerte de las personas”.

alguien utilice sus datos personales para evaluar determinados aspectos de su personalidad (rendimiento laboral, crédito, fiabilidad, hábitos, conducta...) y utilice la información obtenida para tomar algún tipo de decisión que les afecte de forma significativa (determinar si es válido para un puesto de trabajo, concederle una hipoteca...)³⁶.

Y, por otro lado, respecto al derecho de consulta al Registro General de Protección de Datos hay que atender al art. 14 LOPD, en virtud del cual “El Registro General será de consulta pública y gratuita”. Ello nos lleva a afirmar que el interesado podrá acceder gratuitamente a la información relativa a la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento, mediante la simple consulta al Registro de Protección de Datos.

El ámbito de aplicación, regulado en su art. 2, se centra en los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y en toda modalidad de uso posterior de estos datos por los sectores público y privado. No obstante, no será de aplicación a cualquier tipo de fichero que contenga datos personales, pues se excluye de su ámbito de aplicación a determinadas categorías. Se trata de aquellos ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, de ficheros sometidos a la normativa sobre protección de materias clasificadas y a los ficheros creados para la investigación del terrorismo y otras graves formas de delincuencia organizada. Asimismo, quedan expresamente excluidos los ficheros que se rijan por sus propias normas³⁷.

Por último, debemos hacer referencia al ámbito territorial. Los arts. 2.1 LOPD y 3 RDLOPD establecen que para poder aplicar la normativa española de protección de datos, será imprescindible o bien que el tratamiento se efectúe en territorio español, o bien que no estando el responsable del tratamiento en territorio español le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional. De

³⁶ <http://www.cuidatusdatos.com/derechoslopd/impugnacion/index.html>.

³⁷ El Art. 2.3 LOPD enumera los ficheros que se rigen por sus propias normas. Se trata de los siguientes:

- a) Los ficheros regulados por la legislación electoral.
- b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
- c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
- d) Los derivados del Registro Civil y del Registro Central de Penados y rebeldes.
- e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

igual forma, también podrá ocurrir que ni siquiera estando establecido el responsable en territorio de la Unión Europea utilice en el tratamiento de datos medios situados en territorio español y por ende se le aplique la normativa española, salvo que tales medios se usen únicamente como medios de tránsito.

En relación a esto último, la AEPD, en su Informe de 1 de agosto de 2005, se pronunció respecto a la normativa aplicable al tratamiento de un buque que ocasionalmente atravesase aguas españolas, considerando que la normativa española no era aplicable. Por el contrario, en el Informe 0454/2009, en el cual se resuelve el caso de una empresa ubicada en Estados Unidos, que procedía a través de una página web a la recogida de datos personales, como IP, *logs* y dirección de correo electrónico de su cliente situado físicamente en España, instalando además cookies en su equipo y teniendo acceso a su perfil en redes sociales, la AEPD acabó concluyendo que a este supuesto si era aplicable la normativa española³⁸.

III.2. Futuro ámbito jurídico en la protección de datos; la incidencia en el caso de los menores de edad.

III.2.1. *Reglamento UE 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de esos datos.*

El régimen descrito hasta aquí se va a ver sustancialmente modificado por el Reglamento UE 2016/679, conocido como Reglamento General de Protección de Datos, siendo éste un hito fundamental en la normativa sobre protección de datos. Entró en vigor el 25 de mayo de 2016 pero no comenzará a aplicarse hasta dos años después, el 25 de mayo de 2018. Será de aplicación directa en todos los países miembros de la Unión Europea, sin que sea necesario trámite alguno de adaptación, y supondrá la derogación de la Directiva 95/46/CE.

Hasta entonces, tanto la Directiva 95/46/CE como las normas nacionales que la trasponen, entre ellas la española, siguen siendo plenamente válidas y aplicables, pero los Estados de la Unión Europea, las Instituciones Europeas y también las organizaciones que tratan datos deben ir preparándose y adaptándose para el momento

³⁸ ALVAREZ HERNANDO, J. Y CAZURRO BARAHONA, V. *Practicum Protección de datos*. Ob. cit., págs 44 y 45.

en que el Reglamento sea aplicable. En este sentido, la AEPD recomienda a las empresas implicadas en el tratamiento de datos que vayan adoptando o iniciando la elaboración de determinadas normas necesarias para permitir o facilitar la aplicación del Reglamento, advirtiéndole que dichas normas no pueden ser contrarias a las disposiciones de la vigente Directiva, ni tampoco ir más allá de los poderes de actuación normativa que el propio Reglamento prevé de forma explícita o implícita.

El Reglamento da un importante cambio en el sistema de protección de datos de carácter personal, pues se establece un único marco normativo para todos los países integrantes de la Unión Europea, armonizando las normativas vigentes en materia de protección de datos. Esto se traduce en una mayor confianza y seguridad jurídica, pues toda aquella discrepancia normativa que pudiera existir en materia de protección de datos entre los diferentes estados de la Unión Europea desaparece. El propio Reglamento así lo indica en su Considerando 10, señalando que “Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea”.

Los cambios más relevantes que desde la perspectiva de la protección del menor trae consigo este nuevo Reglamento, son los siguientes:

En primer lugar, amplía el ámbito de aplicación territorial al tratamiento de datos fuera de la UE. Es decir, el Reglamento se aplicará como hasta ahora a responsables o encargados de tratamiento de datos establecidos en la UE, pero se amplía también a responsables y encargados no establecidos en la UE, siempre y cuando realicen tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento.

Por otra parte, las exigencias respecto al deber de informar se presentan con mayor extensión. Hasta ahora los ciudadanos teníamos derecho a saber si nuestros datos iban a ser recogidos, almacenados y tratados por una empresa y con qué fin. Pero el

nuevo Reglamento da más importancia a la información que se nos debe ofrecer y contempla una lista exhaustiva de los contenidos que deben ser expuestos. Asimismo, incluye la obligación de que esta información nos llegue de forma concisa, transparente, inteligible y con un lenguaje claro y sencillo, evitando las fórmulas especialmente enfarragosas y que incorporan remisiones a los textos legales. Con ello se pone fin a la necesidad de tener que leer párrafos y párrafos de las políticas de privacidad sin que, quizá, hayamos tenido del todo claro para qué quieren exactamente nuestros datos y qué uso van a hacer de ellos³⁹. Esta mayor exigencia en cuanto al deber de informar y de hacer llegar la información, parece que está pensada por el legislador para proteger a los menores de edad cuando se conectan al mundo virtual, especialmente a las redes sociales. Éstas a menudo integran sus políticas de privacidad con un lenguaje enfarragoso, y no del todo claro y preciso, obviando además aspectos importantes para el menor de edad, de forma que esto es precisamente lo que se pretende evitar con el nuevo Reglamento.

En el marco de los derechos del interesado o afectado, cabe destacar la inclusión de nuevos derechos como el derecho al olvido y el derecho a la portabilidad de los datos, dos nuevos derechos que suponen mayor control para el ciudadano y especialmente para el menor de edad sobre sus datos objeto de tratamiento. En cuanto al primero de ellos, se presenta como la consecuencia del derecho que tenemos a solicitar que nuestros datos personales sean eliminados y borrados cuando ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando se hayan recogido de forma ilícita. Y en cuanto al derecho a la portabilidad de nuestros datos, se presenta como el derecho a solicitar al responsable del tratamiento la recuperación de los mismos, para su posterior transmisión a otra entidad.

Otra de las importantes novedades que introduce el Reglamento en materia de protección de datos es el relativo al consentimiento. Al igual que hasta ahora, el nuevo Reglamento exige que el consentimiento del interesado sea libre, inequívoco, específico e informado, pero añade el requisito de que dicho consentimiento se otorgue “mediante una declaración o una clara acción afirmativa”. Así, en aquellos supuestos en los que sea necesario el consentimiento del interesado, ya no bastará con el simple consentimiento tácito que en ocasiones se permitía, especialmente en el ámbito de

³⁹ ¿Cómo afecta a los usuarios el nuevo Reglamento de protección de datos europeo? NOTICIA DIARIO DE NAVARRA 16/10/2017.

internet, sino que deberá existir una acción positiva por su parte, que en todo caso el responsable del tratamiento deberá poder demostrar. De esta manera, ya no se entenderá otorgado el consentimiento por la simple navegación en una página web. Ello resultará sumamente importante para garantizar la protección del menor de edad, sobre todo en el marco de las redes sociales, como principal usuario de las mismas, y como sujeto especialmente vulnerable y no del todo consciente de los peligros a los cuales puede enfrentarse.

Otro de los aspectos en los que cambia el RGPD es el relativo al régimen sancionador, el cual se endurece bastante, con importantes incrementos en las cuantías de las sanciones. Hasta ahora existían tres grados de infracción: leve, grave y muy grave, previendo una sanción máxima exigible a las empresas de 600.000€, en caso de incumplimiento de la normativa de protección de datos. A partir de 2018, con el nuevo RGPD, se prevé la posibilidad de sancionar las infracciones con multas administrativas de 10 y 20 millones de euros como máximo, según el tipo de infracción que se haya cometido, o de una cuantía equivalente al 2% o el 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, si se trata de una empresa⁴⁰. Resulta significativo que la pena a imponer al responsable o encargado del tratamiento deberá ser la máxima, cuando nos encontremos ante tratamiento de datos de menores de edad en relación con los servicios de la sociedad de la información (art. 83 RGPD).

Por último, y quizás la mayor novedad a destacar que presenta el RGPD es la evolución de un modelo basado fundamentalmente en el control del cumplimiento a otro basado en el principio de responsabilidad activa. De acuerdo a éste principio, el responsable o encargado del tratamiento deberá llevar a cabo una previa valoración del riesgo que pudiera generar el tratamiento de datos de carácter personal, para, a partir de dicha valoración, adoptar las medidas que pudieran resultar necesarias. El Reglamento entiende que actuar sólo cuando ya se ha producido una infracción es insuficiente, dado que esa infracción puede causar perjuicios o daños a los interesados que pueden ser muy difíciles o incluso imposibles de compensar o reparar y es por ello que introduce este principio de responsabilidad activa como forma de prevención por parte de las organizaciones que tratan datos, En este sentido, y como medida de responsabilidad activa, se introduce la figura de un Delegado de Protección de Datos, que deberá contar

⁴⁰ Para conocer la sanción correspondiente a cada posible infracción, se debe consultar los apartados 4 y 5 del art.83 del Nuevo Reglamento General de Protección de Datos.

con conocimientos especializados en Derecho, y por supuesto en protección de datos. Podrá ser un trabajador en plantilla, o contratado de manera externa, y actuará de forma independiente, en el ejercicio de diversas funciones entre las que destacan informar y asesorar, así como supervisar el cumplimiento del citado RGPD por parte del responsable o encargado⁴¹.

Otra medida implementada por el Reglamento y que obedece a este principio de responsabilidad activa es la obligación de realizar una evaluación de impacto (*Privacy Impact Assessment*) para aquellos casos en que una operación de tratamiento de datos pudiera implicar un alto riesgo para los derechos y libertades de las personas físicas. En la misma deberá evaluarse el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo, de forma que si la evaluación de impacto mostrara un alto riesgo de que el responsable no pudiera mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debería consultarse a la autoridad de control antes de efectuar el tratamiento.

Y finalmente, como tercera medida preventiva o de responsabilidad activa, se establece la obligación de notificación de violaciones de la seguridad de los datos personales por parte del responsable del tratamiento de datos. Deberá hacerlo sin dilación indebida y de ser posible, en un plazo de 72 horas desde de que haya tenido constancia de ella, a la autoridad de control competente. Esta obligación persiste, a menos que el responsable del tratamiento pueda demostrar que la violación de la seguridad de los datos personales no va a entrañar ningún tipo de riesgo para los derechos y las libertades de las personas físicas. No obstante, de no ser así y de existir riesgo para el afectado o interesado, la notificación por parte del responsable deberá efectuarse también a él, a fin de poder mitigar los efectos resultantes de la violación.

Con objeto de cumplir con las nuevas medidas implementadas por este Reglamento, la AEPD cuenta con una guía, “Guía del Reglamento General de Protección de datos para Responsables de Tratamiento”, en el que además de enunciar las principales cuestiones que las organizaciones deben tener en cuenta para cumplir con las obligaciones recogidas en el Reglamento se introducen recomendaciones acerca cómo actuar ante estos nuevos cambios, y cómo enfrentarse ante ellos para que a partir

⁴¹ Si se desea conocer todas las funciones atribuidas al Delegado de Protección de Datos, acudir al art. 39 RGPD.

de mayo 2018 las empresas se hayan adecuado a las previsiones del RGPD. Es decir, tal y como anuncia la propia AEPD, se incluyen recomendaciones o propuestas en la Guía para fomentar que las entidades puedan ir anticipándose al momento en el que las medidas sean de obligado cumplimiento.

III.2.2. Proyecto de la LOPD.

En el caso de España, la adaptación de nuestra legislación al Reglamento Europeo de Protección de Datos hace necesaria la elaboración de una nueva Ley Orgánica en sustitución de la actual. Con fecha 10 de noviembre de 2017, el Consejo de Ministros ha aprobado el Proyecto de Ley Orgánica de Protección de Datos⁴² cuyo objetivo no es otro que la adaptación del ordenamiento jurídico español al Reglamento Europeo de protección de datos, a fin de completar sus disposiciones (Título I Proyecto de LOPD). La norma proyecto de LOPD, establece que el derecho fundamental de las personas físicas a la protección de datos de carácter personal, amparado por el art. 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.

Los aspectos más significativos de la nueva normativa en relación con el menor de edad son:

En primer lugar, la regulación de los datos referidos a las personas fallecidas, respecto a lo cual no se hace mención alguna en el Reglamento Europeo. Únicamente se establece que el tratamiento de datos de las personas fallecidas queda excluido de su ámbito de aplicación. No obstante, con este Proyecto de Ley Orgánica se da un paso más, y se permite que los herederos puedan solicitar el acceso a los mismos, así como su supresión o rectificación, en su caso siempre con sujeción a las instrucciones del fallecido. Supone una novedad muy importante, por la posibilidad de encontrarnos perfiles y datos de nuestros familiares o allegados fallecidos en redes sociales y plataformas digitales.

En cuanto a los derechos de las personas, la nueva LOPD adapta al Derecho Español el principio de transparencia en el tratamiento del Reglamento europeo. Se recoge el denominado modelo de información por capas o niveles, para hacer compatible la mayor exigencia de información que introduce el RGPD y la concisión y comprensión en

⁴² El Gobierno aprueba el proyecto de Ley Orgánica de Protección de Datos. NOTICIA EXPANSIÓN. 10/11/2017.

la forma de presentarla. De acuerdo a dicho modelo, se presentaría la información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recogieran los datos, y la información adicional quedaría plasmada en un segundo nivel.

En cuanto al régimen sancionador, se establece en la exposición de motivos del Proyecto de LOPD, que el RGPD contiene un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. De esta forma, en la nueva LOPD se procede a describir las conductas típicas, diferenciando entre sanciones leves, graves y muy graves, tomando en consideración la distinción que hace el Reglamento europeo al fijar la cuantía de las sanciones. En relación al caso de menores de edad, el tratamiento de datos de carácter personal sin recabar su consentimiento, cuando el menor esté en condiciones de prestarlo o el del titular de su patria potestad o tutela cuando no el menor de edad no tenga capacidad para ello, así como el hecho de no acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por el menor de edad o por el titular de su patria potestad o tutela sobre el mismo, supondrán la calificación de infracciones graves y tendrán aparejadas sus correspondientes sanciones (art. 73 Proyecto de LOPD).

Por otra parte, la importancia que adquiere la figura del delegado de protección de datos en el RGPD, queda plasmada en este Proyecto de ley Orgánica, que parte del principio de que puede tener carácter voluntario u obligatorio, formar parte o no de la organización del responsable o encargado y ser tanto persona física como jurídica. En el Reglamento Europeo ya se establecía que la designación de esta figura no sería preceptiva en todo caso, pero en el Proyecto de Ley Orgánica se viene a concretar más detalladamente, y se establece en forma de *numerus clausus* los supuestos en que sí procede su nombramiento. Entre ellos, cabe destacar los casos de tratamientos de datos por prestadores de servicios de la sociedad de la información (redes sociales), o los centros docentes que ofrezcan enseñanzas reguladas por la Ley Orgánica 2/2006, de 3 de mayo, de Educación. El hecho de que el legislador exija el nombramiento de un Delegado de Protección de Datos en estos casos como medida de prevención puede tener su explicación en los sujetos implicados y posibles afectados, que son principalmente los menores de edad.

Finalmente, en el Proyecto de LOPD, se introduce un cambio en relación al consentimiento del menor de edad para el tratamiento de sus datos, sobre el que incidiremos a continuación.

IV. LA PROTECCIÓN DE DATOS EN SU PROYECCIÓN AL MENOR DE EDAD Y EN EL MARCO DE LAS REDES SOCIALES.

IV.1. El menor de edad como sujeto especialmente protegido.

En materia de protección de datos, los menores de edad merecen una protección especial, pues se trata de un sector de la sociedad todavía no formado, un sector frágil y dependiente respecto de sus progenitores o tutores legales.

Estamos hablando de personas especialmente vulnerables, no del todo conscientes de los riesgos y amenazas actuales que la informática puede ocasionar y que acceden a internet sin ningún tipo control, lo cual obliga a tener una mayor exigencia en el tratamiento de sus datos y un mayor rigor en el cumplimiento de los requisitos de la normativa de Protección de Datos.

Ya desde la AEPD se advierte del peligro que, para los menores, los denominados nativos digitales tienen las nuevas tecnologías y en particular internet y de su especial vulnerabilidad en este entorno. Además, subrayan la importancia del papel que deben asumir los padres, tutores y profesores en recordar a los niños que sus datos personales son importantes, que deben protegerlos y cuidarlos, y concienciarles del uso responsable que deben hacer de los mismos^{43,44}.

En definitiva, la falta de madurez de los menores de edad, y su condición como sujetos especialmente vulnerables, hace que proteger su privacidad sea uno de los objetivos primordiales actualmente. En este sentido, el Reglamento Europeo que se aplicará a partir del 25 de mayo de 2018, trata de reforzar a nivel europeo la protección de los datos de carácter personal de los menores de edad, advirtiendo de la necesidad de

⁴³ Internet y Menores. Página web AEPD.

⁴⁴ La AEPD cuenta con un sitio web, “Tú decides en internet”, que contiene dos guías realizadas por ella “No te enredes en Internet” orientada a los menores y “Guíales en Internet”, para padres y profesores, con consejos y recomendaciones dirigidas a ellos. Además, recientemente, concretamente en octubre de 2017, presentó “Los menores y su ciber mundo”, un taller dirigido a familias que contiene diversos videos sobre consejos y pautas a seguir por los padres en su labor de proteger al menor de edad en su uso de las nuevas tecnologías.

garantizar una protección específica de sus datos, pues son menos conscientes de los riesgos, consecuencias, garantías y derechos relativos al tratamiento de sus datos⁴⁵.

IV.2. Peculiaridades en materia de protección de datos respecto al menor de edad.

IV.2.1 Consentimiento para el tratamiento de sus datos.

Como sujetos especialmente protegidos, a los menores de edad se les dispone un régimen específico, con determinadas peculiaridades en materia de protección de datos.

Cuestión clave en este sentido y que merece especial atención, es la relativa al consentimiento para el tratamiento de sus datos. El art. 13 del actual RDLOPD es el encargado de esta cuestión, y exige diferenciar entre menores de 14 años, y mayores de 14. Los primeros necesitarán en todo caso la autorización de sus padres o tutores para consentir en el tratamiento de sus datos, mientras que los restantes podrán hacerlo por sí mismos, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela.

Ello supone considerar que los mayores de 14 años tienen la madurez suficiente como para consentir por sí mismos en el tratamiento de sus datos. Pero, al contrario, a los menores de 14 años no se ofrece una solución favorable a que puedan prestar el consentimiento, por lo que deberá estarse a sus condiciones de madurez, tal y como establece el art. 162.1 del CC: “Se exceptúa de la representación legal de los padres que ostenten la patria potestad de sus hijos menores no emancipados los actos relativos a los derechos de la personalidad que el hijo, de acuerdo con su madurez, pueda ejercitar por sí mismo”. Así, teniendo en cuenta que el derecho a la protección de datos es un derecho de la personalidad, habrá que pensar que quedan incluidos en esta previsión, entendiéndolo así EGUSQUIZA BALMASEDA, al indicar que este precepto faculta al menor de edad con madurez suficiente “para decidir por sí respecto al tratamiento de sus datos”⁴⁶.

Además, debemos recordar la Ley Orgánica 1/1982 sobre protección civil del derecho al honor, intimidad familiar y personal y a la propia imagen, que dispone que, si el menor no tuviera madurez suficiente para prestar su consentimiento en el ámbito de estos derechos, serán sus padres quienes deban hacerlo (apartado 1 art. 3).

⁴⁵ Ello queda expresamente recogido en el Considerando 38 del Reglamento UE 2016/679.

⁴⁶ EGUSQUIZA BALMASEDA, M.A. “Protección de datos: intimidad y salud”, *Cuadernos de Aranzadi Civil*, nº35, Aranzadi, Cizur Menor, 2009, págs. 82 y 83.

Otra norma jurídica importante es la LOPJM, de cuyo art. 4.3 se deriva la posibilidad de que haya sido el propio menor quien, por sí mismo, haya prestado su consentimiento a la utilización de su propia imagen, sin precisar para ello la asistencia de su representante legal, lo que no hace sino ahondar en la conclusión ya referida anteriormente, a partir de lo dispuesto en el artículo 162 del CC⁴⁷.

De forma que cada caso concreto deberá ser estudiado detenidamente, analizando las condiciones de madurez del menor de edad, pues de ello dependerá que se requiera o no el consentimiento de los padres para un posible tratamiento de sus datos. No obstante, siempre recordando que los derechos a la protección de datos pertenecen al menor de edad y no a su representante, que se limita a ejercerlos, siempre en beneficio del menor. Es decir, el hecho de que sean los padres o tutores quienes presten el debido consentimiento, no implicará que la condición jurídica del representante tenga una prioridad absoluta o incondicional sobre el niño, porque el interés superior de este puede, en ocasiones, conferirle derechos relativos a la protección de datos que puedan anular los derechos de los progenitores o representantes⁴⁸. De hecho, el menor de edad podrá revocar en todo caso el consentimiento otorgado por su representante para el tratamiento de sus datos, cuando alcance la mayoría de edad.

Actualmente se habla de los 14 años como edad a partir de la cual los menores pueden prestar por sí mismos el consentimiento para el tratamiento de sus datos personales, pero en este punto el nuevo Reglamento de protección de datos introduce un cambio, fijando como límite los 16 años y no los 14 en el ámbito de los servicios de la sociedad de la información (por ejemplo, redes sociales). No obstante, permite rebajar esa edad y que cada Estado miembro establezca la suya propia, estableciendo un límite inferior de 13 años. En el caso de España, esta edad está fijada actualmente en 14 años, pero con el Proyecto de LOPD se reduce desde los 14 a los 13 años para adaptar así el sistema español al Reglamento (art. 7 Proyecto LOPD).

Tal y como podemos observar, tanto la normativa actual (art. 13 RDLOPD), como el futuro Reglamento de Protección de datos y el Proyecto de LOPD, atienden a un criterio objetivo, la edad, para considerar al menor de edad como sujeto capaz de consentir en el tratamiento de sus datos. Concretamente, queda fijado los 14 años (13

⁴⁷ Consentimiento otorgado por menores de edad. AEPD.

⁴⁸ PÉREZ LUÑO, A.E. “La protección de los datos personales del menor en Internet”, *Anuario de la Facultad de Derecho*, núm. 2, 2009, págs. 143-175.

con la nueva LOPD) como edad a partir de la cual el menor tiene capacidad para ello. En relación a esto, parece lógico preguntarnos por qué utilizar como criterio los 14 años, y no otra edad distinta, más aún si tenemos en cuenta que la legislación civil utiliza otras edades distintas para determinar la capacidad del menor en determinados actos. Así por ejemplo, queda señalada los 12 años como edad a partir de la cual el menor de edad es capaz para consentir su acogimiento o adopción (art. 173 CC), o la edad de 16 años para poder solicitar la emancipación (arts. 317, 320, 321 CC), celebrar un contrato de trabajo o realizar actos de administración ordinaria con respecto a los bienes adquiridos con el rendimiento de su trabajo (art. 164.2. 3º CC).

Asimismo, otro aspecto que no parece del todo razonable y que resulta cuanto menos contradictorio, es que la normativa actual y el Reglamento europeo de protección de datos partan de un criterio objetivo como es la edad para consentir el tratamiento de datos del menor de edad y que otros textos legales, como la Ley Orgánica sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y el art. 162 CC, utilicen como criterio la madurez del menor. A mi modo de ver, debería emplearse un mismo criterio, un criterio uniforme para todos los actos que requieran el consentimiento del menor de edad, considerando además que debiera ser la madurez, pues es la que va a determinar el juicio crítico de cada uno.

Por otra parte, el régimen de tratamiento de datos relativo al menor de edad, contiene límites en cuanto a la recogida de su información o datos personales. El propio RDLOPD señala en su art. 13.4 que en ningún caso podrán solicitarse datos que permitan obtener información relativa a otros componentes de la familia o sobre sus características, como pueden ser los datos referidos a la profesión de los padres, situación económica, datos sociológicos o cualesquiera otros sin el consentimiento de los titulares de los mismos. No obstante, añade que sí podrían recabarse los datos de identidad y dirección de los padres o tutores con la finalidad única de obtener la autorización necesaria para prestar un consentimiento válido.

Finalmente, cómo último aspecto a recalcar respecto al tratamiento de datos de menores de edad es que la información dirigida a ellos deberá expresarse en un lenguaje claro y sencillo, que sea fácilmente comprensible por aquéllos.

IV.2.2 Ejercicio de los derechos ARCO.

El menor de edad, como titular del derecho a la protección de datos personales, es a su vez titular de los llamados derechos ARCO, cuatro derechos personalísimos cuyo ejercicio únicamente cabe por el interesado. No obstante, podrá actuar el representante legal del mismo cuando” el afectado se encuentre en situación de incapacidad o minoría de edad que imposibilite el ejercicio personal de los derechos (art. 23.2 a) RDLOPD). Fuera de esta previsión, ni el artículo 13 RDLOPD se pronuncia al respecto, así como tampoco lo hace el Reglamento Europeo ni en su art. 8 ni en los arts. 15 y siguientes, por lo que se desconoce cuándo el menor es capaz para prestar su consentimiento ante tales derechos y cuándo no lo es. Ante la falta de regulación alguna, autores como REBOLLO DELGADO Y SERRANO PÉREZ entienden que habrá que acudir al art. 13 RDLOPD para resolver la cuestión, de forma que en aquellos supuestos en que no se precise el consentimiento de los titulares de la patria potestad o tutela podrá ejercitarse por el menor de entre 14 a 18 años el derecho ARCO correspondiente.

En este sentido, como el art. 13 RDLOPD requiere el consentimiento de los progenitores para el tratamiento de los datos de los menores de catorce años, también implica que sean estos sujetos quienes ejerciten los derechos de acceso, rectificación, cancelación y oposición, aunque nada diga la norma. En definitiva, consideran que debe aplicarse la regla objetiva de la edad, tanto para el consentimiento, como para el ejercicio de estos derechos ARCO con la finalidad de conseguir una mayor seguridad jurídica, ya que no tendría sentido establecer edades distintas⁴⁹.

Por otra parte, junto a la representación legal por parte de los padres o tutores, en aquellos casos en que el menor de edad ostente capacidad legal plena, esto es, cuando sea mayor de 14 años, podrá nombrar a un representante voluntario para que actúe en su nombre. Deberá hacerlo expresamente mediante el otorgamiento de un poder específico que se refiera al ejercicio del derecho ARCO correspondiente, e indicando claramente los términos en que el apoderamiento se realiza, de forma que en ningún caso el mandatario se exceda de lo dispuesto en los mismos. Dicho poder de representación podrá elevarse a escritura pública, o bien constar en documento privado, pero en este caso, será necesario que la firma del representado sea autenticada ante notario.

⁴⁹ REBOLLO DELGADO, L. Y SERRANO PÉREZ, M.M. *Manual de Protección de Datos*, Dykinson, Madrid, 2014, págs. 126 y 303.

Además, deberá aportarse en todo caso copia del DNI del representado o documento equivalente⁵⁰.

Y junto a estos 4 tradicionales derechos ARCO, de igual manera operaría el ejercicio de dos nuevos derechos incorporados al RGPD como son el derecho a la portabilidad de los datos y el derecho al olvido. Este último derecho, supone una garantía para el menor de edad sobre todo en el marco de las redes sociales e Internet. Se trata de una solución que el nuevo RGPD le ofrece, como sujeto que haya podido proporcionar datos de carácter personal sin haber sido plenamente consciente del impacto que esa información subida a la Red podía causarle en un futuro. Supone para el menor de edad la posibilidad de obtener sin dilación indebida del responsable del tratamiento la supresión total de los datos personales que le conciernan y que haya proporcionado a través de un servicio de información (art. 17 RGPD). Es un derecho que cobra especial importancia, pues la simple cancelación de los datos subidos a la red social no es efectiva, debido a la dificultad de eliminar de forma absoluta el contenido en Internet, incluso cuando el usuario ya se ha dado de baja de la red social.

IV.3. Menores de edad en el uso de las redes sociales: falta de control por parte de los proveedores del servicio en el cumplimiento de los requisitos de la normativa de protección de datos.

IV.3.1 Aspectos generales.

Un ámbito en el que la tutela de los datos resultará especialmente relevante es el de las redes sociales, por la gran cantidad de información que se facilita y se comparte, y por la multitud de riesgos y peligros que puede entrañar su uso. Sobre todo, teniendo en cuenta la sociedad en que vivimos, en la que constantemente los hijos, desde el momento en que nacen, se ven sometidos a la sobreexposición por parte de sus padres, que publican y comparten fotografías y videos a través de las redes sociales, y en la que cada vez los niños hacen un uso más frecuente de ellas⁵¹. Hoy en día, no es de extrañar que ello ocurra, pues navegar por Internet, y formar parte de una red social es relativamente sencillo.

⁵⁰ ALVAREZ HERNANDO, J. Y CAZURRO BARAHONA, V. *Practicum Protección de datos*. Ob. cit., pág. 203.

⁵¹ Los últimos datos que disponemos revelan, de acuerdo a un informe de la OCDE que casi una cuarta parte de los chicos y chicas de 15 años pasa más de seis horas al día en Internet cuando sale de clase y el 17% de los estudiantes empezó a utilizar Internet cuando tenían 6 años o menos. Y más aún, el INE describe como “universal” el uso de internet a los 10 años.

En el propio Dictamen 5/2009 sobre las redes sociales en línea, elaborado por el Grupo de Trabajo 29, queda patente el modo de acceso a ellas. En él se viene a decir que únicamente los usuarios deben proporcionar determinados datos personales para generar su descripción o perfil en una red social, y a partir de entonces, es cuando el proveedor del servicio lleva a cabo un tratamiento de datos personales, legitimación que solamente debiera encontrarse en el consentimiento del menor, y que deber reunir las características de ser libre, inequívoco, específico e informado.

La experiencia demuestra que no existe ningún tipo de control eficaz y seguro que garantice la autenticidad y verificación de los requisitos exigidos por el legislador para poder acceder a una red social, como es la edad mínima exigida como requisito imprescindible (actualmente 14 años), o el consentimiento de los padres o representantes legales en el caso de que el menor no la haya cumplido. Únicamente suele establecerse dentro de las políticas de privacidad y condiciones de uso de determinadas redes sociales como es el caso de Facebook, Instagram o Twitter que si los padres tienen conocimiento de que un menor ha accedido a sus servicios pueden ponerlo de manifiesto al servidor y éste prestará la ayuda necesaria para retirar lo antes posible todo el material o datos que hubieran sido facilitados y para cancelar la cuenta⁵².

Por consiguiente, es necesario y urgente que los responsables de estas aplicaciones, los denominados proveedores del servicio que van a llevar a cabo tratamientos de datos establezcan sistemas de verificación y control seguro, fiable y eficaz que respeten la legalidad y la edad mínima requerida para las mismas, a fin de que no ocurra lo que en la práctica está sucediendo, que menores de 14 años falseen la edad mínima y acceden a la red social. Se trata de un tema bastante preocupante, más aún si tenemos en cuenta el art. 13.4 RDLOPD, según el cual corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Y además, no debemos obviar el nuevo Reglamento de Protección de datos, el cual exige a los responsables del tratamiento de datos, esfuerzos razonables, para verificar que el consentimiento se ha prestado o autorizado por los padres o

⁵² <http://www.lawandtrends.com/noticias/tic/edad-menores-redes-sociales-cual-es-la-edad-en.html>

responsables del menor si éste no ha cumplido la edad mínima establecida por los Estados miembros (art. 8.2 RGPD).

En este sentido, el Grupo de Trabajo 29 ya fomenta investigaciones complementarias sobre la manera de solucionar las dificultades que rodean la comprobación de la edad requerida y la prueba del consentimiento informado, con el fin de afrontar lo mejor posible estos retos que se plantean (Dictamen 5/2009).

Todo ello resulta especialmente importante, máxime si tenemos en cuenta la gran cantidad de información relativa a nuestra vida, preferencias, hábitos, gustos... que pueden manejar las redes sociales una vez que accedemos a ellas, incluso aun sin nuestro consentimiento, y los riesgos y peligros que se pueden derivar. En este sentido, podemos sacar a la luz la resolución R/01870/2017 de la AEPD, en la cual se declara que ésta se ha visto obligada a imponer una sanción de 1,2 millones de euros a Facebook por vulnerar la normativa sobre protección de datos personales de sus usuarios. La agencia ha constatado que la red social recopila, almacena y utiliza información de los usuarios para fines publicidad sin haber obtenido la previa autorización para ello. Concretamente, se desprende que Facebook ha obtenido información sobre la ideología, el sexo, las creencias religiosas, los gustos personales o la navegación de sus usuarios sin que estos le hayan dado un “consentimiento inequívoco”. De igual forma, la AEPD alude a la política de privacidad de Facebook, y señala de la misma que contiene "expresiones genéricas y poco claras", y obliga a acceder a multitud de enlaces distintos para conocerla. Y continúa diciendo que la red social hace referencia de forma imprecisa al uso que va a hacer de los datos que recoge, de forma que el usuario no llega a ser consciente de la recogida de datos que realiza Facebook, ni de su almacenamiento, ignorando en todo momento la finalidad para la cual van a ser utilizados⁵³.

IV.3.2. Consecuencias de la falta de control por parte de los proveedores del servicio en el cumplimiento de la normativa de protección de datos.

De acuerdo al art. 9.1 LOPD, el proveedor de la red social se encuentra obligado a adoptar las pertinentes medidas de índole técnica y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o

⁵³ Protección de Datos multa a Facebook con 1,2 millones por usar información sin permiso. NOTICIA EL PAIS 11/09/2017.

acceso no autorizado. Son los titulares de las redes sociales y han de actuar con la debida diligencia y prevención necesaria, de acuerdo a las prescripciones legales. Ello implica obligaciones como proporcionar a los usuarios menores de edad información detallada sobre las finalidades y las distintas maneras en que van a tratar sus datos personales, así como realizar esfuerzos para verificar que el consentimiento se ha prestado por los padres o responsables del menor si éste no ha cumplido la edad mínima exigida para ello. Así, la falta de cumplimiento de tales obligaciones, u otras como la falta de exigencia del consentimiento expreso y por escrito de los padres o tutores del menor en sus políticas, la no cancelación de perfiles y cookies, la cesión de datos, los usos distintos a la finalidad para la que fueron recogidos, o la indexación de datos y perfiles personales constituirán hechos suficientes para exigir responsabilidad a los proveedores de las redes sociales⁵⁴.

En cuanto a la responsabilidad a la cual podrán estar sujetos en caso de no adecuarse a la normativa de protección de datos, el art.13 LSSICE señala que podrá ser civil, penal y administrativa. Ello dependerá del hecho o infracción cometida, y del perjuicio ocasionado al menor de edad.

Respecto a la responsabilidad civil por los daños y perjuicios causados, el art. 1902 CC establece que “El que por acción u omisión cause daño a otro, interviniendo culpa o negligencia, estará obligado a reparar el daño causado”. Es habitual que este tipo de responsabilidad, además de ser exigible a las propias redes sociales, especialmente cuando no actúen diligentemente en la cancelación de la información cuando la misma haya sido solicitada por el perjudicado, o cuando se trate de menores, cuyo consentimiento expreso no pudiera ser verificable, recaiga también sobre aquellas personas usuarias de la red social, que vulneren la intimidad o la protección de datos personales de terceros, publicando datos, fotografías o videos de otros sin su consentimiento, o con su oposición⁵⁵. Es posible que el afectado sufra un daño moral como consecuencia de una intromisión a su derecho al honor, intimidad o imagen y deba ser reparado del mismo a través de la correspondiente indemnización. En este sentido resulta interesante conocer cómo se valorará el daño moral, y para ello el art. 9 de la Ley Orgánica 1/1982 sobre protección civil del derecho al honor, intimidad

⁵⁴ BARRIUSO RUIZ, C. “Las redes sociales y la protección de datos hoy”, *Anuario de la Facultad de Derecho*, nº. 2, 2009, págs. 301-338

⁵⁵ GIL ANTÓN, A.M. “La privacidad del menor en Internet”, *Revista de Derecho, Empresa y Sociedad*, nº 3, 2013, págs. 60-96.

familiar y personal y a la propia imagen establece que deberá atenderse a las circunstancias del caso y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta, en su caso, la difusión o audiencia del medio a través del que se haya producido.

Sin perjuicio de este tipo de responsabilidad, también el proveedor del servicio podrá estar sujeto a determinadas sanciones por no adecuarse a la normativa de protección de datos. La cuantía de la multa a la cual se enfrentará dependerá del tipo de infracción cometida, leve, grave o muy grave⁵⁶. De acuerdo a la actual LOPD, las infracciones leves serán sancionadas con multa de 900 a 40.000 euros, las graves con multa de 40.001 a 300.000 euros y las infracciones muy graves con multa de 300.001 a 600.000 euros. Así por ejemplo, un tratamiento de datos de carácter personal sin recabar el consentimiento de las persona afectada cuando el mismo sea necesario, o una cesión no consentida de los mismos, implicará para el proveedor de la red social una multa de entre 40.001 y 300.000 euros, por ser considerada tal infracción como grave (arts. 44 y 45 LOPD). Con el Proyecto de la LOPD, estas penas se endurecen, y , el tratamiento de datos de carácter personal sin recabar el consentimiento del menor o del titular de su patria potestad o tutela cuando no el menor de edad no esté en condiciones de prestarlo, así como el hecho de no acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por el menor de edad o por el titular de la patria potestad o tutela sobre el mismo, supondrán infracciones graves y llevarán sanciones de hasta 10 o 20 millones de euros (art. 73 a) y b) Proyecto de LOPD). Por otro lado, si el proveedor de la red social empleara los datos recabados del usuario para una finalidad que no fuera compatible con la finalidad para la cual fueron recogidos, tal conducta sería calificada como infracción muy grave (art. 72 d) Proyecto de LOPD) y también llevaría aparejada sanción administrativa de hasta 10 o 20 millones de euros. Las sanciones a imponer son las que establece el Reglamento Europeo de protección de datos, y su importe dependerán de aspectos tales como la naturaleza, gravedad y duración de la infracción, la intencionalidad o negligencia en la infracción, cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados, el grado de responsabilidad del responsable o del

⁵⁶ Las infracciones con sus correspondientes sanciones se encuentran reguladas en los arts. 44 y 45 de la LOPD y en el Título IX del Proyecto de LOPD.

encargado del tratamiento, etc. (Art. 76 Proyecto de LOPD y art. 83.2 Reglamento Europeo de Protección de datos).

Y por otra parte, si el hecho cometido es constitutivo de infracción penal, también entrará en juego la debida responsabilidad penal. Habrá que estar al hecho delictivo que el proveedor de la red social haya podido cometer, y en función de ello, establecer la pena correspondiente que en su caso establezca el Código Penal.

En definitiva, es importante que los proveedores de las redes sociales no cometan hechos o políticas abusivas, alegales o ilegales, o por el contrario, deberán responder en la vía civil, penal o administrativa por ello.

IV.4. Papel de los padres frente al menor de edad en el uso de las redes sociales.

IV.4.1 Conflicto entre el ejercicio de la patria potestad de los padres frente al derecho a la intimidad del menor.

Todos los peligros derivados de las redes sociales, unidos a las cifras de usuarios de Internet menores de edad reveladas por la OCDE, son suficientes para poner la protección del menor en primera línea de intervención. Los padres deben ser conscientes de ello, y deben acompañar a sus hijos en el mundo de las redes sociales, concienciándoles y previniéndoles de todo peligro que puedan encontrarse. Esta relación de padres e hijos como principales usuarios de las redes, queda recogida en la Ley 10/2017, de 27 de junio, de voluntades digitales catalana, según la cual “los progenitores deben velar por que la presencia del hijo en potestad en entornos digitales sea apropiada a su edad y personalidad, a fin de protegerlo de los riesgos que puedan derivarse”. Asimismo, continúa señalando que “los progenitores podrán promover las medidas adecuadas y oportunas ante los prestadores de servicios digitales y, entre otras, instarlos a suspender provisionalmente el acceso de los hijos a sus cuentas activas, siempre y cuando exista un riesgo claro, inmediato y grave para su salud física o mental, habiéndolos escuchado previamente” (art. 3 Ley de voluntades digitales catalana).

Podemos pensar que una manera de proteger al menor es controlando sus cuentas privadas Facebook, Instagram, Twitter u otras redes que puedan manejar. Pero, ¿Hasta dónde pueden llegar ese control? ¿Es lícito en todo caso?

Para responder a la cuestión planteada, debemos tener en cuenta dos aspectos. Por un lado, la obligación que tienen los padres de respetar la intimidad de los menores

y, por otro lado, la obligación como titulares de la patria potestad de velar por ellos y protegerlos (art. 154 CC). Es decir, nos encontraríamos ante un posible enfrentamiento entre el ejercicio de la patria potestad por parte de los padres, y el derecho a la intimidad del menor.

Cuando se trate de un menor de 14 años, este problema no existiría, pues los padres o tutores no necesitarían el consentimiento de su hijo para acceder a la información publicada en la red social. No obstante, no ocurriría eso en el caso de mayores de catorce años, los cuales podrían negarse a tal acceso⁵⁷.

En este sentido, resulta interesante la Sentencia de 10 de diciembre de 2015⁵⁸, en la cual se estimaron cómo válidas en juicio las pruebas obtenidas a través del acceso por una madre a la cuenta de Facebook de su hija de 15 años, puesto que existían indicios claros de que la menor estaba siendo víctima de acoso sexual a través de dicha red.

El TS señala que en aquellos casos donde haya evidencias de que se está realizando un delito o algún hecho que pueda afectar al menor, los padres si podrán acceder a las redes sociales de sus hijos, para así protegerles. Llama la atención cómo el TS enfatiza que no puede el ordenamiento legal “hacer descansar en los padres unas obligaciones de velar por sus hijos menores, y al mismo tiempo desposeerles de toda capacidad de controlar en casos como el presente”.

Pese a que los menores tienen reconocido su derecho a la intimidad, y así lo deja claro el TS mencionando el art. 4.1 de la Ley de Protección del Menor: “Los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones”, también señala que ese derecho no es absoluto, y puede verse vulnerado cuando choque con otro derecho protegido constitucionalmente, entrando directamente en una ponderación de intereses.

Ello estaría justificado en el principio del interés superior del niño, que debe prevalecer, en caso de intereses en conflicto, incluso frente al derecho a la protección de

⁵⁷ MESSÍA DE LA CERDA BALLESTEROS, J.A., “La utilización y protección jurídico-civil de la imagen de los menores en la red; aspectos legales y de praxis judicial” en FLORES RODRÍGUEZ, J., JORDÁ CAPITÁN, E., MESSÍA DE LA CERDA BALLESTEROS, J.A., DE PRIEGO FERNÁNDEZ, V. *Los derechos de la personalidad de los menores y las Nuevas Tecnologías*, Lefebve El Derecho, Madrid, 2012, págs 130 y 131.

⁵⁸ Sentencia de la Sala Segunda del TS número 864/2015, de 10 de diciembre.

datos. Se recoge en nuestro derecho positivo en la Ley de Protección del Menor, concretamente en su art. 2, que establece lo siguiente: “En la aplicación de la presente Ley primará el interés superior de los menores sobre cualquier otro interés legítimo que pudiera concurrir”.

En conclusión, de la mencionada sentencia podemos acabar afirmando que el *modus operandi* habitual de los padres de menores de edad no puede ser acceder indiscriminadamente y de manera injustificada a las cuentas y perfiles de sus hijos en Redes Sociales, por cuanto, el menor es titular de unos derechos que deben ser respetados⁵⁹. No obstante, cuando puedan estar en conflicto otros derechos fundamentales, entrará en juego la obligación que tienen los padres de velar por sus hijos, por su adecuado desarrollo y por su integridad física y psíquica, de forma que podrían ser válidos determinados actos que algunos progenitores llevaran a cabo “conforme al uso social y a las circunstancias o en situaciones de urgente necesidad” (art. 156 CC). En estos casos, habrá que hacer una ponderación de intereses.

Este conflicto entre el deber de los padres de velar por sus hijos, y el derecho a la intimidad del cual son titulares, parece ser un problema recurrente. De hecho, la Audiencia Provincial de Pontevedra a fecha 25 de diciembre de 2017, ha resuelto esta cuestión y ha dictaminado que los padres deben vigilar el uso de las redes sociales de sus hijos menores de edad. El caso que ha llevado a fallar en tal sentido por la Audiencia viene de una inicial denuncia presentada por una madre contra su exmarido y padre de sus hijos, por haber leído conversaciones de Whatsapp de su hija de 9 años con ella presente, acusándole de descubrimiento de secretos y vulneración de la intimidad de la menor. Sin embargo, el auto de la Audiencia Provincial recuerda que el denunciado comparte con la denunciante la patria potestad de sus hijos menores de edad y por ende, la obligación conforme al art. 154 CC de “velar por ellos, educarles y procurarles una formación integral”. Asimismo, señala que el desarrollo de las redes sociales como también lo es Whatsapp “requiere atención y vigilancia de los progenitores para preservar la indemnidad de los menores”. Y por último, resuelve en tal sentido apoyándose en que “no puede decirse, por el relato de la denuncia, que el padre se apoderase sin conocimiento de la hija menor de edad de sus conversaciones de Whatsapp; que las mismas merecieran la calificación de datos reservados; ni que la

⁵⁹ DAVARA FERNANDEZ DE MARCOS, L. *Menores en internet y redes sociales. Derecho aplicable y deberes de los padres y centros educativos. Breve referencia al fenómeno Pokémon Go*. BOE, pág 73.

menor no quisiera que el padre conociera, y menos aún que el denunciado buscara, descubrir los secretos o vulnerar la intimidad de la menor.

IV.4.2. Problemática en el tratamiento de datos de un menor de edad por parte de padres separados.

Las cuestiones planteadas tienen especial relevancia en el caso planteado del consentimiento prestado por los padres para el tratamiento de datos de su hijo menor edad en caso de que estén separados y uno de ellos quiera publicar imágenes suyas en una red social ¿Valdría con el consentimiento de sólo uno de ellos? ¿Qué ocurre si un progenitor no está de acuerdo?

Como punto de partida, debemos comenzar señalando que este problema sólo tendría sentido plantearse para menores de 14 años, pues respecto a los mayores de 14 sabemos que no es necesario el consentimiento parental. Dicho esto, la respuesta hay que cifrarla en el art. 13.1 RDLOPD, en el cual se establece que será requisito imprescindible contar con el consentimiento de los padres o tutores por tratarse de un menor de 14 años, y especialmente en el art. 156 CC, en el cual se regula el ejercicio de la patria potestad de los mismos, señalando que se ejercerá conjuntamente por ambos progenitores o por uno solo con el consentimiento expreso o tácito del otro. En caso de desacuerdo, cualquiera de los dos podrá acudir al Juez, quien, después de oír a ambos y al hijo si tuviera suficiente juicio y fuera mayor de 12 años, decidirá qué progenitor tendrá la facultad, sin que su decisión pueda ser recurrida.

Es decir, en los casos de padres separados o divorciados con la patria potestad compartida y ejercicio del mismo conjunto, ambos tendrán derecho a tomar decisiones conjuntamente respecto a la vida de sus hijos menores, por lo que no podrá actuar uno sin tener en cuenta el consentimiento del otro (salvo en aquellos casos en que por sentencia judicial se haya otorgado la capacidad de decidir a uno sólo de los progenitores). De esta forma, el progenitor que quiera publicar una foto de su hijo menor en una red social, deberá recabar previamente el consentimiento del otro, y, en caso de que éste se oponga, podrá acudir al Juez y solicitarle que se le autorice a publicar la foto en cuestión. Además, no debiendo olvidar en todo caso que tal publicación no podrá suponer una intromisión ilegítima en el derecho al honor, la

intimidad y la imagen del menor, entendiendo por ello cualquier menoscabo de su honra o reputación, o que sea contraria a sus intereses.⁶⁰

En este sentido se ha pronunciado la Audiencia Provincial de Barcelona, en la Sentencia de 25 de abril de 2017⁶¹, en la que resuelve el desacuerdo entre dos progenitores divorciados a la hora de publicar una foto de su hijo menor de edad, en una red social tan comúnmente usada y conocida como es Facebook.

En la mencionada sentencia, la Audiencia Provincial de Barcelona determina que es necesario el consentimiento previo de ambos progenitores antes de publicar una foto de su hijo menor de edad en Facebook. Incluso va más allá, y señala que si se llegara a subir una imagen de manera unilateral por parte de un progenitor sin el consentimiento del otro, podría considerarse que tal publicación es contraria al ordenamiento jurídico, aunque la difusión quedara reducida inicialmente a su grupo familiar y de amigos. Para llegar a dicha conclusión, la Sentencia alude a los siguientes argumentos:

“El derecho a la propia imagen es un derecho fundamental y la decisión de publicar una fotografía del hijo en una red social pertenece a la esfera de la responsabilidad parental compartida por ambos progenitores, no a la guarda”

“Los padres como titulares de la patria potestad tienen el deber y la responsabilidad de proteger la imagen de sus hijos menores de edad y como señala el TS será preciso el acuerdo de ambos progenitores para poder publicar imágenes del hijo común en las redes sociales. En todo caso los padres deberán evitar en interés del menor una sobreexposición del hijo en estos ámbitos”

De esta forma, pese a que en el caso tratado la guardia del hijo la ostenta el padre, también la madre deberá consentir en la publicación de fotografías de su hijo menor en Facebook, pues ella también ejerce la patria potestad.

⁶⁰ El art. 4 de La Ley orgánica 1/1996 de protección jurídica del menor, establece en su apartado tercero que “*Se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre, en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses, incluso si consta el consentimiento del menor o de sus representantes legales.*”

⁶¹ Sentencia CIVIL Nº 360/2017, Audiencia Provincial de Barcelona, Sección 18, Rec 827/2016 de 25 de abril de 2017.

V. CONCLUSIONES.

PRIMERA. Se ha puesto de manifiesto que los riesgos inherentes a la utilización de las Nuevas Tecnologías preocupan especialmente cuando afectan a los menores de edad. Son los principales usuarios de las redes sociales, y como sector más vulnerable dada sus condiciones de madurez, necesitan una mayor protección. A través de ellas comparten todo tipo de información, sus datos más personales, imágenes, videos... sin ser conscientes que están creando su propia identidad digital y de las amenazas y peligros que ello puede acarrear. Piensan que no hay consecuencia alguna, y publican y comparten contenidos sin cautela.

A ello se suma la falta de control por parte de los responsables de las redes sociales, quienes no establecen mecanismos eficaces y seguros de autenticación y verificación de los requisitos que han de cumplirse para registrarse en ellas. Con ello nos estamos refiriendo principalmente a la edad mínima necesaria para acceder a una red social. La realidad es que no existen mecanismos efectivos al respecto, de manera que los derechos del menor, en este ámbito, no están adecuadamente protegidos.

SEGUNDA. Actualmente se atiende a un criterio objetivo, fijando los 14 años como edad a partir de la cual el menor puede consentir en el tratamiento de sus datos por sí mismo, sin necesidad de sus padres o tutores. Ello queda reflejado en el RLOPD, concretamente en su art. 13. Desde mi punto de vista no es una decisión acertada, pues en más de un caso el hecho de alcanzar los 14 años no supone una madurez suficiente por parte del menor, quien no es consciente todavía de los peligros y riesgos que supone el tratamiento de sus datos. Así ha quedado reflejado con anterioridad en la sentencia de 10 de diciembre de 2015, en la que una menor de 15 años estaba siendo víctima de acoso sexual vía Facebook.

Asimismo, no parece del todo razonable, y resulta cuanto menos contradictorio, que el RLOPD establezca una edad concreta (los 14 años) para consentir y que otros textos legales, como la Ley Orgánica sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y el art. 162 CC, utilicen como criterio la madurez del menor.

A mi modo de ver, debería emplearse un mismo criterio, un criterio uniforme, considerando además que debiera ser la madurez, pues es la que va a determinar el juicio crítico de cada uno. La edad únicamente debería usarse como criterio orientativo.

TERCERA. EL 28 de mayo de 2017 será de aplicación el Reglamento de la UE relativo a la protección de datos, que introduce nuevas medidas de protección, exigiendo una mayor responsabilidad al titular del fichero y que permite rebajar la edad mínima para consentir por parte del menor en el tratamiento de sus datos personales a los 13 años. Novedad última no del todo acertada a mi parecer, pues rebajar la edad mínima para otorgar el consentimiento no supone, sino que incrementar los problemas que ya existen respecto al límite actual de los 14.

CUARTA. Por todo lo expuesto, es necesario que el Derecho no permanezca ajeno a esta realidad y que se prevean medidas de protección tanto a priori como a posteriori de los datos que se comparten en la Red. Además, se hace necesaria una concienciación social sobre la importancia de preservar y proteger nuestros datos más íntimos y sobre el uso responsable que debe hacerse de los mismos, tarea que ya lleva a cabo la AEPD, que cuenta con multitud de Guías con consejos y recomendaciones dirigidas a padres, hijos y profesores.

VI. BIBLIOGRAFÍA.

-ALVAREZ HERNANDO, J, CAZURRO BARAHONA, V. *Practicum Protección de datos*. Aranzadi, 2015.

-DAVARA FERNANDEZ DE MARCOS, L. *Menores en internet y redes sociales. Derecho aplicable y deberes de los padres y centros educativos. Breve referencia al fenómeno Pokémon Go*. BOE.

-DÍAZ REVORIO, F.J. “Principios de la protección de datos: derecho de la información en la recogida de datos. Una perspectiva constitucional», en TRONCOSO REIGADA, A. *Comentario a la ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, Civitas, 2010.

-ECIJA ABOGADOS. *Protección de datos personales*. Aranzadi, 2010.

-ENÉRIZ OLAECHEA, FJ Y BELTRÁN AGUIRRE, JL. *La protección de los datos de carácter personal*. Pamplona, 2012.

-FLORES RODRÍGUEZ, J., JORDÁ CAPITÁN, E., MESSÍA DE LA CERDA BALLESTEROS, J.A., DE PRIEGO FERNÁNDEZ, V. *Los derechos de la personalidad de los menores y las Nuevas Tecnologías*, Lefebve El Derecho, Madrid, 2012.

-GARRIGA DOMINGUEZ, A. *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*. Dykinson, Madrid, 2016.

-GIL ANTÓN, A.M. “La privacidad del menor en Internet”, *Revista de Derecho, Empresa y Sociedad*, nº 3, 2013.

-HERRÁN ORTIZ, M.I. *El derecho a la intimidad en la nueva Ley Orgánica de protección de datos personales*, Dykinson, Madrid, 2002.

-LUCAS MURILLO DE LA CUEVA, P. *El derecho a la autodeterminación informativa*. Tecnos, Madrid, 1990.

- LUCAS MURILLO DE LA CUEVA, P. *Informática y protección de datos personales. Centro de Estudios Constitucionales*. Madrid, 1993.
- LUCAS MURILLO DE LA CUEVA, P. “Perspectivas del derecho a la autodeterminación informativa”, *Revista de Internet, Derecho y Política*, núm 5, 2007.
- LUCAS MURILLO DE LA CUEVA, P. Texto de la conferencia que tuvo lugar el 24 de octubre de 2005 en la sede de la Agencia Catalana de Protección de Datos [En línea]. Disponible en: www.apd.cat [2011, 10 de enero].
- PÉREZ LUÑO, A.E. *Manual de informática y derecho*. Ariel, Barcelona, 1996.
- PÉREZ LUÑO, A.E. “ La protección de los datos personales del menor en Internet”, *Anuario de la Facultad de Derecho*, núm. 2, 2009.
- REBOLLO DELGADO, L. *Derechos fundamentales y protección de datos*. Dykinson, Madrid, 2004.
- REBOLLO DELGADO, L, Y SERRANO PÉREZ, MM. *Introducción a la protección de datos*. Dykinson, Madrid, 2006.
- REBOLLO DELGADO, L y SERRANO PÉREZ, M.M. *Manual de Protección de Datos*, Dykinson, Madrid, 2014
- RUIZ MIGUEL, C. “En torno a la protección de los datos personales automatizados”, *Revista de Estudios Políticos (Nueva Época)*, núm. 84 abril – junio, 1994.
- SERRANO PÉREZ, M.M. “El derecho fundamental a la Protección de Datos. Su contenido esencial”, en *Revista Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, 2005.
- VELÁZQUEZ BAUTISTA R, *Protección jurídica de datos personalizados automatizados*. Colex, 1993.

VII. JURISPRUDENCIA CONSULTADA.

STS 864/2015, de 10 de diciembre.

STC 231/1988, de 2 de diciembre.

STC 254/1993 de 20 de julio.

STC 290/2000, de 30 de noviembre.

STC 292/2000 de 30 de noviembre.

STC 57/1994 de 28 de febrero.

STCFA 15 de diciembre 1983.

SAP de Barcelona 360/2017, de 25 de abril de 2017.

SAP de Pontevedra de 25 de diciembre de 2017.