

# **REGULACIÓN DE LA INTERVENCIÓN DE LOS MENORES EN LAS REDES SOCIALES**

Elena Aguiló Cabrera  
DNI: 43214431F  
TFG curso 2013/2014  
Tutora: Cristina Gil Membrado

# ÍNDICE

|   |    |
|---|----|
| 1. Introducción: Sociedad de la Información   | 3  |
| 2. Regulación y concepto de la protección de datos de carácter personal   | 4  |
| 2.1 Regulación de los datos personales  | 4  |
| 2.2 Concepto de datos personales  | 4  |
| 3.El consentimiento de los menores en las redes sociales  | 5  |
| 3.1 Definición  | 5  |
| 3.2 Características   | 5  |
| 3.3 El caso específico del consentimiento de los menores<br>para actuar en la redes sociales  | 7  |
| 4. Medidas de protección de los menores adoptadas por las redes sociales  | 10 |
| 4.1 El proceso de verificación de la edad establecido en Tuenti   | 10 |
| 4.2 Otras medidas posteriores   | 11 |
| 5. La responsabilidad civil de los progenitores o tutores<br>derivada de la actividad de los menores en las redes sociales                | 12 |
| 5.1 En el ámbito civil  | 13 |
| 5.2 En el ámbito penal  | 14 |
| 6.Breve referencia a las intromisiones ilegítimas del derecho al honor,<br>intimidad y propia imagen de los menores en las redes sociales | 16 |
| 7.El derecho al olvido de los menores en las redes sociales   | 17 |
| 7.1 Regulación actual del derecho al olvido de los menores  | 17 |
| 8. Recomendaciones de la AEPD para proteger a los menores<br>en el uso de las redes sociales  | 19 |
| 9.Bibliografía  | 21 |

## **1.Introducción: Sociedad de la información**

La generalización del uso de Internet en la última década ha supuesto un gran impacto en el mundo de las telecomunicaciones y de la información. Esto ha dado paso a lo que se conoce como la Sociedad de la Información la cual hace referencia a una la posibilidad de estar informados a través de las nuevas tecnologías.

En este contexto, las denominadas redes sociales han dado un giro a la utilidad que venían realizando los usuarios de Internet (el de Web 2.0), en la que no se utiliza de forma exclusiva para obtener una información, sino que son ellos mismos quienes interactúan en la red sin a penas limitaciones, ya que son quienes entregan información de forma activa sobre muchos aspectos, incluido datos sobre su propia vida.

Concretamente en la redes sociales, las informaciones más importantes que se utilizan tienen que ver con los datos personales de los usuarios, ya que primeramente son necesarios para registrarse en una red social y en segundo lugar se exponen cuando se crea un perfil, en el que en muchas ocasiones no únicamente se utilizan los propios, sino que también entran en juego los datos de terceros (cuando por ejemplo, se hace referencia o se publican fotografías de personas del entorno de los usuarios) incluso cuando alguno de estos no tenga un perfil en una red social o tan siquiera no tenga acceso a Internet y por tanto este totalmente desvinculado de la Sociedad de la Información.

Esto crea una problemática en torno al tratamiento de los datos personales de los usuarios y los riesgos que su divulgación por las redes sociales supone a su privacidad. DE MIGUEL ASENSIO<sup>1</sup> determina que los peligros que pueden haber entorno al tratamiento de los datos personales en las redes sociales surgen desde diversos frentes. Por un lado, la forma en que los proveedores de las redes sociales ofrecen sus servicios, ya que esto tiene repercusión en la información a la que pueden tener acceso terceros. Por otro lado, determinar que datos personales son utilizados por el administrador del servicio en la red social. Y por último, el consentimiento realizado por los usuarios para la facilitación de sus datos personales, que vendrá detallado en las condiciones de uso, términos legales y políticas de privacidad de cada red social.

Este conjunto de riesgos tiene una mayor trascendencia cuando hay menores implicados, ya que la generalización del uso de Internet y de las redes sociales y su fácil acceso han generado que se extremen las precauciones al ser un colectivo vulnerable, en cuanto al consentimiento que pueden prestar, los contenidos a los que puedan tener acceso, la responsabilidad que tendrán al realizar determinadas actividades en las redes sociales o la vía que tendrán para suprimir su cuenta. Es necesario que haya una actuación tanto de los progenitores o tutores, como los responsables (administradores o proveedores) de las redes sociales destinada a la protección de los menores ante los riesgos que puede suponer que sean usuarios de las redes sociales.

## **2. Regulación y concepto de la protección de datos de carácter personal**

### **2.1 Regulación de los datos personales**

En el ordenamiento jurídico español, la protección de los datos personales tiene su principal regulación en la Ley Orgánica 15/1999<sup>2</sup> (LOPD)<sup>3</sup>, y en el Real Decreto 1720/2007<sup>4</sup> (RLOPD). Concretamente el art. 1 LOPD es el que establece que el tratamiento de los datos personales de las personas físicas se regularán mediante esta ley orgánica.

### **2.2 Concepto de datos personales**

El concepto de datos personales viene regulado en el art. 3 LOPD que determina que es “cualquier información concerniente a personas físicas identificadas o identificables”. Se define de forma parecida en el art. 5 del RLOPD ya que se añade que esta información “ha de ser numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas”.

El Tribunal Constitucional (TC) ha establecido en su STS 292/2000<sup>5</sup>, que el derecho de las personas a la protección de sus datos personales se ejercita cuando se puede “garantizar a la 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”.

De esta forma sigue argumentando el TC que el derecho a la protección de datos presupone que se requiera el consentimiento previo de la persona afectada para que esos datos personales puedan ser recogidos y tratados, el derecho a ser informado sobre la finalidad del uso de esos datos y además el derecho a acceder, rectificar y cancelar dichos datos. Además establece el contenido del concepto de datos personales:

*“De este modo, el objeto de protección del derecho fundamental a la protección de datos 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, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son 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.”*

En opinión de la autora ARENAS<sup>6</sup> a las redes sociales les sería aplicable la legislación sobre la protección de datos personales ya que de la definición que da el art. 3 LOPD podemos extraer su aplicación teniendo en cuenta que en las redes sociales la mayor parte de la actividad se realiza con los datos personales.

---

2 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE, nº 298, de 14 de diciembre de 1999, págs. 43088 a 43099).

3 La LOPD es la norma transpuesta de la Directiva de la Unión Europea 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995, 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.

4 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE nº 17, de 19 de enero de 2008, págs. 4103 a 4136).

5 STC (Pleno) núm. 292/2000, 30 de noviembre, F. 6º (RTC\2000\292).

6 ARENAS, *Derecho y redes sociales*, p. 120.

### **3.El consentimiento de los menores en las redes sociales**

Cuando una persona crea un perfil en una red social o en la actividad diaria del mismo, se tratan continuamente con los datos personales. El consentimiento del usuario para facilitar sus datos personales tiene un papel esencial dentro de las redes sociales, ya que será lo que le permitirá registrarse y continuar con su uso.

En este ámbito, un colectivo especialmente vulnerable es el de los menores. Por lo que es necesario ver si los menores de 18 años, según la normativa vigente pueden crear un perfil en una red social y sobretodo si son capaces para prestar su consentimiento de forma autónoma, no suponiendo esto un perjuicio en su privacidad o una lesión en sus datos personales.

#### **3.1Definición**

El consentimiento, es un requisito indispensable para el tratamiento de los datos personales en las redes sociales, tanto para mayores de edad como para menores, ya que la información que aparece en las redes sociales es publicada por los propios usuarios, los cuales han prestado su consentimiento para que ello pueda ser compartido de forma pública. Así el consentimiento viene definido en el art. 3.h) LOPD (y en idéntico sentido en el art. 5. 1.d RLOPD) como “toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen”. Además se regula específicamente en el art. 6.1 LOPD y 10.1RLOPD<sup>7</sup>.

En este sentido la Agencia Española de Protección de Datos (AEPD)<sup>8</sup> ha establecido que estos requisitos legalmente determinados se evidencian en la práctica cuando se exige que el usuario introduzca sus datos personales, recabando así su consentimiento.

#### **3. 2 Características**

Por lo que se desprende de las definición establecida es que el consentimiento tiene una serie de características legales y estas son: que se trate de un consentimiento libre, inequívoco, específico e informado. A esto se refiere la AEPD<sup>9</sup>, que ha interpretado el significado que ha de darse a estos conceptos.

Al primer requisito que se hará referencia es cuando el consentimiento se da de forma libre. Esto supone que no se haya ejercido sobre los usuarios cualquier actuación que pueda suponer un vicio del consentimiento para crear un perfil o en el uso del mismo. Por lo que para este caso es aplicable la normativa civil sobre la prestación del consentimiento.<sup>10</sup>

Sobre el consentimiento inequívoco se ha establecido que se dará cuando el usuario realice una acción u omisión que suponga que ha otorgado el consentimiento de forma que no pueda dar lugar a una equivocación. Aunque, este consentimiento inequívoco puede ser tanto expreso como tácito (como ha sido admitido por la AEPD), ya que la normativa existente en la materia no establece como obligatorio que únicamente se pueda dar el consentimiento de forma expresa, por lo que rige la libertad de forma. Y que además en ocasiones se ha previsto expresamente que el consentimiento

## **5**

---

7 En ambas leyes se exige un consentimiento previo e inequívoco del afectado para el tratamiento de los datos personales del afectado, a excepción de que la ley dispusiese otra cosa.

8 Informe jurídico 93/2008, Formas de obtener el consentimiento mediante web. Consentimientos tácitos ([http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes\\_juridicos/consentimiento/common/pdfs/2008-0093\\_Formas-de-obtener-el-consentimiento-mediante-web.-Consentimientos-t-aa-citos.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2008-0093_Formas-de-obtener-el-consentimiento-mediante-web.-Consentimientos-t-aa-citos.pdf)).

9 Informe jurídico 2000\_0000. Caracteres del consentimiento definido por la LOPD ([http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes\\_juridicos/consentimiento/common/pdfs/2000-0000\\_Caracteres-del-consentimiento-definido-por-la-LOPD.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Caracteres-del-consentimiento-definido-por-la-LOPD.pdf)).

10 Será de aplicación la Sección 1ª del Capítulo II del CC, concretamente el art. 1265 que establece la nulidad de del consentimiento por error, violencia, intimidación o dolo.

se haya tenido que dar expresamente (como es el caso de los datos sensibles<sup>11</sup>, el titular tendrá que dar expresamente y por escrito su consentimiento).

Aunque también se expone que para que ese consentimiento tácito pueda considerarse inequívoco es imprescindible que haya un margen de tiempo suficiente para cerciorarse de que la omisión de oponerse al tratamiento implica un consentimiento al mismo.

De esta forma se admite otorgar el consentimiento tanto de formar expresa como tácita, pero en el ámbito de las redes sociales es arriesgado aceptar la forma de consentimiento tácita, ya que muchas veces pueden publicarse fotos en la que aparecen varias personas o hacerse alusión a ellas y no todas haber prestado su consentimiento para ello.

En tercer lugar, en cuanto al consentimiento específico, los responsables del tratamiento de los datos personales de los usuarios en la redes sociales deben de informar sobre la finalidad para que se tratarán los datos personales, ya que los datos irán destinados para ese fin concreto, como así lo determina el art. 4.2 LOPD.

La AEPD ha determinado en este sentido<sup>12</sup> que el consentimiento otorgado por el usuario será nulo cuando desconozca la finalidad a la que destinarán sus datos personales.

Ahora bien en el uso de las redes sociales esto puede quedar difuso porque aunque el usuario configure la privacidad de forma que únicamente comparta sus fotos con sus amigos, estos ya pueden tener acceso a ellas, por lo que el consentimiento que en principio se dio para el tratamiento de los datos con una finalidad específica luego puede quedar impreciso.

Y finalmente, sobre la característica de que se trate de un consentimiento informado, el usuario ha de conocer previamente el tratamiento que tendrán sus datos personales y saber a que se destinarán antes de prestar su consentimiento. Normalmente, la recogida de los datos personales se producirá en el momento en que el usuario se registre, por lo que deberá estar informado ya en ese momento. El art. 5<sup>13</sup> LOPD establece el deber de informar y concretamente sobre que se debe de informar. Esta labor corresponde en el ámbito de las redes sociales a los proveedores o administradores de las mismas (que deberán incluirlo en los enlaces que aparecen denominados como aviso legal o política de privacidad).

No se debe olvidar que una gran parte de los usuarios de las redes sociales son menores de edad, por lo que se ha previsto que además los proveedores han de dar esta información con un lenguaje sencillo y accesible, ya que su grado de madurez para comprender puede ser inferior a la de una persona adulta y por tanto pueden creer que están realmente informados sobre el uso que se dará a sus datos personales y en la realidad no ser así. Además sería conveniente que esta información no fuera demasiado extensa y que fuera obligatoria para continuar con el servicio. Por lo que saber de forma previa la finalidad que tendrán los datos de los usuarios supone una garantía para la privacidad de los mismos.

## 6

---

11 El art 7 LOPD es el relativo a los datos sensibles y estos son ideología, religión, creencias, afiliación sindical, origen racial, salud y vida sexual.

12 Recomendaciones de la AEPD al sector del comercio electrónico, para la adecuación de su funcionamiento a la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, Recomendación 7º ([http://www.agpd.es/portaIwebAGPD/canaIdocumentacion/recomendaciones/common/pdfs/recomendaciones\\_comercio\\_electronico.pdf](http://www.agpd.es/portaIwebAGPD/canaIdocumentacion/recomendaciones/common/pdfs/recomendaciones_comercio_electronico.pdf)).

13 El art. 5.1 LOPD establece que los interesados deberán ser previamente informados de modo expreso, preciso e inequívoco:

- a) *De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
- b) *Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*
- c) *De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
- d) *De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
- e) *De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.*

En este sentido, la AEPD<sup>14</sup> ha determinado en cuanto al consentimiento informado que:

*“La manifestación de los requisitos legalmente exigidos al consentimiento del afectado se realiza en la práctica a través de la información al afectado, en el momento de la recogida de sus datos de carácter personal, de los extremos esenciales relacionados con el tratamiento, recabando a tal efecto su consentimiento en relación con los aspectos específica e inequívocamente hechos constar en la mencionada información.”*

Una vez analizadas estas características, ARENAS<sup>15</sup> expone que aunque no se recoja expresamente en el art. 3. h) LOPD también se debe hacer referencia a que el consentimiento pueda ser revocable<sup>16</sup>.

La revocabilidad supone que el usuario pueda eliminar el consentimiento sobre la información acerca de sus datos personales que ha facilitado en cualquier momento. Esta característica no es fácil que pueda darse en la realidad porque una vez que se ha publicado una información en una red social es complicado que se pueda tener un control real sobre la misma y sobre quien accede a ella. Por lo que la cancelación no siempre puede darse de forma efectiva.

El Dictamen 5/2009<sup>17</sup>, del Grupo de Trabajo del art. 29 (GT 29)<sup>18</sup>, ha entendido que cuando un usuario decide borrar su perfil deberían eliminarse todos los datos personales en el mismo momento en que decida suprimir su cuenta. Así si volviera a reactivar su cuenta esos datos estarían eliminados y tendría que volverlos a introducir.

Del mismo modo, también consideran que si durante un tiempo un usuario mantiene su perfil inactivo se debería primero desactivar su cuenta y posteriormente eliminarla si continúa sin acceder a ella.

### **3.3 El caso específico del consentimiento de los menores para actuar en las redes sociales**

El RLOPD supone un cambio en el tratamiento del consentimiento de los menores de edad. Con anterioridad a este, únicamente se regulaba por las disposiciones establecidas en el Código Civil (CC) por lo que en base al art. 315 CC la edad para poder actuar eran los 18 años.<sup>19</sup>

Concretamente es el art 13 RLOPD el que establece garantías específicas de tratamiento de datos menores de edad que pueden prestar su consentimiento a partir de los 14 años por sí mismos:

*Art. 13. Consentimiento para el tratamiento de datos de menores de edad*

*1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.*

*2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.*

*3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá*

<sup>14</sup> Resolución AEPD, R/00893/2010, F. I.

<sup>15</sup> Arenas, *Derecho y redes sociales*, p. 129.

<sup>16</sup> Arts 6.3 y 11.4 LOPD y art. 17 RLOPD.

<sup>17</sup> Dictamen 5/2009, sobre redes sociales en línea, adoptado el 12 de Junio de 2009 ([http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163\\_es.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf)).

<sup>18</sup> El GT 29 fue creado por el art. 29 de la Directiva 95/46/CE y está integrado por las autoridades de protección de datos de los estados miembro de la UE, el Supervisor Europeo de Protección de Datos y la Comisión Europea.

<sup>19</sup> Los arts. 162 y 163 CC, tratan la representación legal para el caso de menores e incapacitados.

*expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación delo dispuesto en este artículo.*

*4. 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.*

Este artículo es aplicable en el supuesto en que los menores quieran crear un perfil en una red social, así que lo que primeramente se puede extraer es que la edad para otorgar el consentimiento de los menores ha cambiado, porque si antes eran dieciocho años, ahora los mayores de catorce años podrán prestar dicho consentimiento por ellos mismos, sin la asistencia de sus progenitores o tutores (exceptuando los casos en que la Ley expresamente prevea la intervención de éstos). Ahora bien, en el caso de los menores de catorce años siempre necesitarán el consentimiento paterno para poder operar en las redes sociales.

La Audiencia Nacional (AN)<sup>20</sup> resuelve un contencioso sobre el registro en 2006 en una web de un menor de 11 años de edad, el cual tuvo que rellenar un formulario y no completó la información correspondiente a la fecha de nacimiento. La web lo identificó como un mayor de edad y además cedió estos datos del menor para la realización de una campaña publicitaria a otra empresa.

Al suceder los hechos en 2006, no puede ser aplicable el art. 13 del RLOPD, por lo que la AN decide del siguiente modo:

“En el presente caso no concurre el consentimiento exigible pues la recogida y el tratamiento de los datos correspondían a un menor de edad sin que se hubiese recabado el consentimiento de los que ostentaba su patria potestad o tutela. El menor, cuando ocurrieron los hechos, tenía 11 años por lo que, aunque en tal fecha no había entrado en vigor, tampoco podría haber consentido en aplicación de lo previsto en el artículo 13 del Reglamento de la LOPD aprobado por R.D. 1720/2007 según el cual sólo los mayores de 14 años pueden consentir para el tratamiento de sus datos personales. La capacidad de obrar de los menores, como idoneidad para realizar eficazmente actos jurídicos, es decir, para ejercitar derechos o asumir obligaciones, se encuentra limitada y requiere que sus representantes legales ejerciten sus derechos y asuman sus obligaciones, supliendo la limitación de tal capacidad de obrar, situación que no se ha producido en el presente caso.

*[...]La concurrencia del consentimiento inequívoco del afectado, que exige el artículo 6.1 de la LOPD, para el tratamiento de datos de carácter personal, en el caso de que la afectado niega haberlo otorgado, incumbe a quien realiza el tratamiento a través de los medios previstos legalmente a tal fin. En el presente caso existe un hecho indiscutible y es la minoría de edad del titular de los datos tratados por la recurrente y la inexistencia del consentimiento de los progenitores del menor. Frente a tales hechos, la parte recurrente no ha acreditado la concurrencia de tal consentimiento sin que pueda valorarse, a este fin, el horario en que se produce la inserción de datos ni la hora en que el hijo deja el ordenador ni si el mismo es utilizado por otros miembros de la familia pues ninguno de estos aspectos son determinantes de la existencia de consentimiento que la recurrente debió controlar que se había producido de forma inequívoca pues siendo ella la que trata los datos es a ella a quien incumbe la obligación impuesta en el artículo 6.1 de la LOPD”.*

En este aspecto, la AEPD<sup>21</sup> se ha pronunciado y ha determinado que los mayores de catorce años pueden prestar el consentimiento por ellos mismos ya que el artículo 162.1º del Código Civil exceptúa de la representación legal del titular de la patria potestad a “los actos referidos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo”. Además en otros preceptos del CC también se reconoce la capacidad y madurez suficiente para que los menores de edad puedan realizar ciertos actos jurídicamente independientes por sí solos.

## 8

20 SAN (Sala de lo Contencioso – Administrativo, Sección 1ª) 26 de Noviembre de 2009, F. 4º (JUR\2009\496350)

21 Informe jurídico 2000\_0000. Consentimiento otorgado por menores de edad

([http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes\\_juridicos/consentimiento/common/pdfs/2000-0000\\_Consentimiento-otorgado-por-menores-de-edad.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Consentimiento-otorgado-por-menores-de-edad.pdf))

Y concretamente, en el artículo 4.3<sup>22</sup> de la Ley Orgánica 1/1996.<sup>23</sup>

Así habrá que atender a las condiciones de madurez del menor en cada caso concreto para determinar si puede prestar el consentimiento por sí mismo o no para el tratamiento automatizado de sus datos personales.

También en este informe, la AEPD trata el supuesto del consentimiento de los menores de catorce años, estableciendo que es necesario tener en cuenta las condiciones de madurez del menor (en base al art. 162. 1º CC) y cuando éstas no garanticen la plena comprensión por los mismos del consentimiento prestado, tendrán que otorgar el consentimiento sus padres o tutores.

Al tratarse de menores de edad será esencial que los administradores de las redes sociales informen de todos los aspectos recogidos en el art. 5 LOPD en un lenguaje sencillo y comprensible.

Sobre este aspecto se ha pronunciado la AEPD<sup>24</sup> referente a la grabación por parte de un sujeto mayor de edad a unos niños de siete y ocho años que se encontraban de excursión en el Zoo de la Casa de Campo de Madrid con su colegio. Posteriormente este mismo sujeto publicó el video en un canal privado de Youtube que enlaza con la red social Facebook. Aquí se expuso que era necesario el consentimiento de los padres de estos menores de edad para que pudiesen tanto ser grabados como posteriormente publicar en dicha red social el video.

La AEPD en este informe, recuerda que ha emitido una serie de recomendaciones sobre el uso de Internet por parte de los menores en las que se aconseja no publicar fotos que identifiquen a un niño, aunque sí se podrán colgar fotos o vídeos de menores mientras no permitan la identificación de éstos, ya sea porque se hayan realizado las fotos de forma lejana, lo que dificultaría reconocer al menor, o porque se utilicen técnicas de distorsión u ocultamiento del rostro.

Además aquí se expone un principio jurídico esencial que hay que tener en cuenta para aplicar la normativa de protección de datos a menores, es el interés superior del niño. A nivel internacional viene expuesto en diversas normas como el art. 3 de la Convención de Naciones Unidas sobre los Derechos del Niño<sup>25</sup>, y en el ámbito nacional en el art. 2<sup>26</sup> de la LOPJM.

Así, es posible que en base a este principio aunque se haya dado el consentimiento y este sea válido no puedan llegarse a publicar los datos o imágenes referentes al menor:

*“Por consiguiente, el interés superior del menor debe prevalecer, de manera que el derecho a la protección de datos puede tener que ceder ante dicho principio en el caso de que existan intereses en conflicto. De esta forma, incluso en el caso de que el menor mayor de 14 años haya prestado su consentimiento para el tratamiento de su imagen si dicho tratamiento lesiona su derecho a la intimidad, honor y propia imagen, en aplicación del citado principio, entrará en juego la protección otorgada por la Leyes Orgánicas 1/1982 y 1/1998 frente a aquellas intromisiones que supongan una vulneración de dichos derechos.”*

## 9

22 El art. 4.3 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”.

23 Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil (BOE, nº 15, de 17 de enero de 1996, páginas 1225 a 1238).

24 Informe jurídico 2013\_0197. Red social deportiva. Publicación de vídeos de menores ([http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes\\_juridicos/common/pdf\\_destacados/2013-0197\\_Red-social-deportiva.-Publicaci-oo-n-de-v-ii-deos-de-menores..pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdf_destacados/2013-0197_Red-social-deportiva.-Publicaci-oo-n-de-v-ii-deos-de-menores..pdf)).

25 Instrumento de Ratificación de la Convención sobre los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989 (BOE, nº 313, de 31 de diciembre de 1990, páginas 38897 a 38904).

26 El art. 2 expone que “primará el interés superior de los menores sobre cualquier otro interés legítimo que pudiera concurrir.”

Este mismo caso fue tratado por la Sala Tercera de la Audiencia Nacional<sup>27</sup> y se pronunció del mismo modo que la AEPD:

*“Y en el presente caso la divulgación por medio de video de la imagen de los menores, constituye un tratamiento de sus datos de carácter personal, que al ser menores de 14 años de edad, pues contaban entre 7 y 8 años de edad, requiere para poder efectuarlo el consentimiento de sus padres o tutores, como exige el artículo 13.1 del RLOPD en relación con el artículo 6 LOPD que regula el principio del consentimiento para el tratamiento de los datos de carácter personal del afectado. Por tanto, las alegaciones referentes a si los menores no se encontraban acompañados por sus profesoras en el concreto momento en que se grababa el video, resultan irrelevantes a los efectos del presente procedimiento, pues los menores por su edad no podían consentir ni la grabación ni la difusión de su imagen y el citado artículo 6.1 de la LOPD dispone, con carácter general, que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.”*

En el segundo apartado del art. 13 se prohíbe el recabo de datos a menores sobre su grupo familiar a excepción de recabarlos para este mismo fin. Y como ya se ha hecho hincapié con anterioridad, y dada la importancia que tiene, la información que se emita a los menores para solicitar sus datos ha de estar dada de forma sencilla y comprensible, el art. 13 en su apartado tercero lo incluye.

Para finalizar, el apartado cuarto de este artículo impone a los responsables de los ficheros la articulación de medios que garanticen que se compruebe la edad y la veracidad del consentimiento prestado por el menor.

#### **4. Medidas de protección de los menores adoptadas por las redes sociales**

En 2009, en un estudio elaborado sobre la utilización de la web 2.0 por parte de los menores<sup>28</sup> determinaba que un 74,9% de los menores encuestados entre la edad de 11 y 17 años tenía un perfil creado en una red social. La red social preferida por los menores era Tuenti (hoy día también convertida en una operadora de teléfono móvil), ya que un 64,3% estaba dado de alta como usuario en esta red social.

Ante estos elevados datos, para la comprobación de la edad de forma efectiva era necesario, por una parte que los padres o tutores tomasen conciencia, de forma que estableciesen programas o filtros en sus ordenadores que permitiesen un control del acceso de sus hijos menores a las redes sociales. Por otra parte, que se formalizase un procedimiento más exhaustivo por parte de los proveedores o administradores de las redes sociales a la hora de que los menores se registrasen en sus servicios, de forma que no solo la marcación de una casilla supusiera que la utilización de las redes la está realizando una persona mayor de edad.

En este último punto, diversas redes sociales como Tuenti o Facebook, de acuerdo con la AEPD<sup>29</sup>, se comprometieron a ofrecer un servicio más riguroso sobre la confirmación de la edad de los menores. Así Facebook aumentó a 14 años la edad mínima para darse de alta en la red social y Tuenti estableció un procedimiento de verificación de la edad en el que da de baja a usuarios menores de 14 años de su red, y de esta forma se adaptan a la legislación española, tomando en consideración el art. 13 RLOPD.

##### **4.1 El proceso de verificación de la edad establecido en Tuenti**

En 2009, se exigía que la edad mínima para registrarse en la red social Tuenti fuese catorce años.

27 SAN (Sala de lo Contencioso – Administrativo, Sección 1ª) 2 de Enero de 2013, F. 4º (RJCA\2013\100).

28 <http://www.seguridadweb20.es/estudio.php>.

29 Memoria AEPD 2010, p. 28

([http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria\\_2010/common/AEPD\\_Memoria\\_2010.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2010/common/AEPD_Memoria_2010.pdf)).

Por lo que todos aquellos usuarios que fueran menores de esa edad y que la red social estuviese en disposición de confirmarlo serían eliminados de la misma.

Para ello MARTOS<sup>30</sup> exponía que se implantó un protocolo de detección de perfiles de menores de 14 años. Los perfiles de usuarios que decían tener entre 14 y 18 años eran examinados tanto en el momento del registro como posteriormente mediante el sistema de reporte de otros usuarios. Se les comunicaba mediante correo electrónico que debían mandar una fotocopia del DNI o NIE (si eran extranjeros), ya fuera escaneada o por fax en un plazo no inferior a 96 horas. Si finalizaba el plazo y no se recibía la fotocopia el perfil era borrado de la red social. Esto viene explicado en las condiciones de privacidad y términos legales de Tuenti en el que se advierte de que te pueden pedir una fotocopia del DNI para acreditar la edad y sino se lleva a cabo dentro del plazo establecido podrían bloquear o cancelar el perfil.

Después de unos meses de funcionamiento, casi el 100% de los perfiles a los que se les exigía el DNI eran eliminados por no aportar la fotocopia.

PARRA<sup>31</sup>, se hacía eco de este cambio que supuso para la red social este proceso de limitación de acceso a los menores de catorce años pero en su opinión era desproporcionado, ya que el art. 8.5 RLOPD<sup>32</sup> establece que los datos personales que facilitan los usuarios han de ser exactos y por tanto veraces y, en caso contrario tendrán que ser rectificadas o canceladas. Por lo que la norma ya ofrece garantías suficientes para garantizar la edad de los menores y exigir una fotocopia del DNI resulta excesivo.

En mi opinión, encuentro acertado el proceso de verificación de la edad que incorporó Tuenti ya que es cierto que la norma establece la exactitud de los datos personales facilitados por los usuarios, pero como demuestran los datos del estudio, esto no es suficiente ya que hay una gran cantidad de menores de catorce años que se registran en redes sociales y este es un buen método para que se pueda comprobar de forma efectiva la edad real del menor.

#### **4.2 Otras medidas posteriores**

Ya en 2012, la AEPD<sup>33</sup> quiso dar un paso más con la finalidad de fijar procedimientos que sirvieran para verificar la edad y que los menores que accedieran a las redes sociales tuvieran la edad mínima exigida por el RLOPD para poder proceder a prestar el consentimiento en el tratamiento de sus

### **11**

---

30 Martos, *Derecho y redes sociales*, p. 160.

31 <http://www.samuelparra.com/2009/06/18/tuenti-pedir-dni-mantener-cuenta/>

32 El art. 8. 5 RLOPD establece “*Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.*

*Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.*

*Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.*

*En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.*

*Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.*

*Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento.”*

33 Memoria AEPD 2012, p. 44

([http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/memorias/memoria2012/MEMORIA\\_2012\\_web.PDF](http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/memorias/memoria2012/MEMORIA_2012_web.PDF)).

datos personales de forma segura. Con esta finalidad, se pensó incorporar el DNI electrónico del certificado de autenticación suponiendo una solución para acreditar la edad para los menores que se quieran registrar en la red social.

En 2013, Tuenti<sup>34</sup> adoptó esta medida por lo que los usuarios que se encontrasen en el proceso de verificación de edad podrían realizarlo mediante el DNI electrónico.

Por otra parte, en el ámbito europeo, la Comisión Europea aprobó en 2012 una propuesta de Reglamento<sup>35</sup> concerniente a la protección datos personales.

Esta propuesta contiene unas mayores garantías en el tratamiento de los datos personales de los menores, así como en su privacidad. En él, se considera niño a todo sujeto menor de dieciocho años (art. 4. 18), ahora bien para prestar el consentimiento en el tratamiento de los datos personales, el art. 8 contiene una regulación específica y se exige únicamente el consentimiento o autorización del padre o tutor en el caso de que se trate de un menor de trece años, así como en la normativa española, se permite que los mayores de catorce años puedan otorgar el consentimiento por ellos mismos y por tanto pueden acceder a darse de alta en redes sociales.

Además la información ha de venir expresada en un lenguaje claro y sencillo para los menores (art. 11) y el especial reconocimiento en el art. 17 del derecho al olvido y a la supresión de los datos proporcionados siendo niño (como se tratará más adelante).

En conclusión, la propuesta del Reglamento supone una mayor garantía a la privacidad de los menores en el ámbito de las redes sociales pero todavía no ha entrado en vigor. Por el momento las únicas garantías reales que ofrece la normativa existente para la protección de datos personales de los menores en las redes sociales es el establecimiento de una información previa expresada de forma sencilla y comprensible para que los menores puedan entenderlo de la forma más adecuada posible, ya que esto supondrá una mayor seguridad a la hora de que los menores faciliten sus datos. Y además que los proveedores o administradores de las redes sociales han de realizar los procedimientos necesarios 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<sup>36</sup>.

## **5.La responsabilidad civil de los progenitores o tutores derivada de la actividad de los menores en las redes sociales**

La normativa en materia de protección de datos excluye de su ámbito de aplicación aquellos tratamientos que realicen las personas “en el ejercicio de actividades exclusivamente personales o domésticas”. Por lo que en principio, los usuarios de las redes social quedarían al margen. Pero el Dictamen 5/2009<sup>37</sup> ha establecido que hay ocasiones en que se excede de la actividad doméstica y se puede considerar responsable a los usuarios (incluidos los menores de edad) por lo que publican en las redes sociales. Estas causas de responsabilidad son: el uso de las redes sociales con fines comerciales, políticos o sociales; cuando el usuario tenga un gran número de contactos, y por tanto puedan acceder a sus datos personales y conocerlos un elevado número de personas; y por último y es aquí donde principalmente podrán ser responsables los menores, cuando se vulneren derechos de terceros por el tratamiento de los

---

34 <http://corporate.tuenti.com/es/blog/los-usuarios-ya-pueden-verificar-su-edad-a-travs-del-dni-electrnico>.

35 Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos, aprobada el 25 de enero de 2012, por la Comisión Europea (<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF>).

36 Art. 13. 3 y 4 RLOPD.

37 Dictamen 5/2009, sobre redes sociales en línea, adoptado el 12 de Junio de 2009 ([http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163\\_es.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf)).

datos personales que puedan hacer los usuarios.

De esta forma se les exige tener un deber de diligencia cuando operan en las redes sociales, ya que si causan un daño a un tercero puede tener consecuencias en el ámbito civil o penal.

Cuando el usuario es menor y realiza una conducta lesiva, tanto la normativa civil como penal plantean la responsabilidad civil de los padres por lo que sus hijos han publicado en las redes sociales.

### **5.1. En el ámbito civil**

Desde la perspectiva civil, los padres son responsables en virtud del art. 1903CC por responsabilidad por hecho ajeno por culpa “in vigilando” en cuanto se produce una omisión del deber de vigilancia.

La regla general es que el sujeto responda por actos u omisiones propios pero también puede haber responsabilidad por hecho ajeno cuando los daños son causado por aquellas personas de cuyo comportamiento responde el obligado a controlarlas, ya que no se han adoptado las medidas necesarias para que no se cause el daño.

Se trata de una responsabilidad directa, y por tanto no subsidiaria donde el demandante puede dirigirse directamente contra el responsable, sin necesidad de demandar al causante del daño.

Es una presunción iuris tantum de culpa, de manera que, el llamado a responder solo quedará exonerado si demuestra que empleó toda la diligencia de buen padre de familia que le era exigible, como impone el art. 1903 CC<sup>38</sup>.

Por lo que si un menor vulnera los datos personales de otra persona (menor o no), los progenitores o tutores podrán tener que indemnizar a la víctima del daño por omisión del deber de vigilancia en el uso de las redes sociales.

Así, la Audiencia Provincial (AP) de Asturias<sup>39</sup> condenó a pagar una indemnización por daños morales y patrimoniales a la madre de una menor de doce años que profirió amenazas a otra menor a través de la red social Metroflog<sup>40</sup>, al darse los requisitos que establece el art. 1903 CC. La AP considera que hay responsabilidad por culpa de los padres por omisión del deber de vigilancia, y estos no pueden excusarse en que la conducta indebida del menor fue cometida “por su escasa edad y falta de madurez”.

## **13**

---

38El art. 1903 CC recoge “La obligación que impone el artículo anterior es exigible, no sólo por los actos u omisiones propios, sino por los de aquellas personas de quienes se debe responder.

*Los padres son responsables de los daños causados por los hijos que se encuentren bajo su guarda.*

*Los tutores lo son de los perjuicios causados por los menores o incapacitados que están bajo su autoridad y habitan en su compañía.*

*Lo son igualmente los dueños o directores de un establecimiento o empresa respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones.*

*Las personas o entidades que sean titulares de un Centro docente de enseñanza no superior responderán por los daños y perjuicios que causen sus alumnos menores de edad durante los períodos de tiempo en que los mismos se hallen bajo el control o vigilancia del profesorado del Centro, desarrollando actividades escolares o extraescolares y complementarias.*

*La responsabilidad de que trata este artículo cesará cuando las personas en él mencionadas prueben que emplearon toda la diligencia de un buen padre de familia para prevenir el daño.”*

39 SAP Asturias (Sección 5ª), Sentencia núm 217/2013, de 22 de Julio (AC\2013\1559).

40 Metroflog fue un blog creado para colgar fotografías de los usuarios, pero después ha sido convertido a red social donde es posible crear listas con los gustos y aficiones de los registrados, elegir una foto de perfil o dejar comentarios en el espacio diseñado para ello.

En este sentido, citando el pronunciamiento del Tribunal Supremo (TS) en una de sus sentencias<sup>41</sup>, declaró que:

"Dada la complejidad de la vida moderna y su consiguiente aumento de riesgo, es patente la tendencia a hacer responder de los daños derivados de esos riesgos a quienes los crean, y en este sentido el padre o cuidador de un menor responde de los daños que éste cause a terceros, pues con su falta de cuidado creó el riesgo de una conducta nociva del menor traducida en daño efectivo y real y debe, por ello, resarcirlo, a menos que pruebe haber utilizado la diligencia exigida por la Ley, lo que no ocurrió en el caso debatido."

En el caso de que los padres no tengan ningún conocimiento sobre el uso de Internet, y concretamente sobre las redes sociales, ¿pueden ser responsables al desconocer como evitar el daño que puedan causar sus hijos menores?

Esto fue alegado como motivo (por vulneración del último apartado del art. 1903 CC) en un recurso de apelación, por una progenitora que afirmaba carecer de conocimientos informáticos, y en primera instancia era condenada como responsable civil por las manifestaciones realizadas por su hijo menor en la red social Tuenti contra un profesor de su instituto, vulnerando así su honor.

En este sentido, la AP de Madrid<sup>42</sup> no entró a pronunciarse sobre el fondo de la cuestión, ya que lo alegó por primera vez en segunda instancia, cuando tendría que haberlo realizado en la contestación a la demanda o en la audiencia previa.

En mi opinión, este motivo no tendría que ser acogido por los tribunales como exoneración de la responsabilidad de los padres por las actuaciones de sus hijos en las redes sociales. Aunque el medio utilizado para realizar la conducta indebida sea desconocida por los progenitores, si son conocedores de que en cualquier ámbito hay expresiones u opiniones que pueden atentar contra los derechos de las personas, como puede ser el honor o la intimidad e incluso si ya tienen una gran intensidad podrían llegar a considerarse constitutivas de delito (amenazas, vejaciones, cyberbullying, entre otros) castigado por la vía penal pero que puede tener repercusión en el ámbito civil, y en tal caso no habrían empleado toda la diligencia de un buen padre de familia para prevenir el daño. Así, el art. 1903 CC hace referencia a una responsabilidad en general que deben de tener los progenitores por los hechos dañosos que cometan sus hijos menores, con independencia de que este daño se haya cometido a través de una red social.

De esta forma, si se reconociera tal exoneración muchas de estas conductas que pueden ser condenadas mediante esta responsabilidad civil, quedarían sin castigar ya que aún hay muchos progenitores que no son usuarios de las redes sociales (y por tanto desconocen su funcionamiento) o directamente no utilizan Internet. Cuando es posible que sus hijos menores sí fueran conscientes de que haciendo cierto tipo de manifestaciones (ya pueden ser escritas o mediante la exhibición de fotografías), están realizando un daño a otra persona (aunque no sepan que eso puede constituir un ilícito civil que puedan causar daños morales o patrimoniales).

## **5.2 En el ámbito penal**

Cuando el hecho dañoso realizado por el menor sea constitutivo de delito (como puede ser ciberacoso), se regirá por la Ley Orgánica 5/2000<sup>43</sup> (LORPM). El art. 61. 3<sup>44</sup> de esta ley establece la

### **14**

41 STS 4 de mayo de 1984 (RJ\ 1984\2396).

42 SAP Madrid (Sección 11ª) Sentencia núm 256/2013, de 17 de mayo (JUR\2013\222432).

43 Ley Orgánica 5/2000, de 12 de enero, modificada por la Ley Orgánica 8/2006, de 4 de diciembre, reguladora de la responsabilidad penal de los menores (BOE, nº 11, de 13/01/2000).

44 El art 61. 3 establece que *"cuando el responsable de los hechos cometidos sea un menor de 18 años, responderán solidariamente con él de los daños y perjuicios causados sus padres, tutores, acogedores y guardadores legales o de hecho, por este orden. Cuando éstos no hubieren favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada por el juez según los casos"*

responsabilidad de los padres de forma objetiva y solidaria con los menores imputables mayores de 14 años y menores de 18 (art. 1) por una omisión del deber de vigilancia.

Así los padres tendrán que indemnizar por el hecho dañoso que haya cometido su hijo y únicamente si no hubiesen favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada, que no eliminada. La moderación se llevará a cabo si se prueba que tuvieron la diligencia exigida en su deber de vigilancia de sus hijos menores por lo que publicaron en las redes sociales.

La AP de Valencia <sup>45</sup> se pronunció en 2010 no moderando la responsabilidad civil de los padres de un menor, que mantenía contacto a través de Messenger con otra menor, y mientras que por webcam le enseñaba los pechos, el chico lo grabó en video y lo difundió a otros compañeros del instituto. Esto provocó burlas y un daño moral en la menor. El menor acusado fue condenado por un delito contra la integridad moral y a una indemnización por responsabilidad civil, conjuntamente con sus padres, de 2700€ por el daño moral provocado.

No hay moderación de la responsabilidad civil porque la AP de Valencia considerará que hubo una omisión del deber de vigilancia por parte de los padres no controlaron el uso que hacía su hijo menor de este servicio que ellos mismos le proporcionaron, con los riesgos que puede generar si se utiliza de forma indebida. Por lo que no actuaron con la diligencia que les era exigible.

Además como ya se ha expuesto, recalca que la esencia de esta responsabilidad civil es la omisión del deber de vigilancia, pero concretamente supone:

*“[...]la trasgresión del deber de vigilancia que a los padres y asimilados incumbe, en el desempeño de la patria potestad, y que comprende también los deberes de educación y formación integral del menor, en la tolerancia y respeto de los derechos individuales y propiedad de los demás, estimándose inadecuadas tanto las conductas de dejadez en la educación, como las actitudes de protección y de justificación a ultranza de la conducta del menor.”*

Y añade que la finalidad es doble:

*“En primer lugar amparar mejor los derechos de las víctimas al liberarles de tener que probar la culpa del responsable civil, protegiéndola también frente a la frecuente insolvencia del menor infractor, asegurándoles así la indemnización de los daños sufridos por tales víctimas; y en segundo lugar, conseguir una mayor implicación de los padres y demás responsables en el proceso de socialización de los menores, imponiéndoles las consecuencias civiles de las infracciones que éstos cometan por la trasgresión del conjunto de deberes que tienen sobre ellos.”*

Por contra, la AP de Valladolid<sup>46</sup> consideró que sí había una moderación de la responsabilidad civil en un caso de suplantación de identidad de una menor, en su perfil en la red social Tuenti, por parte de otra menor, en la que insultaba a sus compañeros de instituto. A consecuencia de esto, la menor suplantada sufrió un daño psicológico. La acusada fue condenada a un delito de descubrimiento y revelación de secretos en primera instancia, y en apelación se alegaba responsabilidad civil.

La AP estimó que en parte las pretensiones de la víctima, y condenó a la menor y a sus progenitores a una responsabilidad civil solidaria si bien si hubo una moderación de la cuantía ya que si hubo una omisión del deber de vigilancia, pero no se pudo probar que los padres hubiesen obrado con dolo o negligencia grave en la conducta de la menor.

Si fuesen menores de 14 años resultan inimputables y por tanto, el demandante deberá acudir a la jurisdicción civil en base al art. 1903 CC (art. 3 LORPM). De este modo los padres sí podrán eximirse de responsabilidad (probando que no hubo una omisión del deber de vigilancia), aunque sus hijos hubiesen cometido un ilícito civil.

45 SAP Valencia (Sección 5ª), Sentencia núm 22/2010, de 14 de enero (JUR\2010\211507).

46 SAP Valladolid (Sección 2ª), Sentencia núm. 58/2011, de 9 de Marzo (JUR\2011\168918).

Por lo que como se puede observar hay una gran diferencia entre que los padres respondan en el ámbito civil o en el ámbito penal ya que en el CC esta responsabilidad se plantea por el hecho ajeno y pueden exonerarse si prueban que actuar con la debida diligencia para prevenir el daño. Mientras que en el ámbito penal se produce como plantea MOURE<sup>47</sup> casi una objetivación de la responsabilidad por parte de la jurisprudencia y sólo se permitirá la moderación de la responsabilidad.

## **6. Breve referencia a las intromisiones ilegítimas del derecho al honor, intimidad y propia imagen de los menores en las redes sociales**

En el ámbito de las redes sociales es muy común que los daños que puedan realizarse contra los usuarios afecten a su honor, intimidad personal y a su propia imagen. Estos derechos aparecen recogidos en el apartado primero del art. 18<sup>48</sup> de la Constitución Española (CE)<sup>49</sup>, mientras que el apartado cuarto de este mismo artículo establece que la ley limitará el uso de la informática para garantizar estos derechos. De esta forma, la protección civil de estos derechos viene establecida en la Ley Orgánica 1/1982<sup>50</sup>, recogido tanto para los mayores como para los menores de edad. El primer artículo determina que estos derechos que la ley expone son irrenunciables, inalienables e imprescriptibles, y se protegen contra intromisiones ilegítimas.

No tendrá consideración de intromisión ilegítima cuando el interesado otorgue su consentimiento para ese fin, aunque siempre es revocable y en todo caso se indemnizará por los daños y perjuicios ocasionados (art. 2). En el caso de los menores de edad, se permite que este consentimiento puedan otorgarlo por ellos mismos si sus condiciones de madurez lo permitieran de acuerdo con la legislación civil<sup>51</sup>, y en los restantes casos lo tendrán que otorgar sus representantes legales previa comunicación al Ministerio Fiscal (art. 3).

Se consideran intromisiones ilegítimas del derecho al honor, la intimidad y la propia imagen que puedan darse a través de las redes sociales la divulgación de fotografías, opiniones, imágenes, informaciones, fotomontajes, grabaciones de sonido o de imagen que puedan provocar un desprestigio del menor en consideración con su entorno, atentando contra su dignidad como persona (art. 7. 3, 5 y 7).

En la actualidad, ante el uso en masa de las redes sociales por parte de menores, es frecuente que ellos mismos renuncien a su derecho a la intimidad, propia imagen, o incluso al honor proporcionando datos y difundiendo imágenes propias y puede que ajenas (en este caso sin el consentimiento de los menores afectados o de sus representantes legales).

Esto provoca una serie de riesgos ya que sus condiciones de madurez no son las mismas que las de un mayor de edad y por tanto pueden no ser conscientes de que esas publicaciones pueden tener repercusiones negativas para ellos mismos y para terceros, ya que en el caso de intromisiones ilegítimas en el derecho al honor, intimidad y propia imagen de terceros si causasen daños podrían ser responsables civil o penalmente y en este caso también lo serían los progenitores responsables en base al art. 1903 CC y al 61. 3 LORPM, respectivamente (conforme a lo explicado anteriormente).

## **16**

---

47 Moure, *Revista de asociación española de abogados especializados en responsabilidad civil y seguros*, p. 16

48 Art. 18.1 CE: “*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*”.

49 Constitución Española, 1978 (BOE, nº 311, de 29/12/1978).

50 Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE, nº. 115, de 14 de mayo de 1982, páginas 12546 a 12548).

51 Arts. 154. 3 y 162. 1 CC.

Heras<sup>52</sup> sostiene que para contrarrestar las consecuencias negativas (y ante la ausencia legal) de que los menores puedan otorgar el consentimiento, podría aplicarse el art. 4.3 LOPJM el cual establece que la utilización de la imagen o el nombre del menor en los medios de comunicación que fuera en contra de sus propios intereses, sería una intromisión ilegítima en su derecho al honor, la intimidad y la propia imagen, aún cuando el menor hubiera prestado su consentimiento.

De esta forma habría una mayor protección de los menores en cuanto a lo que publicasen en las redes sociales y pudiera ser lesivo para su dignidad.

## **7.El derecho al olvido de los menores en las redes sociales**

Se puede definir el derecho al olvido en el ámbito de Internet como un derecho de los usuarios (y por tanto, incluidos los menores) para que puedan eliminar información concerniente a ellos publicada a través de este medio, así como la obligación de no darles más difusión, después de un período de tiempo determinado.

Darse de baja en una red social entraña una serie de dificultades porque no por el mero hecho de eliminar la cuenta, desaparecen los datos personales que los usuarios han compartido en la red, lo que supone que puede seguir circulando esta información sin su consentimiento. Por ello, se busca que de forma efectiva pueda darse el derecho al olvido de los datos personales proporcionados, en el momento de cancelación de la cuenta.

En este caso, se trata de ver si la regulación existe ampara el derecho al olvido de los menores cuando deciden cancelar el perfil que han creado en la red social.

### **7.1 Regulación actual del derecho al olvido de los menores**

En la actualidad ni al normativa europea, ni la española recogen explícitamente este derecho. Únicamente la LOPD tan solo regula los denominados derechos ARCO, es decir acceso, rectificación, cancelación y oposición<sup>53</sup> a los datos personales cedidos, y aunque los menores

## **17**

---

52 HERAS, *Revista IUS*, p. 8.

53Art. 15 derecho de acceso:

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.
2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
- 3.El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

### Art. 16 derecho de rectificación y cancelación

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.
- 2.Serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.
3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.
- 4.Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.
- 5.Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

puedan hacer uso de ellos, no son suficientes para dar una solución efectiva, ya que no se crearon para subsanar los problemas derivados del uso de las redes sociales (ni de Internet en general), y por tanto no regulan de forma completa esta problemática.

Sobre este aspecto no hay pronunciamientos judiciales, pero la AEPD dictó una resolución<sup>54</sup> en la que se visualiza esta insuficiencia normativa cuando una persona quiere desaparecer de una red social. Así, una usuaria de Facebook reclamaba a la sucursal de Facebook en España, la cancelación de sus datos personales correspondientes a su dirección de correo electrónico, cuando era utilizado por otra persona para dar de alta a la interesada en dicha red social. La AEPD determinó que Facebook no es responsable de los datos personales que los usuarios publiquen, pero sí es responsable del fichero donde se guardan dichos datos, como además de realizar las gestiones necesarias para retirar o impedir el acceso a los mismos cuando la AEPD o la persona interesada mediante sus derechos de acceso, rectificación, cancelación y oposición, así lo soliciten.

Además la AEPD añade que los usuarios de las redes sociales:

“[...]deben gozar de mecanismos reactivos amparados en Derecho (como el derecho de cancelación de datos de carácter personal) que impidan el mantenimiento secular y universal en la Red de su información de carácter personal”.

Pero, pese a este reconocimiento, consideró que la interesada tenía que ejercitar su derecho a cancelación (especificando siempre que desease que fuera cancelado) ante Facebook cuando tuviese constancia que es utilizado por otra persona para darle de alta en dicha red social (no pudiendo haber un derecho de cancelación con expectativas futuras para cancelar la cuenta automáticamente).

En la propuesta del Reglamento europeo de protección de datos, concretamente en el art. 17. 1, aparece regulado el derecho al olvido de los menores. Así, los responsables o proveedores de las redes sociales deberán suprimir los datos personales cedidos por los menores y abstenerse de darles más difusión cuando el menor lo solicite. Se recogen una serie de supuestos tasados en los que el menor podrá solicitarlo cuando los datos ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados; si el menor revocara el consentimiento en que se basa el tratamiento, o ha finalizado el plazo de conservación autorizado; si hay oposición al tratamiento de datos personales; y finalmente, cuando por cualquier otro motivo el tratamiento de los datos no sea conforme con la propuesta del reglamento.

Además el apartado segundo establece que el proveedor de la red social si hubiese cedido a terceros esos datos tendrá que adoptar las medidas organizativas o técnicas necesarias, para informar a terceros sobre la solicitud que le interesado ha realizado para que se supriman sus datos.

Aunque este derecho al olvido no se tratará de un derecho absoluto, ya que cederá en el caso de ejercicio del derecho a la libertad de expresión; por motivos de interés público en el ámbito de la salud pública; con fines de investigación histórica, estadística y científica; y finalmente para dar cumplimiento de una obligación legal de conservación de los datos personales.

De aprobarse el Reglamento, el derecho al olvido supondría una garantía a la privacidad de los usuarios de las redes sociales menores de edad, ya que se otorgaría un control adicional sobre sus propios datos, reforzando el derecho de cancelación de sus datos en las red.

## **8.Recomendaciones de la AEPD para proteger a los menores en el uso de las redes sociales**

Visto los riesgos que pueden desentrañar la actuación de los menores en una red social, la AEPD consciente de esta problemática ha desarrollado una guía<sup>55</sup> de recomendaciones, tanto para los padres como para los menores, con la finalidad de mejorar el uso y sobretodo de proteger a los menores de los riesgos existentes.

El primer consejo da la AEPD dirigido a los menores es que no se divulguen más datos personales de los estrictamente necesarios, y sobretodo no dárselos a usuarios que sean desconocidos para el menor. En este caso lo adecuado será que se le comunique este hecho a los padres. A este respecto, se recomienda que los menores utilicen pseudónimos para interactuar en las redes sociales.

En este sentido también hay que incluir la no comunicación (tanto a extraños como a conocidos) de las contraseñas, ya que esto pertenece a la privacidad del menor.

Es necesario leer la información sobre la red social facilitada por los proveedores, ya que ahí se explica quienes son los titulares de la misma y la finalidad para la que solicitan los datos.

Como ya se ha explicado, si el menor tiene menos de catorce años necesitará el consentimiento de los padres o tutores y ellos serán quienes tendrán que aprobar la suscripción o no.

Si el menor fuera víctima de alguna conducta lesiva, lo más adecuado es que inmediatamente lo ponga en conocimiento de sus padres o tutores y que se denuncie a ese usuario mediante los mecanismos que dispone la misma red social. Si además la conducta fuera delictiva, se deberá denunciar a la policía (en la que han creado brigadas especializadas en los delitos derivados del uso de Internet y concretamente de las redes sociales).

En cuanto a las recomendaciones dirigidas a los padres o tutores, se establece que vigilen sus hijos menores cuando utilicen el ordenador, y que para ello tengan el ordenador en una zona común de la casa o que utilicen herramientas de monitorización que permitan conocer las rutas de navegación de los menores y que éstos no puedan eliminar ni desbloquear dichos contenidos. Así pueden realizar un control sobre lo que publican sus hijos en las redes sociales y acceder a las condiciones aplicadas respecto a su privacidad. Ahora bien, esto último es una medida extrema porque no se debe de olvidar el derecho del menor a la vida privada, por ello sólo deberá realizarse cuando indispensable.

Es conveniente que los padres comuniquen a sus hijos los contenidos que son adecuados que visiten y los que no. Además habrá que enseñarles a distinguir el tipo de información (fotografías o videos) que es adecuada para que publiquen y el riesgo que puede suponer la utilización de cámaras web, sobretodo si la utilizan con usuarios desconocidos.

Además la AEPD expone que es recomendable que se establezca el correo del padre o tutor como correo de contacto secundario porque así, cualquier petición proveniente de la red social llegará a su dirección del correo electrónico, pudiendo así conocer las actividades que realiza su hijo.

Asegurar que los controles de verificación de la edad están implementado, así como que las páginas a las que acceden los menores disponen de sistemas de reconocimiento de edad, y de la información previa respecto al tipo de contenidos que se visualizan.

También puede resultar interesante la instalación de un bloqueador de contenidos. De esta forma se puede confirmar que los menores no accederán a contenidos no recomendables, tanto desde el

---

55 Guía de Recomendaciones en 2008 “Derechos de niños y niñas- deberes de padres y madres” ([http://www.agpd.es/portalwebAGPD/canal\\_joven/common/pdfs/recomendaciones\\_menores\\_2008.pdf](http://www.agpd.es/portalwebAGPD/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf)).

ordenador, como desde teléfonos móviles.

En conclusión, de la actuación conjunta de los progenitores o tutores, así como de los proveedores o administradores de las redes sociales han de procurar que los menores accedan e interactúen en las redes sociales con las mayores garantías de seguridad para que sean protegidos en su uso, ya que aunque los mayores de catorce años puedan consentir por ellos mismo, siguen siendo un colectivo vulnerable y por tanto expuesto a mayores riesgos que los usuarios mayores de edad.

## **9. BIBLIOGRAFÍA**

ARENAS RAMIRO, Mónica, “El consentimiento en las redes sociales”, en RALLO LOMBARTE, Artemi; MARTÍNEZ MARTÍNEZ, Ricard (coord.), *Derecho y redes sociales*, Aranzadi, 2010, ISBN 978-84-470-3462-8, p. 117-142.

CASADO, Óscar, *Blog Tuenti Corporate*, (<http://corporate.tuenti.com/>), <http://corporate.tuenti.com/es/blog/los-usuarios-ya-pueden-verificar-su-edad-a-travs-del-dni-electrnico> (Última visita: 03 de Mayo de 2014).

DE HARO, M<sup>a</sup> Verónica; GRANDÍO, M<sup>a</sup> del Mar; HERNÁNDEZ, Manuel (coords.), *Historias en la red: impacto de las redes sociales en los procesos de comunicación*, Murcia, 2012, Universidad de Murcia, ISBN 978-84-15463-28-3.

DE MIGUEL ASENSIO, Pedro Alberto, “Internet, vida privada y redes sociales. Nuevos retos”, en CHAMPEAU, S; INNERARITY, D (coord.), *Internet y el futuro de la democracia*, Paidós, ISBN 978-84-493-2740-7, pp. 97-118.

Estudio sobre la utilización de la web 2.0 por parte de los menores, (<http://www.seguridadweb20.es/>), <http://www.seguridadweb20.es/estudio.php>. (Última visita: 03 de Mayo de 2014).

HERAS HERNANDEZ, María del Mar, “Internet y el derecho al honor de los menores”, en *Revista IUS*, vol.6, n<sup>o</sup>. 29, 2012, (<http://www.scielo.org/>) [http://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S1870-21472012000100007](http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472012000100007) (Última visita: 03 de Mayo de 2014).

MARTOS DÍAZ, Natalia, “Políticas de privacidad, redes sociales y protección de datos. El problema de la verificación de la edad”, en RALLO LOMBARTE, Artemi; MARTÍNEZ MARTÍNEZ, Ricard (coord.), *Derecho y redes sociales*, Aranzadi, 2010, ISBN 978-84-470-3462-8, p. 145-160.

MOURE GONZÁLEZ, Eugenio, “De padres que no educan y educadores que no son padres. Responsabilidad de padres y educadores ante las conductas de 'ciberbullying'”, en *Revista de asociación española de abogados especializados en responsabilidad civil y seguros*, n<sup>o</sup> 38, segundo trimestre, 2011 (<http://asociacionabogadosrcs.org/>), <http://www.asociacionabogadosrcs.org/revistas/rc38.pdf> (Última visita: 03 de Mayo de 2014).

PARRA, Samuel, “Protección de los datos personales”, *Blog especializado en datos personales*, (<http://www.samuelparra.com/>), <http://www.samuelparra.com/2009/06/18/tuenti-pedir-dni-mantener-cuenta/> (Última visita: 03 de Mayo de 2014).

SIMÓN CASTELLANO, Pere, El derecho al olvido en el universo 2.0, en *Textos universitarios de biblioteconomía y documentación*, n<sup>o</sup>28, 2012, (<http://bid.ub.edu/>) <http://bid.ub.edu/28/simon2.htm> (Última visita: 03 de Mayo de 2014).

TRONCOSO REIGADA, Antonio, Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales, parte dos, en *Revista de Internet, derecho y política*, n<sup>o</sup> 16, 2013 Dialnet (<http://dialnet.unirioja.es>) <http://dialnet.unirioja.es/servlet/articulo?codigo=4477236> (Última visita: 03 de Mayo de 2014).