AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Informe 0197/2013

La consulta plantea si, de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, la red social deportiva a que se refiere la consulta está autorizada a publicar material audiovisual en que aparecen menores. Indica que la mecánica consiste en que los participantes suban su material a canales privados de Youtube que después se enlaza a través de la red social. La red social a que la consulta se refiere tiene a estos efectos un perfil en Facebook. Consulta, asimismo, en caso de que surgiesen problemas tras enlazar el material que previamente estará subido en Youtube en quien derivaría la responsabilidad.

I

Como punto de partida, y dada la escasez de datos aportados en la consulta, debe tenerse en cuenta que la misma hace referencia a la existencia de una red social deportiva, a este respecto debe recordarse que la persona o personas que proporcionan dicho servicio de red social tendrán la condición de responsable tal y como dicha figura viene definida en el artículo 3 d) de la Ley Orgánica 15/1999, esto es, como la *"persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".*

En este sentido el Grupo de trabajo del artículo 29, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de 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 su Dictamen 5/2009 relativo a las redes sociales en línea, adoptada el 12 de junio de 2009, al determinar a quien se atribuye la condición de responsable del fichero o tratamiento de datos señala que los proveedores de servicios de redes sociales *"son responsables del tratamiento de datos en virtud de la Directiva relativa a la protección de datos. Proporcionan los medios que permiten tratar los datos de los usuarios, así como todos los servicios «básicos» vinculados a la gestión de los usuarios (por ejemplo, el registro y la supresión de cuentas)."*

De este modo, en su calidad de responsables del fichero o tratamiento estarán sujetos a todas aquellas obligaciones y deberes impuestos por la Ley Orgánica 15/1999 y su normativa de desarrollo, que no se encuentran limitadas a la notificación de la creación del fichero para su inscripción en el

Registro General de Protección de datos, así como a las responsabilidades que conforme a dicha Ley sean exigibles.

II

Como señala el aludido Dictamen 5/2009 los usuarios deben proporcionar datos personales para generar su descripción o perfil. De este modo el proveedor de un servicio de redes sociales lleva a cabo un tratamiento de datos personales definido en el artículo 5.1.t del Reglamento de desarrollo de la Ley Orgánica 15/1999 como "*cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."*

El tratamiento de datos de carácter personal debe encontrarse fundado en alguna de las causas legitimadoras previstas en el artículo 6 de la Ley Orgánica 15/1999, disponiendo a este respecto su número primero que "*El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa."* En lo que al presente supuesto se refiere la legitimación para el tratamiento de datos personales solamente puede encontrarse en el consentimiento de los interesados. Dicho *c*onsentimiento debe reunir las características señaladas en el artículo 3.h de la misma Ley que lo define como "*manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen*".

Esta Agencia ha venido describiendo en sus informes dichas características de manera que se entiende por consentimiento libre aquel que ha sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

El consentimiento específico viene referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.1 de la Ley Orgánica 15/1999.

Para que pueda hablarse de consentimiento inequívoco se exige la realización de una acción u omisión que implique la existencia del consentimiento.

En cuanto al requisito de la información, supone que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. A este respecto será preciso, que se facilite al

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

interesado la información a que hace referencia el artículo 5.1 de la Ley Orgánica 15/1999 según el cual ***"****Los interesados a los que se soliciten datos personales 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."

Por consiguiente, los proveedores de servicios de redes sociales deben informar a los usuarios de su identidad y proporcionarles información clara y completa sobre las finalidades y las distintas maneras en que van a tratar los datos personales.

El Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, precisa en el segundo inciso de su artículo 12.1 que *"La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos."* Y añade en el número segundo que *"Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo."*

Señala igualmente en este sentido el dictamen 5/2009 respecto de la información a facilitar que "*Los proveedores de SRS deberían informar a los usuarios de su identidad y de los distintos fines para los que tratan los datos personales, de conformidad con las disposiciones del artículo 10 de la Directiva relativa a la protección de datos, a saber, entre otras cosas:*

- la utilización de los datos con fines de comercialización directa;
- la posible distribución de datos a categorías específicas de terceros;
- una reseña de los perfiles: su creación y sus principales fuentes de datos;
- la utilización de datos sensibles."

En lo que respecta a la prueba de la obtención del consentimiento el Reglamento de desarrollo de la Ley Orgánica 15/1999, dispone en su artículo

12.3 que *"corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho."*

Por consiguiente, rige el principio de libertad de forma para acreditar la obtención del consentimiento, ello sin perjuicio de lo previsto en el artículo 7 de la Ley Orgánica 15/1999 que exige que el consentimiento sea expreso para el tratamiento y cesión de datos que hagan referencia al origen racial, a la salud y a la vida sexual y que sea, además de expreso, por escrito cuando se trate de datos que revelen la ideología, afiliación sindical, religión y creencias, con la salvedad de lo previsto para su tratamiento en el segundo inciso del artículo 7.2. Rige igualmente, tras la Sentencia de 15 de julio de 2010, de la Sala Tercera del Tribunal Supremo, el principio de libertad de forma para acreditar el cumplimiento del deber de información.

En los supuestos de recogida de datos online esta Agencia ha considerado suficiente la existencia de una política de privacidad fácilmente accesible por el usuario como acreditación del cumplimiento del deber de información, igualmente ha considerado que puede servir como prueba de la prestación del consentimiento la acreditación de que el programa impide introducir los datos sin antes haber aceptado dicha política de privacidad.

Por consiguiente, las finalidades declaradas en dicha política de privacidad vinculan al responsable del tratamiento, (en el presente supuesto el proveedor del servicio de red social) que no podrá modificar sus términos sin obtener un nuevo consentimiento informado. Dispone así el artículo 4.2 de la Ley Orgánica *" Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."*

Asimismo, los datos a recabar deberán ser adecuados, pertinentes y no excesivos en relación con las finalidades perseguidas que deberán constar en la política de privacidad, dichas finalidades deberán ser además de determinadas y explícitas, legítimas tal y como dispone el número primero del artículo 4 según el cual " *Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."*

III

En el caso que nos ocupa, los datos a tratar por el proveedor del servicio

de red social pueden ser datos de menores de edad, por lo que es preciso tener en cuenta las específicas previsiones que el Reglamento de desarrollo de la Ley Orgánica 15/1999 efectúa al respecto. Así, en lo que se refiere al otorgamiento de consentimiento el número primero del artículo 13 establece que "*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."*

Por consiguiente, el consentimiento para el tratamiento de los datos personales solamente puede ser otorgado por el interesado, salvo en el caso en que el afectado sea menor de 14 años o incapaz, en cuyo caso deberá ser otorgado por sus padres o tutores, sin perjuicio de que estos deban completar la capacidad del menor, aunque sea mayor de 14 años, en aquellos supuestos en que una Ley así lo establezca.

La obligación de información prevista en el artículo 5 de la Ley Orgánica 15/1999 exige un mayor rigor cuando el consentimiento se obtiene de un menor de edad, puesto que se dirige a una persona todavía no formada, lo que justifica que deba ser adaptada para que éste pueda comprenderla, dispone así el artículo 13.3 " *Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo."*

En cuanto a los datos que se pueden recabar, el artículo 4.1 de la LOPD dispone que "*Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados*, *pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.*" Deben tenerse en cuenta aquí las cautelas establecidas en el número 2 del artículo 13 del Reglamento, en cuanto a la información que se puede solicitar al menor, al disponer que " *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."*

Esta prohibición tiene una única excepción, a fin de permitir que se complete la capacidad del menor para consentir, señala así el último inciso del artículo 13.2 del Reglamento que "*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."*

En cuanto a la prueba del consentimiento, se establecen en el

Reglamento mayores exigencias cuando se trata de menores de edad, dispone así el número 4 del artículo 13 *"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.*

Igualmente el Dictamen 5/2009 del Grupo de Trabajo del artículo del 29 se refiere a la necesidad de proteger a los menores señalando los siguientes parámetros a incorporar a los tratamientos de datos de menores en redes sociales:

"- un tratamiento justo y legal frente a los menores, por ejemplo no pedir datos sensibles en el formulario de registro, no realizar comercialización directa destinada específicamente a los menores, el acuerdo previo de los padres antes del registro, así como grados adecuados de separación lógica entre las comunidades de niños y de adultos;
- la instauración de tecnologías que mejoren la protección de la intimidad, es decir, parámetros por defecto respetuosos de la intimidad, ventanas emergentes de advertencia en fases adecuadas, así como programas informáticos de verificación de la edad;"

IV

En lo que respecta a la publicación de contenidos en la propia red social o a través del enlace que se realiza a material previamente subido a servicios como Youtube que, de lo señalado en la consulta parece desprenderse que se efectúa exclusivamente por los propios usuarios, debe tenerse en cuenta lo siguiente:

En primer lugar, si las imágenes que constan en videos o fotografías permiten la identificación de las personas que en ellas aparecen tendrán la consideración de datos personales encontrándose amparadas por lo previsto en la Ley Orgánica 15/1999.

Debe, asimismo, examinarse si, aún siendo la imagen un dato personal, en los términos vistos, la toma y difusión de imágenes realizada por particulares puede quedar excluida de la aplicación de la normativa de protección de datos. Establece a este respecto la Ley Orgánica 15/1999 en su artículo 2 que "*El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación: a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas."*

En cuanto a la determinación de que se entiende por actividades personales o domésticas dispone el Reglamento de desarrollo de la LOPD en su artículo 4 que "*Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se*

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

inscriben en el marco de la vida privada o familiar de los particulares."

Esta es también la interpretación del término "personal" contenida en la Sentencia de la Audiencia Nacional de 15 de junio de 2006 al señalar que *"(…) Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos. "*

En consecuencia, la obtención y difusión de imágenes si se encuentra encuadrada en dicho ámbito personal y doméstico estará excluida de la aplicación de la Ley orgánica 15/1999, en virtud de lo previsto en su artículo 2.

No obstante, debe tenerse en cuenta que la utilización que se haga de las imágenes puede en algunos casos superar dicho ámbito de la vida privada o familiar de los particulares, lo que daría lugar a la aplicación de la Ley Orgánica 15/1999. Este sería el supuesto de la publicación de las fotos o vídeos en Internet cuando no existen limitaciones para su acceso, en cuanto que dicha publicación constituye una cesión de datos, definida en el artículo 3 j) de la LOPD como *"Toda revelación de datos realizada a una persona distinta del interesado",* ya que en estos supuestos, como señalaba la sentencia la Sentencia de 6 de noviembre de 2003 (caso Bodil Lindqvist) del Tribunal de Justicia de las Comunidades Europeas, no se inscribe en el marco de la vida privada o familiar de los particulares *"un tratamiento de datos personales consistente en la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de personas."*

Debe añadirse que la limitación en el acceso a las imágenes puede no ser el único indicador de que estamos ante un uso familiar o doméstico, así el Grupo de trabajo del artículo 29 en el aludido Dictamen 5/2009 destaca que habitualmente, el acceso a los datos (datos de perfil, archivos subidos a la red, textos…) aportados por un usuario viene limitado a los contactos por él mismo elegidos. Sin embargo, en algunos casos los usuarios pueden llegar a tener un gran número de personas de contacto, y de hecho puede darse el caso de que no conozca a algunos de ellos. Señala el Dictamen que un alto número de contactos puede ser una indicación para que no se aplique la exclusión a la normativa de protección de datos a que se viene haciendo referencia y se considere al usuario responsable de un fichero, debiendo asumir algunas de las responsabilidades de éstos.

De este modo la Ley Orgánica 15/1999 resultará aplicable en aquellos supuestos en que se supere dicho ámbito personal, como el supuesto en que las imágenes se publiquen en Internet en una página de libre acceso para cualquier persona o cuando el alto número de personas invitadas a contactar con dicha página resulte indicativo de que dicha actividad se extiende más allá de lo que es propio de dicho ámbito. En estos casos, nos hallamos ante una

cesión de datos sujeta al régimen establecido por la Ley Orgánica 15/1999, que exige el consentimiento del interesado y en caso de que este sea menor de 14 años el de sus padres o tutores.

Cabe así recordar la Sentencia de 2 de enero de 2013 de la Audiencia Nacional, confirmatoria de una Resolución de esta Agencia declarando una infracción por vulneración del principio de consentimiento (recogido en el artículo 6 de la Ley Orgánica 15/1999), por la difusión efectuada por un usuario de Facebook de un vídeo en su muro, libremente accesible a cualquier usuario de dicha red social, en que éste aparece conversando con un grupo de escolares menores de edad (de entre 7 y 8 años) que miran a la cámara y cuyo rostro resulta identificable sin que dicho usuario de la red social hubiera obtenido para dicha difusión el consentimiento de sus padres o tutores.

Debe así tenerse en cuenta que en el Dictamen 5/2009 se señala que "El Grupo de Trabajo recomienda que:

- los proveedores de SRS adviertan adecuadamente a los usuarios sobre los riesgos de ataque a su intimidad y a la de otros cuando ponen información en línea en los SRS;
- los SRS recuerden a sus usuarios que poner en línea información relativa a otras personas puede perjudicar su derecho a la intimidad y a la protección de datos;

- los SRS aconsejen a sus usuarios que no pongan en línea fotografías o información relativa a otras personas sin el consentimiento de éstas."

No obstante, aunque en una red social sean los propios usuarios quienes hacen públicos datos personales y a ellos a quien se imputaría, en su caso, la responsabilidad por una actuación vulneradora de lo previsto en la Ley Orgánica 15/1999 con motivo de la publicación de datos personales, debe recordarse que el proveedor de la red social se encuentra obligado a adoptar las pertinentes medidas de seguridad tal y como establece el artículo 9.1 de la Ley Orgánica 15/1999 según el cual "*El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural."* Dichas medidas vienen actualmente recogidas en el Reglamento de desarrollo de la Ley Orgánica 15/1999. De este modo la inexistencia de medidas de seguridad o su inadecuación que permitan un acceso fuera del ámbito de los contactos elegidos por el usuario determinarían la responsabilidad del responsable de la red social.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Señala en relación a estas cuestiones el Dictamen 5/2009 que "*Un tratamiento seguro de la información es un elemento clave para la confianza en los SRS. Los responsables deben adoptar las medidas técnicas y de organización apropiadas «tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos» con objeto de garantizar la seguridad e impedir todo tratamiento no autorizado, habida cuenta de los riesgos que presente el tratamiento y la naturaleza de los datos que deban protegerse."*

Un elemento importante de los parámetros de confidencialidad es el acceso a los datos personales publicados en un perfil. Si no existe ninguna restricción a tal acceso, los terceros podrán acceder a toda clase de detalles íntimos sobre los usuarios, bien como miembros del SRS, o mediante motores de búsqueda. Sin embargo, solamente una minoría de usuarios que se registran en tal servicio modifican los parámetros por defecto. Los SRS deberían pues establecer parámetros por defecto respetuosos de la intimidad, que permitan a los usuarios aceptar libre y específicamente que personas distintas de sus contactos elegidos accedan a su perfil, con el fin de reducir el riesgo de un tratamiento ilícito por terceros. Los perfiles de acceso limitado no deberían ser localizables por los motores de búsqueda internos, incluso por la función de búsqueda por parámetros como la edad o el lugar. Las decisiones de ampliar el acceso pueden no estar implícitas, por ejemplo mediante la posibilidad de exclusión voluntaria proporcionada por el responsable del SRS."

V

Debe igualmente recordarse en materia de responsabilidad que, además de la protección otorgada por la Ley Orgánica 15/1999, la publicación de vídeos o fotografías de terceros sin su consentimiento puede infringir su derecho al honor, a la intimidad o a la propia imagen, derechos cuya protección se rige por lo dispuesto en la 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.

Asimismo, dentro de los principios jurídicos fundamentales a la hora de aplicar la normativa de protección de datos a menores, el principal es el interés superior del niño. Este principio viene recogido en diversas normas internacionales tales como el artículo 3 de la Convención de las Naciones Unidas sobre los derechos del niño, el Convenio Europeo sobre el ejercicio de los derechos del niño del Consejo de Europa en su artículo 6 y el artículo 24.2 de la Carta de de derechos Fundamentales de la Unión Europea. En nuestro derecho positivo se recoge expresamente en la 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, que establece en su artículo 2 que "*En la*

aplicación de la presente Ley primará el interés superior de los menores sobre cualquier otro interés legítimo que pudiera concurrir. Asimismo, cuantas medidas se adopten al amparo de la presente Ley deberán tener un carácter educativo."

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 en 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.

VI

Entre los derechos de los interesados, y correlativa obligación de hacer efectivos los mismos por parte del proveedor de la red social, se encuentran los derechos de acceso, rectificación, cancelación y oposición regulados en los artículos 15 y siguientes de la Ley Orgánica 15/1999 y en los artículo 23 a 36 de su Reglamento de desarrollo.

Debe señalarse que el ejercicio de estos derechos no se encuentra restringido a los usuarios de la red social sino que corresponde a cualquier persona cuyos datos se traten, por lo que la red social deberá proporcionar un medio para ejercer dichos derechos. El artículo 24 de Reglamento de desarrollo de la Ley Orgánica dispone a este respecto que "*Deberá concederse al interesado un medio, sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición"*

Asimismo, debe recordarse que la Ley Orgánica 15/1999 que exige, con carácter general, el consentimiento del interesado para el tratamiento y cesión de datos, permite, igualmente, la revocación del mismo, esto es, que el interesado pueda exigir el cese en el tratamiento de sus datos mediante su pura y simple manifestación de voluntad, tal y como se recoge en los artículos 6.3 y 11.4, siendo en estos supuestos el procedimiento a seguir el regulado en el artículo 17 del Reglamento.

VII

Debe asimismo tenerse en cuenta que el tratamiento de datos

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

efectuado por el responsable de la red social deberá respetar el principio de conservación, previsto en el artículo 4.5 de la Ley Orgánica 15/1999, según el cual "*Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados".*

Respecto del plazo de cancelación, establece el artículo 16. 5 de la Ley Orgánica 15/1999 que *"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".*

El artículo 8.6 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, dispone que *"Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.*

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento."

Ello sin perjuicio del ejercicio de los derechos de cancelación, oposición o revocación que asisten al interesado a los que se ha hecho referencia en el punto anterior.

Debe señalarse que la cancelación de los datos no supone su eliminación automática, sino su bloqueo tal y como dispone el artículo 16.3 de la Ley Orgánica 15/1999 al establecer que *"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."*

El aludido Reglamento de desarrollo de la Ley Orgánica 15/1999, define en su artículo 5.1. b) la cancelación como "*Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.*"

En cuanto al modo de llevar a cabo el bloqueo, se señalaba en informe de esta Agencia de 5 de junio de 2007 que "*deberá efectuarse de forma tal que no sea posible el acceso a los datos por parte del personal que tuviera habitualmente tal acceso, por ejemplo, el personal que preste sus servicios en el centro consultante, limitándose el acceso a una persona con la máxima responsabilidad y en virtud de la existencia de un requerimiento judicial o administrativo a tal efecto. De este modo, pese a permanecer el tratamiento de los datos, el acceso a los mismos quedaría enteramente restringido a las personas a las que se ha hecho referencia.*"

En informe de 1 de agosto de 2005 se indicaba que resulta imposible establecer una enumeración taxativa de los períodos en que el dato habrá de permanecer bloqueado, en relación con lo dispuesto en el artículo 16.3, no obstante, señalaba los siguientes criterios:

> *"En cuanto a las causas que podrán motivar la conservación del dato, sujeto a su previo bloqueo, además de la relación jurídica con el afectado, a la que se refiere el artículo 16.5 de la Ley Orgánica 15/1999, éstas deberán fundarse en lo dispuesto "en las disposiciones aplicables" o a la "atención de las posibles responsabilidades nacidas del tratamiento", tal y como prevé dicha Ley.*
>
> *En este sentido, para la determinación del período de bloqueo de los datos debe tenerse en cuenta que la Sentencia del tribunal Constitucional 292/2000, de 30 de noviembre, viene a imponer, expresamente, el principio de reserva de Ley en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier limitación a ese derecho (como sería la derivada del artículo 16.3 de la Ley) deberá constar en una disposición con rango de Ley para que el bloqueo de los datos pueda considerarse lícitamente efectuado. Así, a título de ejemplo, podría considerarse que el bloqueo habrá de efectuarse durante los plazos de prescripción de las acciones*

derivadas de la relación jurídica que funda el tratamiento, en los términos previstos por la legislación civil o mercantil que resulte de aplicación, así como el plazo de cuatro años de prescripción de las deudas tributarias, en cuanto los datos puedan revestir trascendencia desde el punto de vista tributario (habida cuenta de la obligación de conservación que impone el artículo 111 de la Ley General Tributarias y el plazo legal de prescripción de cuatro años previsto en el artículo 24 de la Ley de Derechos y Garantías de los Contribuyentes).

En todo caso, debe recordarse que el mantenimiento del dato bloqueado, supone una excepción al borrado físico del mismo que, en definitiva, es el fin último de la cancelación (tal y como prevé el propio artículo 16.3, al indicar que "cumplido el citado plazo deberá procederse a la supresión)."

A los períodos mencionados en el informe citado cabe añadir el plazo de prescripción de 3 años, previsto en el artículo 47.1 de la propia Ley Orgánica 15/1999 en relación con las conductas constitutivas de infracción muy grave, sin perjuicio de que otras normas con rango de Ley, puedan establecer otros plazos de conservación de los datos.

Por consiguiente, los datos deberán cancelarse una vez hayan dejado de ser necesarios para la finalidad para la que se recabaron, lo que deberá determinarse en cada caso, manteniéndose bloqueados en los términos vistos, al menos durante el tiempo necesario para la prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula al consultante con los usuarios de sus servicios, el plazo de prescripción previsto en el artículo 47.1 de la Ley Orgánica 15/1999 o los establecidos en otras normas con rango de Ley que resulten de aplicación al caso, debiendo eliminarse los datos una vez transcurridos dichos plazos.

Por su parte el Dictamen 5/2009 al referirse al deber de conservación señala que "*Los datos personales comunicados por un usuario cuando se registra en un SRS deberían suprimirse en cuanto el usuario o el proveedor de SRS decida suprimir la cuenta. Del mismo modo, la información suprimida por el usuario cuando actualice su cuenta no debería conservarse. Los SRS deberían informar a los usuarios antes de proceder a estos trámites, a través de los medios de que disponen, sobre estos períodos de conservación. Por razones jurídicas y de seguridad, en algunos casos específicos, podría justificarse conservar datos y cuentas actualizados o suprimidos durante un período de tiempo determinado con el fin de contribuir a impedir las*

operaciones maliciosas resultantes de la usurpación de identidad y demás infracciones o delitos.

Cuando un usuario no utiliza el servicio durante un período determinado, el perfil debería desactivarse, es decir, dejar de ser visible por otros usuarios o por el mundo exterior y, después de otro periodo, los datos de la cuenta abandonada deberían suprimirse. Los SRS deberían informar a los usuarios antes de proceder a estos trámites a través de los medios de que dispongan."

VIII

Por último, tomando en consideración que la red social deportiva a que la consulta se refiere va a permitir su uso por menores, debe recordarse que esta Agencia ha publicado unas recomendaciones para la protección de datos de los menores, en las que se señalaba que deben extremarse las precauciones en Internet y, en particular, se indicaba que "no es aconsejable publicar fotos que identifiquen a un niño, por ejemplo situándole en el contexto de un colegio y/o actividad determinados."

De este modo para que fuera compatible dicha consideración con la actividad, señalada en la consulta, de enlace de los vídeos subidos a otros canales como Youtube, debería recomendarse a los usuarios que eviten subir a dichos canales videos o fotografías de menores, salvo en el caso de que no permitan la identificación de éstos, bien por la distancia con que se tomen las imágenes o bien mediante la utilización de técnicas de distorsión u ocultamiento del rostro.

Resultan especialmente de interés en el caso de los menores las recomendaciones del Grupo de Trabajo del 29 en el Dictamen 5/2009 a que se ha venido haciendo referencia, relativas a las advertencias que se deben efectuar a los usuarios de la red sobre los riesgos de ataque a su intimidad y a la de otros cuando ponen información en línea en redes sociales, y se recuerde que difundir videos o fotografías de otras personas sin su consentimiento puede infringirse el derecho a la protección de datos o los derechos al honor, a la intimidad o a la propia imagen.

Asimismo, resultan plenamente de aplicación, dentro ya del ámbito de la red social deportiva a que la consulta se refiere, las recomendaciones sobre el establecimiento de parámetros respetuosos del derecho a la protección de datos desde el diseño mismo de la red social estableciendo mecanismos en que por defecto los datos personales no sean accesibles a un número indeterminado de personas.