AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

**Informe 0184/2013**

La consulta plantea diversas dudas respecto a la aplicación de lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, a la creación de una red social en la que, según señala el consultante, existirán 3 tipos de perfiles (personas físicas, profesionales o autónomos y empresas, que podrán dar de alta a empleados). Señala que en la red social además de interaccionar unas personas con otras se crean contenidos por parte de los usuarios y empresas (conversaciones, mensajes, debates, consultas, publicaciones, etc.).

**I**

La consulta hace referencia a la creación de una red social por el consultante en la que participarán tanto particulares como empresas, por lo que es preciso examinar el carácter con el que todos ellos actúan dentro de dicha red desde el punto de vista del derecho a la protección de datos personales, en tanto que ello determinará sus derechos y obligaciones conforme a dicha normativa.

1. Así en primer lugar en lo que se refiere al consultante, 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, el consultante en su calidad de responsable del fichero o tratamiento estará sujeto a todas aquellas obligaciones y deberes impuestos por la Ley Orgánica 15/1999 y su normativa de desarrollo, así como a las responsabilidades que conforme a dicha Ley sean exigibles.

2. En lo que se refiere a los usuarios de la red social que sean personas físicas, debe señalarse que el tratamiento de datos personales de terceros que realicen en la red puede quedar excluido 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 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. “*

También dará lugar a la aplicación de la Ley Orgánica 15/1999, por superar el ámbito de la vida privada o familiar de los particulares la publicación de datos de terceros en la red cuando no existan limitaciones de acceso a su perfil, 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.”*

Igualmente la limitación en el acceso a los datos contenidos en su perfil 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 propias de un responsable.

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 un perfil de libre acceso para cualquier persona o cuando el alto número de personas invitadas a contactar con dicho perfil 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.

3. Asimismo, cuando la persona física utilice la red social actuando en nombre de una empresa o una asociación o utilice la red principalmente como una plataforma con fines comerciales, políticos o sociales<0} asume todas las obligaciones de un responsable de datos que está revelando datos personales a otro responsable de datos (el servicio de redes sociales) y a terceros (otros usuarios de Servicios de Redes Sociales o, potencialmente, otros responsables de datos con acceso a los mismos).

Este sería la posición que ocuparán los profesionales o autónomos cuando utilicen la red social como tales para sus propios fines y no como particulares o, en su caso, los particulares cuando utilizan una red social en la forma señalada en el párrafo anterior. En lo que se refiere a las personas jurídicas, resulta plenamente aplicable la Ley Orgánica 15/1999.

Por consiguiente, todos ellos, en dicha calidad de responsable del tratamiento de datos, deberán asumir aquéllas obligaciones que la Ley Orgánica 15/1999 impone a éstos. Ahora bien, teniendo en cuenta que dicho tratamiento se efectúa en el marco de una determinada red social, en la que las reglas de funcionamiento son impuestas por el proveedor de la red, algunas de estas obligaciones podrán encontrarse limitadas a aquéllos aspectos en los que el consultante tiene libertad para actuar.

**II**

Todos los responsables a que anteriormente se ha hecho referencia llevarán a cabo un tratamiento de datos personales de terceros, 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."*

1. En lo que respecta al proveedor del servicio de red social la legitimación para el tratamiento de datos personales solamente puede encontrarse en el consentimiento de los interesados. Dicho consentimiento 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 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, 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."*

2. De la misma manera los profesionales, autónomos o empresarios, así como los particulares cuando el tratamiento de datos personales que lleven a cabo exceda del ámbito personal o doméstico, llevan a cabo un tratamiento de datos personales que exigirá el consentimiento de los interesados.

El consentimiento en dichos casos deberá igualmente reunir los requisitos del artículo 3 en antes citado, esto es libre, específico, inequívoco e informado

sobre la finalidad o finalidades de la recogida de datos, y de la identidad y dirección del responsable en cada caso, así como de la posibilidad de ejercer sus derechos de acceso, rectificación, cancelación y oposición ante el mismo.

La consulta no especifica los mecanismos de interacción entre particulares y empresas, por lo que no cabe pronunciarse sobre la manera en que los responsables distintos al proveedor del servicio de red social puedan obtener el consentimiento de los terceros, en los términos vistos, y probar tanto la obtención del mismo como la del cumplimiento del deber de información, debiendo la red social articular algún mecanismo para facilitar a dichos responsables el cumplimiento de sus obligaciones en materia de protección de datos.

Debe recordarse que el carácter de inequívoco del consentimiento implica una acción u omisión que implique la existencia del consentimiento por lo que no cabe el tratamiento de datos de terceros que no lo hayan prestado aunque su perfil se encuentre abierto, ya que dicha circunstancia no implica el consentimiento de sus titulares para el tratamiento de los datos personales contenidos en el mismo.

Asimismo, debe tenerse en cuenta que el tratamiento de los datos se encuentra limitado por el principio de proporcionalidad recogido en el artículo 4.1 de la Ley 15/1999, antes transcrito, de modo que la utilización de información contenida en el perfil de aquéllos que hayan otorgado su consentimiento para el tratamiento de sus datos por un responsable del tratamiento se encuentra limitada a aquéllos datos estrictamente necesarios para lograr la finalidad para la que se ha prestado el consentimiento.

**Si se pretendiera además recolectar datos adicionales contenidos en el perfil, por ejemplo, los relativos a gustos, aficiones, periodicidad de la utilización de los servicios del consultante o cualquier otro que pueda utilizarse con la finalidad de remitirle una publicidad personalizada, deberá informarse de la existencia de dicho tratamiento de datos y de la finalidad del mismo, a fin de que sea conocido y consentido por los interesados.**

**No obstante, la incorporación de los datos de quienes hayan consentido su tratamiento a los propios sistemas de los responsables distintos del proveedor del servicio de redes sociales exige el consentimiento de los afectados, en los términos señalados. Dicha incorporación, implicaría que el consultante adquiere además de la condición de responsable del tratamiento la de responsable del fichero, y en consecuencia, se encuentra obligado a notificar la creación del fichero para su inscripción en el Registro General de Protección de Datos, así**

**como la plena adopción de las medidas de seguridad que, en función, de la naturaleza de los datos a tratar exigen los artículos 9 de la Ley Orgánica 15/1999 y concordantes del Reglamento de desarrollo de dicha Ley, aprobado por Real Decreto 1720/2007, de 21 de diciembre.**

Mención especial debe hacerse al tratamiento de los datos en la red social de los empleados de empresas o profesionales y autónomos, en tanto la consulta señala que éstos podrán dar de alta a sus empleados en la red social, desconociéndose tanto los datos que personales que pueden tratarse como la clase de tratamiento de datos que pueda llevarse a cabo. Debe así recordarse que la comunicación de datos de los empleados por el empleador tanto a la red social como a otros usuarios, constituye una cesión de datos de carácter personal definida en el artículo 3 i) de la Ley Orgánica 15/1999 como *"Toda revelación de datos realizada a una persona distinta del interesado".*

A este respecto cabe recordar lo señalado en informe de esta Agencia de 29 de abril de 2010 en relación con una consulta sobre la publicación en una página web de datos de empleados de una empresa, dicho informe tomaba como punto de partida lo señalado en el Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral adoptado por el Grupo de Trabajo del Artículo 29, en el que se enumeran y desarrollan los principios fundamentales de la protección de datos que los empresarios deberán tener siempre en cuenta en el contexto laboral.

Recordaba dicho informe que en cuanto a la legitimación del tratamiento señala expresamente el Dictamen 8/2001 que "Por lo que respecta al "Consentimiento", el Grupo del artículo 29 considera que si un empresario debe tratar datos personales como consecuencia inevitable y necesaria de la relación laboral, no debería legitimar este tratamiento a través del consentimiento. Por el contrario, el recurso al consentimiento deberá limitarse a los casos en los que el trabajador pueda expresarse de forma totalmente libre y tenga la posibilidad de rectificar posteriormente sin verse perjudicado por ello."

Concluía dicho informe que el consentimiento para la comunicación por Internet de los datos de sus empleados, no podría entenderse válidamente prestado en el contexto de la relación laboral si su negativa a darlo, llevase aparejada algún tipo de consecuencia adversa o discriminatoria, no pudiendo hablarse de consentimiento libre, por lo que la comunicación de los datos de los empleados en Internet no puede ampararse en el consentimiento del trabajador.

Esta es también la postura de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), cuyo

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

considerando 34 señala lo siguiente. *"El consentimiento no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal cuando exista un desequilibro claro entre el interesado y el responsable del tratamiento. Así sucede especialmente cuando el primero se encuentra en una situación de dependencia respecto del segundo, por ejemplo, cuando los datos personales de los trabajadores son tratados por el empresario en el contexto laboral.(…)"*

De este modo, en cuanto que el consentimiento no vendría a legitimar una cesión de datos de los trabajadores en una red social, habría que examinar si, en cada caso, dicha comunicación forma parte del contrato de trabajo (por ser precisamente el objeto de dicho contrato como ocurriría, por ejemplo, en el supuesto del trabajador contratado para ser la imagen de la empresa) así como si se ajusta a los principios de protección de datos y en particular al de proporcionalidad, para determinar si la misma es conforme a la Ley Orgánica 15/1999.

**III**

La difusión de datos personales en una red social que no se ajuste a los principios señalados en la Ley Orgánica 15/1999 dará lugar a una infracción de la misma imputable en cada caso al responsable del tratamiento contrario a ella.

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.

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.

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."*

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, cabe recordar al consultante como proveedor de un servicio de red social que en el Dictamen 5/2009 se señalaba 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."

A ello habría que añadir en el presente caso que se advierta a los empleadores de que es responsabilidad suya la difusión datos de sus empleados sin que se encuentre debidamente legitimada en lo establecido en la Ley Orgánica 15/1999, tal y como anteriormente se ha indicado.

**IV**

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.

El ejercicio de estos derechos deberá llevarse a cabo ante los responsables del tratamiento distintos del proveedor del servicio de red social a que la consulta se refiere cuando se refiera a datos difundidos por aquéllos en el espacio de que dispongan para sus contenidos dentro de la red social.

**V**

Debe asimismo tenerse en cuenta que el tratamiento 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."*