GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

01189/09/ES

WP 163

Dictamen 5/2009 sobre las redes sociales en línea

Adoptado el 12 de junio de 2009

Este Grupo de Trabajo, creado por el artículo 29 de la Directiva 95/46/CE, es un organismo de la UE, con carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y el artículo 15 de la Directiva 2002/58/CE.

De la secretaría del Grupo se encarga la Dirección C (Derechos fundamentales y ciudadanía) de la Comisión Europea, Dirección General de Justicia, Libertad y Seguridad, B-1049 Bruselas, Bélgica, despacho LX-46 01/02.

Sitio Web: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Índice

Resumen

El presente dictamen se centra en la forma en que el funcionamiento de los sitios de redes sociales cumple los requisitos de la legislación de la UE en materia de protección de datos. Su objetivo principal es proporcionar orientaciones a los proveedores de SRS en cuanto a las medidas que deben establecerse para garantizar el cumplimiento del Derecho comunitario.

Este dictamen tiene en cuenta que los proveedores de SRS y, en numerosos casos, los proveedores terceros, son responsables del tratamiento de datos, con las responsabilidades que ello implica para con los usuarios de SRS. El dictamen destaca que un gran número de usuarios funcionan en un ámbito puramente personal, poniéndose en contacto con personas que forman parte de su ámbito personal, familiar o doméstico. En estos casos, el dictamen considera que se aplica la «exención doméstica», y que, por tanto, no se aplica la normativa que regula a los responsables del tratamiento de datos. El dictamen precisa también en qué circunstancias las actividades de un usuario de SRS no están cubiertas por la «exención doméstica». La difusión y utilización de la información disponible en los SRS con fines secundarios, no buscados, es una preocupación principal del Grupo de Trabajo del artículo 29. El dictamen recomienda una seguridad sólida y unos parámetros por defecto propicios al respeto de la vida privada como punto de partida ideal para todos los servicios ofrecidos. El acceso a la información del perfil constituye la principal fuente de preocupación. El dictamen aborda también temas como el tratamiento de datos o imágenes sensibles, la publicidad o la comercialización directa en los SRS, así como las cuestiones referentes a la conservación de datos.

Las recomendaciones esenciales se refieren a la obligación de los proveedores de SRS de cumplir la Directiva relativa a la protección de datos y de mantener y reforzar los derechos de los usuarios. Es de primordial importancia que los proveedores de SRS informen a los usuarios acerca de su identidad desde el momento de su registro e indiquen todos los fines para los que se tratan los datos personales. Los proveedores de SRS deberían también prestar una atención especial al tratamiento de los datos personales de los menores. El dictamen recomienda que los usuarios no pongan en línea fotografías o información relativa a otras personas sin su consentimiento. Además, el dictamen considera que los proveedores de SRS tienen la obligación de asesorar a sus usuarios por lo que se refiere al derecho a la intimidad de los demás.

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[1],

Vistos el artículo 29 y el artículo 30, apartado 1, letra a), y apartado 3, de dicha Directiva, así como el artículo 15, apartado 3, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002,

Visto el artículo 255 del Tratado CE y el Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión,

Visto su Reglamento interno,

HA ADOPTADO EL PRESENTE DOCUMENTO:

1. Introducción

La evolución de las comunidades virtuales y los servicios alojados en Internet, tales como los servicios de redes sociales («SRS»), es un fenómeno relativamente reciente, cuyo número de usuarios sigue multiplicándose de manera exponencial.

La información personal publicada en línea por un usuario, a la que se añaden los datos que describen las acciones e interacciones del usuario con otras personas, puede crear un perfil muy preciso de los intereses y actividades del usuario. Los datos personales publicados en los sitios de redes sociales pueden ser utilizados por terceros con distintos fines, en particular, comerciales, y pueden representar grandes riesgos, como la usurpación de identidad, pérdidas económicas, pérdida de actividad económica o posibilidades de empleo, o ataque a la integridad física.

En marzo de 2008, el Grupo de Trabajo internacional de Berlín sobre protección de datos en las telecomunicaciones adoptó el *Memorándum de Roma*[2]. Este memorándum analiza los riesgos a la intimidad y a la seguridad que presentan las redes sociales y proporciona directrices a los reguladores, proveedores y usuarios. La recientemente adoptada Resolución sobre la protección de la vida privada en los servicios de redes sociales[3] examina también los retos que plantean los SRS. El Grupo de Trabajo tiene en cuenta también el documento de orientación publicado en octubre de 2007 por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), titulado «*Cuestiones de seguridad y recomendaciones para las redes sociales en línea*»[4], destinado a los reguladores y proveedores de redes sociales.

2. Definición de «servicio de red social (SRS)» y modelo comercial

---

1 Diario Oficial nº L 281 de 23.11.1995, p. 31, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

2 http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

3 Adoptada en la 30 Conferencia internacional de los Comisarios responsables de la protección de datos y la vida privada en Estrasburgo, 17.10.2008,http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf

4 http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

Los SRS pueden definirse generalmente como plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes. En sentido jurídico, las redes sociales son servicios de la sociedad de la información, según se definen en el artículo 1, apartado 2, de la Directiva 98/34/CE, modificada por la Directiva 98/48/CE. Los SRS comparten determinadas características:

- los usuarios deben proporcionar datos personales para generar su descripción o «perfil»;

- los SRS proporcionan también herramientas que permiten a los usuarios poner su propio contenido en línea (contenido generado por el usuario como fotografías, crónicas o comentarios, música, vídeos o enlaces hacia otros sitios[5]);

- las «redes sociales» funcionan gracias a la utilización de herramientas que proporcionan una lista de contactos para cada usuario, con las que los usuarios pueden interactuar.

Los SRS generan la mayoría de sus ingresos con la publicidad que se difunde en las páginas web que los usuarios crean y a las que acceden. Los usuarios que publican en sus perfiles mucha información sobre sus intereses ofrecen un mercado depurado a los publicitarios que desean difundir publicidad específica y basada en esta información.

Es por tanto importante que los SRS funcionen respetando los derechos y libertades de los usuarios, que tienen la expectativa legítima de que los datos personales que revelan sean tratados de acuerdo con la legislación europea y nacional relativa a la protección de datos y de la intimidad.

3. Aplicación de la Directiva relativa a la protección de datos

Las disposiciones de la Directiva relativa a la protección de datos se aplican en la mayoría de los casos a los proveedores de SRS, aunque su sede se encuentre fuera del EEE. El Grupo de Trabajo del artículo 29 remite a su dictamen previo sobre los motores de búsqueda, con el fin de obtener información complementaria sobre las cuestiones del establecimiento y la utilización de equipo como determinantes para la aplicabilidad de la Directiva relativa a la protección de datos y de las normas derivadas del tratamiento de las direcciones IP y la utilización de «cookies»[6].

3.1 ¿Quién es el responsable del tratamiento de datos?

Proveedores de SRS

Los proveedores de SRS 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). Los proveedores de SRS determinan también la manera en que los datos de los usuarios pueden utilizarse con fines publicitarios o comerciales, incluida la publicidad proporcionada por terceros.

Proveedores de aplicaciones

[5] Cuando los SRS prestan servicios de comunicaciones electrónicas, también se aplican las disposiciones de la Directiva 2002/58 sobre la privacidad y las comunicaciones electrónicas.

[6] WP148, Dictamen 1/2008 sobre asuntos relativos a la protección de datos vinculados a las herramientas de búsqueda.

Los proveedores de aplicaciones también pueden ser responsables del tratamiento de datos, si desarrollan aplicaciones que funcionan además de las de los SRS y que los usuarios deciden utilizar.

Usuarios

En la mayoría de los casos, los usuarios se consideran personas interesadas. La Directiva no impone las obligaciones de un responsable del tratamiento de datos a una persona que trata datos personales «en el ejercicio de actividades exclusivamente personales o domésticas». En algunos casos, la exención doméstica puede no cubrir las actividades de un usuario de SRS y puede entonces considerarse que el usuario ha asumido algunas de las responsabilidades de un responsable de datos. A continuación figuran algunos de estos casos:

3.1.1. Objeto y naturaleza

La tendencia creciente de los SRS es el «*paso de la Web 2.0 para el ocio a la Web 2.0 para la productividad y los servicios*»[7], donde las actividades de algunos usuarios de SRS pueden superar una actividad puramente personal o doméstica, por ejemplo cuando el SRS se utiliza como una plataforma de colaboración para una asociación o una empresa. Si un usuario de SRS actúa en nombre de una empresa o de una asociación o utiliza el SRS principalmente como una plataforma con fines comerciales, políticos o sociales, la exención no se aplica. En este caso, el usuario asume la plena responsabilidad de un responsable del tratamiento de datos que revela datos personales a otro responsable del tratamiento de datos (SRS) y a terceros (otros usuarios de SRS o incluso, potencialmente, a otros responsables del tratamiento de datos que tienen acceso a ellos). En tales circunstancias, el usuario necesita el consentimiento de las personas interesadas u otra base legítima que figure en la Directiva relativa a la protección de datos.

Generalmente, el acceso a los datos de un usuario (datos del perfil, mensajes, historias…) se limita a los contactos elegidos. Sin embargo, en algunos casos, los usuarios pueden adquirir un gran número de contactos terceros y no conocer a algunos de ellos. Un gran número de contactos puede indicar que no se aplica la excepción doméstica y el usuario podría entonces ser considerado como un responsable del tratamiento de datos.

3.1.2. Acceso a la información del perfil

Los SRS deberían garantizar el establecimiento de parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos.

Cuando el acceso a la información del perfil va más allá de los contactos elegidos, en particular, cuando todos los miembros que pertenecen al SRS pueden acceder a un perfil[8] o cuando los datos son indexables por los motores de búsqueda, el acceso sobrepasa el ámbito personal o doméstico. Del mismo modo, si un usuario decide, con perfecto conocimiento de causa, ampliar el acceso más allá de los «amigos» elegidos, asume las responsabilidades de un responsable del tratamiento de datos. En la práctica, se aplica entonces el mismo régimen jurídico que cuando una persona utiliza otras plataformas tecnológicas para publicar datos personales en Internet[9]. En varios Estados miembros, la falta de restricciones de acceso (y por tanto, el carácter público de los datos) supone que el usuario asume las responsabilidades de

[7] Discurso de la Sra. Reding, Comisaria europea responsable de la Sociedad de la Información y los Medios de Comunicación, durante la reunión relativa al futuro de Internet del Consejo Europeo de Lisboa en Bruselas, el 2 de febrero de 2009. Este discurso se titula «Internet del futuro: Europa debe desempeñar un papel principal».

[8] O cuando pueda alegarse que la aceptación de contactos no es objeto de una selección, es decir, si los usuarios aceptan «contactos» sin preocuparse de la relación que les une.

[9] Como las plataformas de publicación que no son SRS, o los programas informáticos que se alojan a sí mismos.

un responsable del tratamiento de datos a efectos de la aplicación de la Directiva relativa a la protección de datos[10].

Debe tenerse en cuenta que, aunque la exención doméstica no se aplique, el usuario de SRS puede beneficiarse de otras exenciones, como la exención con fines periodísticos, artísticos o literarios. En estos casos, debe establecerse un equilibrio entre la libertad de expresión y el derecho a la intimidad.

3.1.3 Tratamiento de datos de terceros por los usuarios

La aplicación de la exención doméstica se ve también limitada por la necesidad de garantizar los derechos de los terceros, especialmente por lo que se refiere a los datos sensibles. Además, cabe señalar que, aunque se aplique la exención doméstica, un usuario puede ser responsable en virtud de las disposiciones generales del derecho civil o penal nacional en cuestión (en particular, difamación, responsabilidad por violación del derecho a la personalidad o responsabilidad penal).

3.2 Seguridad y parámetros de confidencialidad por defecto

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 [11].

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[12], por ejemplo mediante la posibilidad de exclusión voluntaria proporcionada por el responsable del SRS.

---

[10] En su sentencia Satamedia, el TJCE decide lo contrario en el apartado 44: «*De ello resulta que esta excepción debe interpretarse en el sentido de que es aplicable únicamente a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares (véase la sentencia Lindqvist, antes citada, apartado 47). Manifiestamente éste no es el caso de las actividades de Markkinapörssi y Satamedia, que tienen por objeto poner los datos recogidos en conocimiento de un número indefinido de personas*».

[11] Artículo 17 y considerando 46 de la Directiva relativa a la protección de datos.

[12] El informe y directrices sobre la intimidad en los servicios de redes sociales («Memorándum de Roma») señala riesgos tales como «El concepto engañoso de la comunidad», p. 2, o «Revelar más información personal de la que se cree», p. 3. Una empresa de seguridad informática advierte a un importante SRS sobre el acceso por defecto a miembros en la misma localización geográfica: http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html

3.3 Información proporcionada por los SRS

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.

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[13].

3.4 Datos sensibles

Los datos que revelan el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia sindical y los datos relativos a la salud y a la vida sexual se consideran sensibles. Los datos personales sensibles sólo pueden publicarse en Internet con el consentimiento explícito de la persona interesada o si esta misma persona ha hecho públicos estos datos[14].

En algunos Estados miembros de la UE, las imágenes de personas se consideran una categoría especial de datos personales, puesto que pueden utilizarse para distinguir entre el origen racial o étnico o para deducir sus creencias religiosas o datos relativos a la salud. El Grupo de Trabajo no considera, en general, que las imágenes en Internet sean datos sensibles[15], salvo si se utilizan claramente para revelar datos sensibles sobre las personas.

Como responsables del tratamiento de datos, los SRS no pueden tratar datos sensibles relativos a sus miembros o no miembros sin su consentimiento explícito[16]. Si un SRS incluye en los formularios de registro preguntas relativas a datos sensibles, deberá indicar muy claramente que la respuesta a tales preguntas es totalmente voluntaria.

---

[13] Esto podría verse facilitado por la introducción de herramientas de gestión de etiquetas de la información en los sitios de redes sociales, en particular, creando espacios en un perfil personal para indicar la presencia de un nombre de usuario en imágenes o vídeos con etiqueta que estén a la espera del consentimiento del usuario en cuestión, o fijando plazos de expiración para las etiquetas que no hayan recibido el consentimiento de la persona señalada.

[14] Los Estados miembros pueden prever excepciones a esta norma; véase el artículo 8, apartado 2, letra a), segunda frase, y el artículo 8, apartado 4, de la Directiva relativa a la protección de datos.

[15] No obstante, la publicación de imágenes en Internet suscita inquietud por lo que respecta a la intimidad a medida que mejoran las técnicas de reconocimiento facial.

[16] El consentimiento debe ser libre, informado y específico.

3.5 Tratamiento de datos de no miembros

Muchos SRS permiten a los usuarios proporcionar datos sobre otras personas, como añadir un nombre a una imagen, evaluar a una persona, o poner una lista de «gente que he conocido/quiero conocer» en acontecimientos. Esta información puede identificar también a no miembros. Sin embargo, el tratamiento de este tipo de datos relativos a no miembros por el SRS sólo puede realizarse si se cumple uno de los criterios contemplados en el artículo 7 de la Directiva relativa a la protección de datos.

Además, la creación de perfiles de no miembros prerrellenados mediante la agregación de datos proporcionados independientemente por usuarios de SRS, incluidos los datos afines deducidos de las listas de contactos en línea, no tiene ninguna base jurídica[17].

Incluso aunque el SRS tuviese los medios para ponerse en contacto con el no usuario e informarle de la existencia de datos personales relativos a él, una posible invitación por correo electrónico para adherirse al SRS con el fin de acceder a estos datos personales violaría la prohibición prevista en el artículo 13, apartado 4, de la Directiva sobre la privacidad y las comunicaciones electrónicas, relativa al envío de mensajes electrónicos no solicitados con fines de comercialización directa.

3.6 Acceso de terceros

3.6.1 Acceso por medio de los SRS

Además del servicio básico de los SRS, la mayoría de los SRS ofrecen a los usuarios aplicaciones adicionales proporcionadas por diseñadores terceros, que también tratan datos personales.

Los SRS deberían tener los medios para garantizar que las aplicaciones de terceros se ajusten a las Directivas relativa a la protección de datos y sobre la privacidad y las comunicaciones electrónicas. Eso supone, en particular, que informen a los usuarios clara y específicamente acerca del tratamiento de sus datos personales y que sólo tengan acceso a los datos personales necesarios. Los SRS deberían por tanto ofrecer a los diseñadores terceros un acceso progresivo para que puedan optar por un método de acceso intrínsecamente más limitado. Además, los SRS deberían garantizar que los usuarios pueden comunicar fácilmente sus inquietudes con respecto a las aplicaciones.

3.6.2 Acceso de terceros por medio de los usuarios

Los SRS permiten a veces a los usuarios acceder y actualizar sus datos gracias a otras aplicaciones. Los usuarios pueden por ejemplo:

- leer y enviar mensajes a la red desde su teléfono móvil;
- sincronizar los datos de sus amigos del SRS con su agenda de un ordenador de sobremesa;
- actualizar automáticamente su situación o localización en el SRS utilizando otro sitio web.

[17] El considerando 38 de la Directiva relativa a la protección de datos precisa: «*Considerando que el tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención.*» Para algunos SRS, la publicación de los perfiles de no miembros se ha convertido supuestamente en una manera no desdeñable de comercializar sus «servicios».

Los SRS publican la forma en que estos programas informáticos pueden crearse en forma de una «interfaz de programación». Eso permite a cualquier tercero crear programas informáticos para realizar estas tareas y permitir a los usuarios elegir entre varios prestadores de servicios terceros[18]. Al ofrecer una interfaz de programación que permita el acceso a los datos, los SRS deberían:

- establecer un nivel de detalle que permita al usuario elegir un nivel de acceso destinado a terceros y que se limite únicamente a la realización de una tarea determinada.

Al acceder a datos personales a través de una interfaz de programación de un tercero en nombre de un usuario, los prestadores de servicios terceros deberían:

- tratar y conservar los datos durante no más del tiempo necesario para realizar una tarea específica;

- limitar las operaciones sobre los datos de los contactos importados por el usuario al uso personal del usuario que los ha proporcionado.

3.7 Bases jurídicas de la comercialización directa

La comercialización directa constituye una parte esencial del modelo comercial de los SRS; éstos pueden utilizar diferentes modelos de comercialización. No obstante, la comercialización que utilice los datos personales de los usuarios deberían cumplir las disposiciones aplicables de la Directiva relativa a la protección de datos y sobre la vida privada y las comunicaciones electrónicas[19].

La *comercialización contextual* se adapta al contenido visto por el usuario o al que accede éste.[20.]

La *comercialización segmentada* consiste en difundir publicidad a grupos de usuarios específicos[21]; se coloca al usuario en un grupo en función de la información que ha comunicado directamente al SRS[22].

Por último, la *comercialización de comportamiento* selecciona la publicidad basándose en la observación y análisis de la actividad del usuario a lo largo del tiempo. Estas técnicas pueden estar sujetas a requisitos jurídicos, dependiendo de las bases jurídicas aplicables y de las características de las técnicas utilizadas. El Grupo de Trabajo recomienda no utilizar datos sensibles en los modelos publicitarios de comportamiento, a menos que se cumplan todos los requisitos jurídicos.

Cualquiera que sea el modelo o la combinación de modelos utilizados, la publicidad puede ser difundida directamente por el SRS (el proveedor de SRS ejerce aquí una actividad de intermediario), o por un publicitario tercero. En el primer caso, los datos personales de los usuarios no deben revelarse a terceros. Sin embargo, en el segundo caso, el publicitario tercero probablemente tratará los datos personales de los usuarios, en particular, si trata la dirección IP del usuario o una cookie situada en el ordenador de éste.

---

18 Si bien «interfaz de programación» es un término técnico amplio, en este caso se refiere al acceso en nombre de un usuario, lo que significa que los usuarios deben dar sus datos de acceso al programa informático para que pueda actuar en su nombre.

19 El Grupo de Trabajo tiene la intención de tratar los distintos aspectos de la publicidad en línea en otro documento en un futuro inmediato.

20 Por ejemplo, si la página vista menciona la palabra «París», la publicidad difundida puede presentar un restaurante en esta ciudad.

21 Cada grupo queda definido por una serie de criterios.

22 En particular, cuando se registra en el servicio

3.8 Conservación de datos

Los SRS no están incluidos en el ámbito de aplicación de la definición de servicios de comunicaciones electrónicas prevista en el artículo 2, letra c), de la Directiva marco (2002/21/CE). Los proveedores de SRS pueden ofrecer servicios adicionales incluidos en el ámbito de los servicios de comunicación electrónica tales como un servicio de mensajería electrónica accesible públicamente. Tal servicio estará sujeto a las disposiciones de la Directiva sobre la protección de la vida privada en el sector de las comunicaciones electrónicas y la Directiva sobre conservación de datos.

Algunos SRS permiten a sus usuarios enviar invitaciones a terceros. La prohibición de utilizar el correo electrónico con fines de comercialización directa no se aplica a las comunicaciones personales. Para cumplir la excepción de las comunicaciones personales, un SRS debe cumplir los siguientes criterios:

- no incentivar al remitente ni al destinatario;
- el proveedor no selecciona a los destinatarios[23];
- la identidad del remitente debe mencionarse claramente;
- el remitente debe conocer todo el contenido del mensaje que se enviará en su nombre.

Algunos SRS conservan también los datos de identificación de los usuarios suspendidos del servicio, con el fin de garantizar que ya no podrán registrarse de nuevo. En tal caso, estos usuarios deben ser informados de que se está realizando tal tratamiento. Además, la única información que puede conservarse es la información de identificación y no las razones por las que se suspendió a estas personas. Esta información no deberá conservarse durante más de un año.

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[24]. 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.

---

[23] Es decir, que está prohibida la práctica que realizan algunos SRS de enviar invitaciones indiscriminadamente a toda la lista de contactos de un usuario.

[24] De conformidad con lo dispuesto en el artículo 6, apartado 1, de la Directiva relativa a la protección de datos, los datos deben ser *«conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente»*

3.9 Derechos de los usuarios

Los SRS deberían respetar los derechos de las personas afectadas por el tratamiento de datos, de conformidad con lo dispuesto en los artículos 12 y 14 de la Directiva relativa a la protección de datos.

Los derechos de acceso y rectificación de los usuarios no se limitan a los usuarios del servicio, sino a toda persona física cuyos datos se tratan[25]. Los miembros y no miembros de los SRS deben tener un medio de ejercer su derecho de acceso, rectificación y supresión. La página inicial de los sitios SRS debería hacer referencia claramente a la existencia de una «oficina de reclamaciones», creada por el proveedor de SRS con el fin de gestionar los problemas relativos a la protección de datos y la intimidad, así como las denuncias de los miembros y no miembros.

El artículo 6, apartado 1, letra c), de la Directiva relativa a la protección de datos exige que los datos sean *«adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente»*. En este contexto, cabe señalar que el SRS puede tener necesidad de registrar algunos datos de identificación de sus miembros, pero no es preciso que publique su verdadero nombre en Internet. Por tanto, los SRS deberían considerar si pueden justificar el hecho de obligar a sus usuarios a actuar bajo su verdadera identidad en vez de bajo un seudónimo. Son argumentos de peso para que los SRS dejen la elección a este respecto a los usuarios, y es una exigencia legal al menos en un Estado miembro. Estos argumentos son especialmente sólidos cuando el SRS en cuestión tiene miembros en todo el mundo.

El artículo 17 de la Directiva relativa a la protección de datos exige que el responsable del tratamiento aplique las medidas técnicas y de organización adecuadas para la protección de los datos personales. Tales medidas de seguridad incluyen, en particular, el control del acceso y mecanismos de autenticación que pueden aplicarse aunque se utilicen seudónimos.

4. Niños y menores

Una gran parte de los servicios de SRS es utilizada por niños y menores. El dictamen WP147[26] del Grupo de Trabajo examinó la aplicación de los principios de protección de datos en el medio escolar y educativo. El dictamen destacó la necesidad de tener en cuenta los intereses del niño, lo que también figura en la Convención internacional sobre los derechos del niño de las Naciones Unidas. El Grupo de Trabajo desea subrayar la importancia de este principio en el contexto de los SRS.

Las autoridades encargadas de la protección de datos han emprendido iniciativas interesantes[27] en todo el mundo, centradas principalmente en la sensibilización en materia de SRS y los posibles riesgos. El Grupo de Trabajo fomenta investigaciones complementarias sobre la manera de solucionar las dificultades que rodean la comprobación de la edad requerida y la prueba del consentimiento informado, con el fin de afrontar lo mejor posible estos retos.

---

[25] Es el caso, en particular, en que el servicio de SRS utiliza la dirección electrónica de una persona para enviarle una invitación.

[26] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf

[27] Por ejemplo, la iniciativa portuguesa «Dadus» http://dadus.cnpd.pt/ o la insignia danesa de control del chat, http://www.fdim.dk/

Basándose en las consideraciones anteriores, el Grupo de Trabajo opina que una estrategia pluridimensional sería adecuada para abordar la protección de datos de los niños en el contexto de los SRS. Tal estrategia se basaría en:

- iniciativas de sensibilización, fundamentales para garantizar el compromiso activo de los niños (mediante las escuelas, la inclusión en el programa escolar de elementos de protección de datos, la creación de herramientas educativas ad hoc y la colaboración de organismos nacionales competentes);

- 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;

- la autorregulación de los proveedores con el fin de fomentar la adopción de códigos de buenas prácticas que deberían incluir medidas de ejecución eficaces y sanciones disciplinarias;

- en caso necesario, medidas legislativas ad hoc para desalentar prácticas desleales y/o fraudulentas en el contexto de los SRS.

5. Resumen de los derechos y obligaciones

Aplicabilidad de las directivas comunitarias

1. **La Directiva relativa a la protección de datos se aplica generalmente al tratamiento de datos personales por los SRS, aunque su sede se encuentre fuera del EEE.**

2. **Los proveedores de SRS se consideran responsables del tratamiento de datos en virtud de la Directiva relativa a la protección de datos.**

3. **Los proveedores de aplicaciones pueden eventualmente ser considerados responsables del tratamiento de datos en virtud de la Directiva relativa a la protección de datos.**

4. **Los usuarios se consideran interesados por lo que respecta al tratamiento de sus datos por los SRS.**

5. **El tratamiento de datos personales por los usuarios corresponde en la mayoría de los casos a la exención doméstica. Existen casos en que las actividades de un usuario no se benefician de esta exención.**

6. **Los SRS no entran en el ámbito de aplicación de la definición de los servicios de comunicaciones electrónicas, y por tanto la Directiva sobre conservación de datos no se aplica a los SRS.**

Obligaciones de los SRS

7. Los SRS deberían 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.

8. Los SRS deberían establecer parámetros por defecto respetuoso de la intimidad.

9. Los SRS deberían informar y advertir a sus usuarios frente a los riesgos de atentado a la intimidad cuando transfieren datos a los SRS.

11. Los SRS deberían recomendar a sus usuarios no poner en línea imágenes o información relativa a otras personas sin el consentimiento de éstas.

12. Como mínimo, en la página inicial de los SRS debería figurar un enlace hacia una oficina de reclamaciones, tanto para miembros como para no miembros, que cubra cuestiones de protección de datos.

13. La actividad comercial debe ajustarse a las normas establecidas por la Directiva relativa a la protección de datos y la Directiva sobre la protección de la vida privada en el sector de las comunicaciones electrónicas.

14. Los SRS deben establecer plazos máximos de conservación de los datos de los usuarios inactivos. Las cuentas abandonadas deben suprimirse.

15. Por lo que se refiere a los menores, los SRS deberían adoptar medidas adecuadas con el fin de limitar los riesgos.

<u>Derechos de los usuarios</u>

16. Tanto los miembros como los no miembros de los SRS tienen los derechos de los interesados si procede, de acuerdo con las disposiciones de los artículos 10 a 14 de la Directiva relativa a la protección de datos.

17. Tanto los miembros como los no miembros deberían tener acceso a un procedimiento de tratamiento de las denuncias establecido por los SRS y de fácil uso.

18. Los usuarios deberían, en general, poder adoptar un seudónimo.

Hecho en Bruselas, 12 de junio de 2009

Por el Grupo de Trabajo
El Presidente
Alex TÜRK