

Las redes sociales digitales: ¿hacia una nueva configuración de los derechos fundamentales en Internet?

Ana Isabel Herrán Ortiz

DOI: <https://doi.org/10.47623/ivap-rvap.87.88.2010.16>

«El pasado siempre permanece en el presente y será accesible en el futuro ya que en internet ninguna información desaparece».

Antonio Troncoso Reigada

Sumario: I. Impacto jurídico, social y económico de las redes sociales. Las claves del éxito.—II. Definición y caracterización de las redes sociales. Su tipología. 1. Las redes sociales generalistas o de ocio. 2. Las redes sociales profesionales.—III. Redes sociales y riesgos. La problemática de los derechos de la persona.—IV. Protección de datos personales en las redes sociales. 1. Marco legal europeo de protección de datos personales. 2. Normativa española de protección de datos personales y su aplicación a las redes sociales.—V. El acceso de los menores a las redes sociales.—VI. Actuaciones públicas en defensa del usuario.—VII. Conclusiones.—VIII. Reseña bibliográfica.

Laburpena. Hitz gakoak.—Resumen. Palabras clave.—Abstract. Keywords.

I. Impacto jurídico, social y económico de las redes sociales. Las claves del éxito

Todos coincidimos en afirmar que el ser humano es un ser social por naturaleza, que necesita de los demás para realizarse y desarrollar su vida en sociedad. Hoy, la máxima representación de esta sociabilidad se encuentra en el espectacular crecimiento de las redes sociales. La sociedad española no ha sido ajena a este fenómeno, y se sitúa en Europa como primer país en número de usuarios de redes sociales, y segundo del mundo (1). Esta realidad se refleja en el reciente Estudio del Observatorio de la Seguridad de la Información, cuando revela que el 80% de los encuestados manifiesta en 2009 que accede habitual u ocasionalmente a

(1) ONTSI, Informe sobre el Sector de las tecnologías de la Información en España 2008, 2009.

redes sociales, frente al 22.6% que reconocía acceder a estas plataformas en 2008 (2). Y así, seguramente, hemos tenido en alguna ocasión la oportunidad o la tentación de establecer nuevas amistades y relaciones con personas a quienes no conocemos pero que nos invitan a participar en su red de contactos, y con las que nos une un interés profesional, laboral, personal, de ocio... Bienvenido entonces al mundo de las redes sociales.

En una sociedad dominada por la información, donde el poder se sitúa en el conocimiento, y donde valemos tanto más por nuestras relaciones o contactos como por lo que somos, las redes sociales han venido a configurar e impulsar un nuevo concepto de relación personal y social. Tal y como recuerda ORIHUELA, hoy en día cuesta imaginar aquellas agendas y libretas de contactos, que representaban nuestra red social y que han sido superadas por nuevas herramientas de comunicación que facilitan una forma virtual de contacto y relación; así, primero irrumpe el móvil con agenda, y después, las redes sociales digitales, como representación virtual y pública de nuestras relaciones personales, profesionales y laborales (3).

En efecto, cuando en 2002 emerge la denominada web 2.0 el internauta ya no sólo busca y decide la información que desea obtener sino que también la edita, comenta y comparte. De una internet que hasta entonces se presentaba estática, y en la que el usuario era un mero espectador, se llega a una internet colaborativa, dinámica y social, donde el usuario no se conforma con ser parte activa de la red y relacionarse con otros internautas, sino que se convierte en protagonista voluntario de una comunidad virtual, desde la que se promueven encuentros, movimientos sociales de apoyo o rechazo y se convocan reuniones o manifestaciones. Nos hallamos ante una internet social e interrelacional, en la que las redes sociales son su principal herramienta.

Y en este cambio de comportamiento y actitud, en el que se busca compartir entre personas, empresas e instituciones, tanto experiencias, sensaciones, viajes, amistades, como música o conocimientos ha de situarse el espectacular crecimiento de las redes sociales. Éxito que sin duda se ha visto favorecido por la generalización del uso de los teléfonos móviles y de ordenadores portátiles que por su agilidad permiten compartir en breve espacio de tiempo y desde cualquier lugar experiencias, información, vídeos o fotografías.

Las redes sociales han abierto una forma impensable de hacer política, han establecido un espacio de libertad de expresión inimaginable

(2) OBSERVATORIO DE SEGURIDAD DE LA INFORMACIÓN (INTECO), *Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles (10.ª Oleada) Tercer Trimestre (2009)*, 2010.

(3) ORIHUELA, José Luis, «Internet: la hora de las redes sociales», *Nueva Revista*, n.º 119, 2008, pp. 57-ss.

hasta ahora, y han favorecido las relaciones laborales y profesionales en un momento tan crítico como el que actualmente vivimos. Sin embargo, las incuestionables bondades descritas, no pueden hacernos olvidar que los usuarios comparten información, datos personales, imágenes, en ocasiones muy sensibles, e incluso de terceras personas, lo que sin duda debe interpretarse como un cambio en la consideración de la intimidad y la privacidad personal por parte del propio usuario, que expone en ocasiones a un riesgo evidente importantes derechos fundamentales de la persona.

Efectivamente, el propio concepto y el funcionamiento de las redes sociales conllevan cierta renuncia a la intimidad por quienes acceden a las mismas y comparten su vida privada, y si bien puede decirse que se trata de una renuncia voluntaria, no siempre es consciente y reflexiva. Se desconoce, en ocasiones, la política de privacidad de estas plataformas, que no resulta de fácil comprensión, y de manera mecánica de aceptan cuantas condiciones son precisas para poder participar en estas comunidades virtuales, especialmente cuando se trata de los más jóvenes.

Como tendremos oportunidad de estudiar, desde las más diversas instancias públicas se insiste en recomendar a los usuarios la misma prudencia que emplearían en sus actividades fuera de las redes sociales, se les solicita que no actúen de manera inconsciente, impulsiva o imprudente, y que sus actos se guíen por los mismos criterios que les animan en el mundo real. Debemos medir las consecuencias de nuestros actos, y no actuar de manera irreflexiva y poco cautelosa. Las oportunidades, las posibilidades y ventajas que ofrecen las redes sociales no deben quedar en entredicho por las actuaciones imprudentes, abusivas y arriesgas de los usuarios o de terceros malintencionados.

Desde la perspectiva empresarial y económica, las redes sociales han reforzado la presencia de empresas y medios de comunicación en la red, facilitando la realización de negocios a través de internet. Hoy en día tener un espacio de negocio en las redes sociales más populares puede significar un aumento considerable de los beneficios, ya que tal y como demuestran los diferentes estudios analizados, los usuarios de Internet reconocen en su mayoría acceder habitualmente a estas comunidades y buscar todo lo que necesitan a través de ellas. De igual manera, al constituirse en espacio de sociabilización, se convierten en una herramienta incomparable para analizar a posibles competidores, o comunicarse con potenciales clientes, quienes además consultan e indagan dentro de estas plataformas antes de concretar alguna compra o negocio. Por todo ello, no debe menospreciarse la trascendencia comercial, empresarial y económica de las redes sociales, habida cuenta del número de usuarios que pertenecen a estas comunidades virtuales y de las actividades que en ellas se desarrollan.

El panorama descrito y la realidad incontestable de su éxito convierten a este nuevo fenómeno de las redes sociales en fuente y objeto de inagotables y trascendentes incertidumbres y conflictos jurídicos que han despertado el interés y la atención de juristas, instituciones, sociólogos y empresarios; y así, desde este estudio se pretende ofrecer, a partir de una perspectiva jurídica, un análisis que permita explicar y despejar las sombras y recelos que han acompañado estos últimos tiempos a las redes sociales.

II. Definición y caracterización de las redes sociales. Su tipología

Para comprender y analizar el desarrollo de las redes sociales debemos establecer previamente su concepto y caracteres y así poder explicar el éxito de su crecimiento y de su popularidad. De acuerdo con la definición ofrecida en el Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes online del Instituto Nacional de Tecnologías de la Comunicación (en adelante INTECO) y la Agencia Española de Protección de Datos (en adelante AEPD), las redes sociales online son «servicios prestados a través de internet que permiten a los usuarios generar un perfil, desde el que hacer públicos datos e información personal y que proporcionan herramientas que permiten interactuar con otros usuarios y localizarlos en función de las características publicadas en sus perfiles» (4).

Por su parte, el Observatorio de la Seguridad de la Información, definía a la red social como la «aplicación online que permite a los usuarios, de forma completamente descentralizada, generar un perfil público, compartir información, colaborar en la generación de contenidos y participar de forma espontánea en movimientos sociales y corrientes de opinión». Así mismo, deben destacarse como elementos claves que configuren este concepto: un aspecto sociológico, por el que cualquier persona con conexión a internet puede acceder a estos servicios; un aspecto tecnológico, por el cual gracias al avance en las telecomunicaciones se ha favorecido el crecimiento y normalización del uso de estas redes; y por último, un elemento jurídico, que exige el cumplimiento de la normativa aplicable a estos servicios y la adopción de medidas de tutela de los derechos de los usuarios de estas plataformas (5).

(4) INTECO y AEPD, *Estudio sobre privacidad de los datos y la seguridad de la información en las redes online, 2009*. (Fecha de consulta: 15/03/2010) http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/est_red_sociales_es

(5) OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN (INTECO), *Guía Redes sociales, menores de edad y privacidad en la red, 2008*. (Fecha de consulta: 17/03/2010) http://www.inteco.es/Seguridad/Observatorio/manuales_es/guiaManual_redes_menores

Siguiendo la definición de ORIHUELA, las redes sociales en línea «son servicios basados en la web que permiten a sus usuarios relacionarse, compartir información, coordinar acciones y en general, mantenerse en contacto», en palabras del autor, estos servicios y aplicaciones representan nuestra red social, permiten la construcción de nuestra identidad digital, y facilitan la difusión de nuestras actividades en la red (6).

Jurídicamente, los servicios de redes sociales pueden definirse como «plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes» (7). En este sentido, las redes sociales se convierten en espacios virtuales de relación personal, en los que no sólo gestionamos nuestra identidad digital sino en los que además podemos restringir y limitar la información que nos interesa y concierne en atención a nuestros gustos, preferencias e intereses.

De estas definiciones se desprenden las siguientes consideraciones en torno a las funcionalidades que definen a las redes sociales online, y por las que puede afirmarse que nacen con la finalidad de interrelacionar personas, fomentar la relación offline de los usuarios, y favorecer la difusión de la propia red a través de sus usuarios, mediante lo que se ha venido en denominar proceso viral de expansión de las redes sociales.

En definitiva, hacemos nuestras las acertadas consideraciones de CACHIA, por las que las redes sociales, con carácter general, se definen por (8):

- La presentación personalizada de los usuarios mediante la creación de sus propios perfiles.
- La gratuidad, salvo excepciones como el caso de redes sociales profesionales que ofrecen servicios avanzados.
- La facilidad de uso, que no precisa de usuarios expertos informáticos.
- La fuerza social que les permite actuar como grupos de presión u opinión.
- La interconexión personal o profesional, ya que favorece el contacto entre personas con intereses comunes.
- La posibilidad de gestionar la red de contactos por cada usuario.

En su Informe Sobre los problemas y recomendaciones de seguridad de las redes sociales, la Agencia Europea ENISA, señaló que son características que definen a la red social digital que (9):

(6) ORIHUELA, José Luis, «Internet: la hora de las redes sociales, *Nueva Revista*, n.º 119, 2008, p. 58.

(7) GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 5/2009 sobre las redes sociales en línea, adoptado el 12 de junio de 2009, Doc. WP 163.

(8) CACHIA, Romina, «Los sitios de creación de redes. Aspectos sociales», *Cuadernos de Comunicación e Innovación*, n.º 16, 2008, pp. 72-ss.

(9) EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA), «Security Issues and Recommendations for Online Social Networks», 2007.

- Se trata de herramientas para la publicación de datos personales a partir del perfil personal creado por el usuario vinculado a sus propios intereses y a su vida personal.
- Se constituyen como herramientas para personalizar, socialmente centradas en la interacción, y basadas en el perfil personal.
- Son herramientas para la definición de las relaciones sociales que determinan quién tiene acceso a los datos disponibles y qué pueden comunicarse, con quién y cómo.

Realizadas estas consideraciones, debemos apuntar que las peculiaridades anteriormente indicadas, comunes a toda tipología de red social, no impiden la necesaria clasificación de las mismas. Si bien antes conviene introducir un importante apunte, se piensa siempre en redes sociales digitales, cuando lo cierto es que las redes sociales, tal y como se ha puesto de manifiesto al inicio de este estudio, existen y se han desarrollado antes de internet, porque no debemos olvidar que el ser humano es un ser social. Así, siguiendo las acertadas consideraciones de FERNÁNDEZ BURGUEÑO (10) y sus criterios de clasificación de las redes sociales, hay que diferenciar, en primer lugar, las redes analógicas o redes sociales Off-Line, aquellas en las que las relaciones sociales, con independencia de su origen, se desarrollan sin mediación de aparatos o sistemas electrónicos, y las redes digitales o redes sociales On-Line, aquellas que tienen su origen y se desarrollan a través de medios electrónicos. Debemos subrayar que nuestro interés se centra en analizar este último fenómeno, por lo que cualquier referencia a las redes sociales, en el marco de este estudio, ha de entenderse necesariamente realizada en relación con las redes sociales digitales.

1. Las redes sociales generalistas o de ocio

Las redes sociales digitales, a su vez, por el sujeto principal de la relación, pueden clasificarse en redes sociales de contenidos, en las que las relaciones se desarrollan uniendo perfiles a través de contenido publicado, los objetos que posee el usuario o los archivos que se encuentran en su ordenador, y en redes sociales humanas, aquellas que centran su atención en fomentar las relaciones entre personas uniendo individuos según su perfil social y en función de sus gustos, aficiones, lugares de trabajo, viajes y actividades.

Son, sin duda, estas últimas las más conocidas, las que mayor difusión y trascendencia pública han alcanzado, y su pretensión principal

(10) FERNÁNDEZ BURGUEÑO, Pablo, *Clasificación de redes sociales*. (Fecha de consulta: 24/03/2010) <http://www.pabloburgueno.com/2009/03/calificacion-de-redes-sociales/>

consiste en promocionar y fomentar las relaciones personales entre los usuarios que a ellas acceden. Estas redes, cuyo espectacular crecimiento ha sido puesto de manifiesto en diversos informes, sitúan su éxito, por un lado, en la variedad de aplicaciones y funcionalidades que ofrecen a los usuarios, que pueden prescindir de herramientas externas de comunicación; y por otro lado, en la posibilidad de desarrollar aplicaciones propias ejecutadas en la red social o externas que se interconectan con la propia plataforma.

Si atendemos a su localización geográfica, las redes se clasifican en redes sociales sedentarias, que cambian en función de las relaciones entre personas, los contenidos compartidos o los eventos creados, y redes sociales nómadas, que se componen y recomponen a tenor de los sujetos que se hallen geográficamente cerca del lugar en el que se encuentra el usuario, los lugares que haya visitado o aquellos a los que tenga previsto acudir.

Y por último, atendiendo a su finalidad y temática, se clasifican en redes sociales horizontales, dirigidas a todo tipo de usuario y sin una temática definida, y que permiten la entrada y participación libre y genérica sin un fin definido; y redes sociales verticales, concebidas sobre la base de un eje temático unificador. Su objetivo es el de congregarse en torno a una temática definida a un colectivo concreto. En función de su especialización, pueden clasificarse a su vez en:

- *Redes sociales verticales de ocio*: Su objetivo es congregarse a colectivos que desarrollan actividades de ocio, deporte, usuarios de videojuegos, fans, etc.
- *Redes sociales verticales mixtas*: Ofrecen a usuarios y empresas un entorno específico para desarrollar actividades tanto profesionales como personales en torno a sus perfiles.
- *Redes sociales verticales profesionales*: Están dirigidas a generar relaciones profesionales entre los usuarios.

Nos detendremos en el próximo epígrafe a profundizar en el estudio de estas redes sociales profesionales, que por su evolución e impacto económico despiertan la curiosidad y el interés de las empresas y los profesionales, y son las que mayor proyección de crecimiento han experimentado.

2. Las redes sociales profesionales

Siguiendo un interesante Informe Preliminar del Estudio presentado por el Instituto Madrileño de Desarrollo, si en 2008 un 50% los usuarios que accedía a una determinada red social manifestaba hacerlo motivado

por un interés personal, en 2009 son menos de la mitad; y sin embargo, se cuadruplican aquellos que hacen un uso estrictamente profesional de las redes sociales (5% vs. 21%), lo que sin duda permite subrayar en un primer momento, el auge que han experimentado estas plataformas también en el ámbito profesional y empresarial (11).

Se presentan estas redes sociales como ámbitos y espacios para establecer contactos profesionales entre usuarios, que las valoran positivamente y que reconocen en ellas una nueva oportunidad para presentarse laboralmente y para conocer las últimas noticias y novedades relacionadas con su negocio o profesión.

Ahora bien, si atendemos a los datos publicados en un Estudio realizado por Sage «Radiografía de la PYME 2010», únicamente el 17% de estas empresas emplea las redes sociales asociadas al negocio; y para estar al día en el sector únicamente la utilizan el 6.55%, en tanto que se revela que para la obtención de algún beneficio en su empresa el 83% no utiliza las redes sociales, manifestando que el 39.5% nunca ha utilizado redes sociales en el ámbito de su actividad empresarial (12). Estos datos demuestran, a nuestro juicio, que todavía en el ámbito empresarial y de los negocios no se ha avanzado tanto como pudiera pensarse y que son muchos los recelos y las dudas que se ciernen sobre el uso profesional de las redes sociales. No sucede así en Estados Unidos, donde se señala que el 68% de las compañías de B2C de venta electrónica reconocen haber conseguido clientes a través de Facebook (13).

Como aspectos más significativos de esta tipología de redes sociales se señalan desde una perspectiva laboral, que ofrecen al trabajador la búsqueda de nuevas oportunidades de empleo y que facilitan el establecimiento de nuevos contactos profesionales y laborales; y desde el ámbito empresarial, permiten el acceso a candidatos en los procesos de selección, facilitan el seguimiento de las actividades de empresas competidoras, favorecen el marketing personalizado, promueven la difusión y publicidad de la actividad empresarial, y permiten a las empresas ofrecer servicios premium para que sus usuarios accedan a servicios avanzados.

No puede afirmarse que el riesgo para el usuario es menor cuando accede a las plataformas profesionales, piénsese que en ellas se comparten principalmente datos personales de ámbito profesional y de experiencia laboral, y en ocasiones, también datos relativos a la vida privada y familiar, de especial interés para empresas u otros usuarios. Ciertamente, una

(11) Primer Estudio del impacto de Twitter en la generación y difusión de la innovación, Instituto Madrileño de Desarrollo, Madrid Network, 2010.

(12) http://www.sage.es/radiografiadelapyme2010/Radiografia_de_la_pyme_2010.pdf (Fecha de consulta: 10/03/2010).

(13) <http://www.emarketer.com/Results.aspx?N=0&Ntk=basic&Ntt=B2C> (Fecha de consulta: 03/03/2010).

lectura de la política de privacidad y de las condiciones de uso de cualquier plataforma profesional permite concluir que los riesgos que afectan a los usuarios de redes sociales de ocio amenazan igualmente a quienes acceden a las redes sociales profesionales. En efecto, así se desprende de las advertencias que desde el Observatorio de la Seguridad se han recogido en las diferentes Guías de ayuda para usuarios, también de redes profesionales. Sirva como ejemplo, que para ser usuario de LinkedIn es necesario tener las cookies activadas, y que en caso contrario, no se puede utilizar el servicio ofrecido. Así mismo, se permite la indexación de los datos de LinkedIn por parte de los buscadores y se produce la conservación de datos de forma indefinida; según se expresa en las citadas Guías, otra plataforma profesional Xing, no informa a propósito de la conservación de datos personales, y se denuncia por estas Guías, que esta red social presenta importantes dificultades en el proceso de cancelación de las cuentas de sus usuarios (14).

Resumiendo, no se ajusta a la realidad manifestar que son menores los riesgos y peligros que desde las redes sociales profesionales afectan a los usuarios, en tanto que el análisis de las políticas de privacidad y de las condiciones de uso de estas plataformas permite afirmar que la privacidad y el derecho a la protección de datos personales pueden verse afectados en igual medida que en las redes sociales generalistas o de ocio.

III. Redes sociales: riesgos y amenazas. La problemática de los derechos de la persona

Por la propia naturaleza y esencia de los servicios de las redes sociales, no hay que olvidar que nos hallamos ante plataformas de contactos y de intercambio de información (15), y precisamente por ello, estas comunidades representan en sí mismas una amenaza y un riesgo para sus usuarios. Como recuerda MIRALLES, las virtudes y defectos del mundo real se encuentran reflejados también en internet, si bien los principios que se aplican en ambos espacios no se corresponden exactamente. Coincidimos con el autor, cuando advierte que no hay nada más real que internet, lo que allí sucede no desaparece cuando cerramos la aplicación y apagamos el ordenador, y los efectos y las consecuencias permanecen,

(14) OBSERVATORIO DE SEGURIDAD DE LA INFORMACIÓN Y UPM, *Guías de ayuda para la configuración de la privacidad y seguridad de las redes sociales*, 2010. (Fecha de consulta: 17/03/2010) http://inteco.es/Seguridad/Observatorio/manuales_es/guia_ayuda_redes_sociales

(15) «Facebook te ayuda a comunicarte y compartir tu vida con las personas que conoces», de este modo se presenta una de las plataformas preferidas por los usuarios españoles. «Como usuario encontrarás una nueva forma de interactuar e intercambiar conocimientos, oportunidades y consejos con otros profesionales», proclama la página de presentación de una red social profesional.

y afectan no sólo a nuestros intereses en internet, sino también a nuestra realidad física (16).

En efecto, si consideramos que el fin y la esencia de las redes sociales se halla en compartir información, amigos, contactos, experiencias, no resulta difícil comprender los recelos y las reservas que las redes sociales despiertan en instituciones, empresas y juristas. Ahora bien, rápidamente vienen a nuestra mente actividades humanas que conllevan riesgo, incluso peligro para la propia vida y la de los demás, y no por ello dejamos de realizarlas, ni desde las instituciones se recomienda abstenerse en su realización. En efecto, el usuario debe identificar y conocer la existencia de los riesgos inherentes a las redes sociales como instrumentos de comunicación, sin que por ello deba denostarse el uso de esta herramienta, antes bien al contrario, al tiempo que se ensalzan sus innegables ventajas y bondades, deben señalarse sus peligros, y debe informarse y educarse para una actuación prudente, ordenada y vigilante, que ayude al usuario a actuar con el sentido común y la prudencia deseables en todas las situaciones de la vida cotidiana.

Con carácter general, y sin referencia a concretas redes sociales, se señalaban en la 30.^a Conferencia Internacional de Autoridades de Protección de Datos (17), los riesgos más destacados para la protección de los datos personales de los usuarios de estas plataformas, distinguiendo, entre otros:

- La dificultad para eliminar el perfil y cancelar los datos personales.
- La indexación de la información personal por motores de búsqueda.
- El rastreo por terceros de los datos personales que quedan expuestos públicamente en la red social.
- La obtención, cruce, enlace de la información personal por terceros para obtener perfiles diferentes al deseado y creado por la propia persona.
- La facilidad con la que terceros se pueden apropiar ilícitamente de la identidad de la persona, lo que escapa al control de cada uno si no es usuario de la red social y no le avisan de ello. La suplantación de la identidad tendrá intención bien de dañar a la propia persona o a un tercero. Para cuando la denuncia se presenta el abuso está ya cometido.
- La utilización comercial de nuestros datos personales, para enviar publicidad no deseada de manera personalizada al usuario.

(16) MIRALLES, Ramón, «Uso y abuso de las redes sociales», en *Curso de verano sobre Redes sociales: ¿autocontrol o descontrol de la privacidad en internet?*, Universidad de Barcelona, 6-10 de julio de 2009.

(17) 30.^a Conferencia Internacional de Autoridades de Protección de Datos y privacidad, Resolución sobre la protección de la privacidad en los servicios sociales, Estrasburgo, 15-17 de octubre de 2008.

- La descontextualización de la información personal del usuario, que amenaza la privacidad del individuo y su derecho a la protección de datos personales.

Puede decirse que estos riesgos no son los únicos ni los más frecuentes para los usuarios, porque al conflicto que enfrenta a la protección de datos personales con las redes sociales, deben sumarse también la problemática con el derecho a la intimidad, el honor y la propia imagen, el enfrentamiento con el secreto de las comunicaciones, la posible vulneración de la producción y creación artística, literaria y científica.

Desde este estudio se pretende realizar una aproximación detallada a los posibles inconvenientes y problemas que implican los servicios de las redes sociales para los derechos de las personas, que permita identificar concretas situaciones de riesgo, y ofrezca una perspectiva real de las dificultades a las que se enfrentan los usuarios de redes sociales. En efecto, siguiendo la evolución que desde el Estudio de la AEPD e INTECO se propone para analizar la problemática jurídica que encierran las redes sociales, el momento mismo del registro como usuario de estas plataformas ya presenta inconvenientes. Con carácter general, se señala que en estos formularios se demanda excesiva información, que no es necesaria para acceder al servicio, y no se informa al usuario de su carácter no obligatorio. En otras ocasiones, además, la información personal que se solicita afecta a aspectos esenciales de su personalidad y se trata por ello de información sensible.

En otro orden de consideraciones, las plataformas trasladan al usuario la responsabilidad y decisión sobre el grado de privacidad que se concederá al perfil creado a partir de dicha información personal, circunstancia que obligará al usuario a configurar un grado máximo de privacidad de sus datos, sin olvidar que desde las redes sociales, por defecto, se establece el grado máximo de publicidad para los datos que integran el perfil personal del usuario. Y si valoramos los diferentes estudios e informes que analizan el comportamiento de los usuarios de redes sociales, se concluye que son mayoría quienes al registrarse no cambian la difusión del perfil que las redes sociales configuran por defecto (18). En relación con las redes sociales, tal y como apunta SANDOVAL MARTÍN, la solución al problema de la intimidad en el nuevo entorno debe centrarse en la búsqueda de un equilibrio entre la redefinición de los derechos tradicionales y las posibilidades de su realización y tutela en el nuevo marco tecnológico, las nuevas amenazas y las actuales exigencias de protección (19).

(18) Por todos, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS E INTECO, *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*, Madrid, 2009.

(19) SANDOVAL MARTÍN, María Teresa, «La red: el nuevo mercado de la vida privada», *Ambitos*, n.º 5, 2000, pp. 154-155.

Llegados a este punto, no puede ignorarse que los riesgos y amenazas afectan especialmente a determinados colectivos de usuarios más vulnerables al impacto de las redes sociales, es el caso de los menores de edad. La particular incidencia que para los derechos de los menores presentan las redes sociales se halla condicionada entre otros por dos factores, a saber: por un lado, la soledad y frecuencia de sus accesos y por otro, la errónea creencia de considerar que nada escapa a su control y que la mayor difusión de su vida privada les acercará a más usuarios y les hará más originales y populares en la comunidad virtual.

En este sentido, no puede ignorarse que la funcionalidad de estas plataformas, en las que el usuario comparte sus fotos, experiencias o eventos con otros usuarios (20), favorece que se difunda información personal de terceros, por lo que se debe actuar con cautela y prudencia por los usuarios. Se aconseja que antes de dicha publicación se informe a los afectados, y pueda obtenerse su consentimiento informado. La AEPD ya se ha pronunciado a este respecto, al advertir que la captación y publicación de imágenes de terceros en tales plataformas sin el consentimiento de la persona vulnera el derecho a la protección de datos, y exige garantizar el derecho de cancelación frente al responsable respecto de datos personales facilitados por terceros sin consentimiento (21).

Constituye igualmente un riesgo para los derechos de la persona, la indexación automática de los perfiles de usuarios por motores de búsqueda, lo que permite el acceso a los datos personales que constituyen el perfil por terceras personas ajenas a la propia red social, y a ello debe sumarse igualmente, la amenaza que representa la instalación de cookies en el equipo del usuario, sin su conocimiento. Estas controvertidas cuestiones serán objeto de detenido análisis cuando abordemos en próximos epígrafes la polémica que enfrenta a las redes sociales y la protección de datos personales.

Ofrece importantes incertidumbres jurídicas desde la perspectiva de la protección de datos personales en las redes sociales, la denominada publicidad contextual o personalizada, que precisa del tratamiento de datos personales de los usuarios, y que adquiere especial relevancia en el caso de las redes sociales. Constituye igualmente otra actuación ilícita frecuente en estas plataformas el envío de comunicaciones comerciales no deseadas a partir de actuaciones abusivas en las redes sociales mediante la creación de perfiles falsos que actúan de reclamo para los usuarios o

(20) Según revela un reciente Estudio de INTECO, el 52.9 % de los usuarios encuestados manifestó que accedía a las redes sociales para compartir fotos y el 45.7 % para enviar mensajes públicos. Véase OBSERVATORIO DE SEGURIDAD DE LA INFORMACIÓN (INTECO), *Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles (10.º Oleada) Tercer Trimestre, 2009*.

(21) Véase RESOLUCIÓN R/01712/2009, de 20 de julio de 2009.

a partir de la creación de grupos sobre intereses comunes, o mediante la utilización de aplicaciones que permiten acceder automáticamente a la libreta de direcciones de contacto de los usuarios.

Pueden aparecer situaciones comprometidas para el usuario en el momento de cancelar la cuenta y darse de baja del servicio; en este caso, la problemática más habitual será la dificultad del procedimiento de cancelación, y las indicaciones poco explícitas o confusas del servidor, que pueden inducir al usuario a error sobre aspectos tan importantes como la finalidad y los períodos de conservación de sus datos personales por la red social. Debemos recordar, que conforme a la normativa española, la conservación de los datos personales generados en las comunicaciones y la posibilidad de acceso a informaciones muy útiles para las empresas, no se acomoda a la legislación actual y conculca el principio de calidad de los datos personales que sólo se conservarán mientras se mantenga la relación entre el usuario y la plataforma.

Coincidimos con DUMORTIER cuando señala como un importante factor de riesgo la descontextualización de la información en las redes sociales, cuyo origen se encuentra, a juicio del autor, en la simplificación de las relaciones sociales, la amplia difusión de la información y los efectos de globalización y normalización de las redes sociales (22). Siguiendo las reflexiones de este autor, incrementar la responsabilidad del usuario de redes sociales, imponiéndole obligaciones propias de un controlador de datos no se corresponde con los niveles de conciencia y conocimientos propios de los usuarios sobre sus derechos y obligaciones, y así, propone diseñar las estructuras de las redes sociales de modo que eviten cualquier interferencia con la privacidad y la protección de datos, siempre que no sea estrictamente necesario conforme las normas propias de un Estado democrático.

Y por último, como actuaciones especialmente perjudiciales para los usuarios deben citarse la suplantación de identidad del usuario (23), las actuaciones de acoso en la red y el grooming, o acoso de contenido sexual que ejerce un adulto sobre menores de edad. Ahora bien, como subraya TRONCOSO REIGADA es imprescindible no ofrecer una imagen

(22) DUMORTIER, Franck, «Facebook y los riesgos de la “descontextualización” de la información», *Revista de Internet, Derecho y Política*, n.º 9, 2009, pp. 25-41.

(23) Así ha sucedido en Gran Bretaña donde una persona fue condenada por los tribunales de este país a pagar una indemnización de 21.500 euros, por difamar a un antiguo compañero de colegio, al que suplantó la personalidad en Facebook, utilizando sus datos personales y fotografías, pero incluyendo en su perfil datos falsos. Véase <http://elmundo.es/navegante/2008/07/24/tecnologia/1216919445.html>. Más recientemente, en España un joven fue detenido por suplantar la identidad de un compañero de clase en Tuenti, lo que le permitió insultar, en su nombre, a otros usuarios de la red, con lo que consiguió, provocar desprestigio y enemistad en la red hacia el joven denunciante, a quien había suplantado en su identidad. Véase <http://www.europapress.es/extremadura/badajoz-00380/> (Fecha de consulta: 03/03/2010).

negativa de las redes sociales, que resultaría contradictoria con el esfuerzo de las instituciones por generalizar y promocionar el acceso de los ciudadanos a las nuevas tecnologías, se trata de reconocer e identificar los riesgos y amenazas y ofrecer respuesta ante los posibles conflictos que puedan plantearse (24).

Y en este contexto, en el que se dibuja un fenómeno acuciado por la desconfianza y el recelo de las instituciones, y en menor medida de los usuarios, se enmarca la propuesta de las administraciones de acoger la autorregulación como mecanismo de protección de los derechos de los usuarios en las redes sociales. En efecto, los códigos de conducta y las condiciones de uso representan una valiosa herramienta para prevenir y encauzar posibles conflictos en el uso de estos servicios, al tiempo que ofrecen un importante respaldo a las propias redes ante usos ilícitos y abusivos por los usuarios. Así lo expresa PÉREZ SAN JOSÉ cuando sostiene que los códigos de conducta constituyen un elemento de autorregulación fundamental para el desarrollo seguro y confiable de los servicios de internet y la privacidad y seguridad de sus usuarios (25).

IV. Protección de datos personales en las redes sociales

Sin ánimo de inquietar al lector más allá de lo necesario, el panorama anteriormente descrito permite concluir, a juicio de algunos autores, que la normalización y globalización de las redes sociales ha favorecido la revisión y redefinición de los derechos fundamentales de la persona, que deben contemplarse ahora desde la realidad tecnológica que representan internet y las novedosas aplicaciones de las redes sociales (26). Y ciertamente, así parece, la irrupción de la web 2.0 ha establecido nuevos hábitos de conducta entre los ciudadanos, ha generado nuevas necesidades entre los usuarios y ha forzado la necesidad de interpretar los derechos de las personas desde los nuevos parámetros que las tecnologías perfilan. Aún siendo esto cierto, la realidad demuestra que ha sido el propio usuario quien, en un intento por no quedar rezagado ante el avance tecnológico y perderse las nuevas herramientas que ofrece, ha establecido y redefinido los derechos que el ordenamiento jurídico le reconoce. Y así,

(24) TRONCOSO REIGADA, Antonio, «Las redes sociales y la APDCM», *Datospersonales.org*, n.º 43, 2010.

(25) PEREZ SAN JOSÉ, Pablo, «La autorregulación como instrumento para la protección de la privacidad y de la seguridad en las redes sociales», *Revista datospersonales.org*, n.º 43, 2010.

(26) ABRIL I ABRIL, Amadeu, «Redes sociales, Web 2.0 y la desaparición del espacio privado», en *Redes sociales: ¿autocontrol o descontrol de la privacidad en internet?*, Barcelona, 6-10 de julio de 2009.

se pretende construir una identidad digital, que compartimos en la red social voluntariamente con los demás, a quienes deseamos hacer partícipes también de nuestras experiencias, sentimientos, logros o decepciones. Por ello, nunca antes las relaciones sociales y profesionales fueron tan visibles e interactivas. Nunca antes el ser humano había renunciado de manera libre y voluntaria a tantas parcelas de su vida privada.

No debe extrañar, por tanto, que la problemática que envuelve a las redes sociales centre la atención de los juristas, que pretenden explicar y analizar esta nueva forma virtual de relación a partir de los principios y criterios jurídicos que conforman y reconocen los derechos fundamentales de la persona. En especial, el conflicto que suscita el ejercicio del derecho a la protección de datos personales en las redes sociales ha animado el debate doctrinal, y ha impulsado el celo de las instituciones, que vigilan y observan a las redes sociales con la firme pretensión de garantizar el cumplimiento de la normativa existente, y velar por los derechos de los usuarios. Y a este intenso e interesante debate jurídico en torno a los datos personales y su tratamiento en las redes sociales pretendemos sumarnos desde este estudio, con las consideraciones que a continuación se presentan.

1. Marco legal europeo de protección de datos personales

Desde la aprobación del Convenio 108 del Consejo de Europa, que define los principios básicos de protección de datos personales, reconoce los derechos que constituyen el contenido esencial de la protección de datos y delimita los procedimientos para la tutela de este derecho, la evolución tecnológica ha forzado la revisión de sus fundamentos, y ha obligado a las instituciones a renovar sus esfuerzos para una efectiva tutela de los datos personales.

En el ámbito de la Unión Europea, el reconocimiento explícito del derecho a la protección de datos se contempla en el artículo 8 de la Carta Europea de Derechos Fundamentales, que establece un tratamiento leal de los datos para fines concretos que se sustenta en el consentimiento de la persona afectada o en virtud de un motivo legítimo; se reconoce igualmente el derecho de acceso y rectificación a la información que nos concierne, y se distingue a las autoridades independientes como entidades de control del cumplimiento de la legislación vigente (27).

Por su parte, la adopción de la Directiva 95/46/CE de 24 de octubre relativa a la protección de las personas físicas en lo que respecta al trata-

(27) Carta de los Derechos Fundamentales de la Unión Europea, Doc. C 364/5, de 18 de diciembre de 2000.

miento de datos personales y a la libre circulación de estos datos, facilitó la armonización y adaptación por los Estados miembros de sus legislaciones en materia de protección de datos personales, y se alza como marco normativo que garantiza el necesario equilibrio que debe presidir la relación entre la libre circulación de datos personales y la tutela de la vida privada de los ciudadanos en la Unión Europea.

Una primera cuestión que debe resolverse en el marco de la normativa comunitaria, es el ámbito subjetivo de aplicación, que tal y como dispone el artículo 4 de la citada Directiva 95/46/CE, será aplicable a todo tratamiento de datos personales cuando: primero, el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro; segundo, el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público; y tercero, el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.

Toda vez que se han establecido los criterios de aplicación de la norma, resulta fundamental señalar los principios más destacados sobre los que se configura en la norma comunitaria la protección de datos personales, y a estos efectos, destaca el principio de calidad de los datos, por el cual éstos deberán ser adecuados, pertinentes y no excesivos en relación con la finalidad para la que serán tratados, circunstancia que las redes sociales deben observar principalmente en el cuestionario inicial de registro del usuario.

Así mismo, y salvo los motivos legales descritos en la norma, el tratamiento de la información personal precisa el consentimiento previo del titular de los datos, y en este punto, deberán observarse los requisitos por los cuales se entiende prestado válidamente dicho consentimiento.

La tutela efectiva de este derecho se encuentra directamente vinculada a la garantía de los diferentes derechos que la norma reconoce a los ciudadanos: el derecho de acceso, rectificación, cancelación y oposición en relación con la información personal que les concierne. Abundando en lo expresado, debe asegurarse que los datos personales comunicados por un usuario al registrarse en una red social deberán cancelarse cuando el usuario o la propia red decidan suprimir la cuenta, y lo mismo debe afirmarse cuando el usuario actualiza la información personal de su perfil. En este sentido, el Grupo de Trabajo del Artículo 29 sugiere que las redes sociales automáticamente desactiven un perfil que dejará de ser visible si el usuario no ha accedido al servicio durante un tiempo determinado, y pos-

teriormente, y de forma definitiva, se cancelen los datos de la cuenta, informando previamente a los usuarios de estos procesos y de los períodos de tiempo establecidos a tales efectos (28).

A estos principios básicos de protección de datos, se debe sumar el de seguridad del tratamiento, de suerte que se arbitren medidas técnicas y normativas, de ámbito supranacional, adecuadas al avance y desarrollo de las aplicaciones tecnológicas y que garanticen la tutela de los derechos de los usuarios. A este respecto, se ha señalado en la 31.^a Conferencia de Autoridades de Control celebrada en Madrid en 2009, la necesidad de elaborar estándares internacionales de protección de datos, entre los que destacan los relativos a las denominadas «medidas proactivas», orientadas a garantizar técnica y jurídicamente el cumplimiento de la normativa de protección de datos personales (29).

Ciertamente, la solución no puede hallarse en políticas legislativas internas o nacionales, antes bien al contrario, se deben alcanzar unos estándares internacionales compartidos que garanticen una eficaz protección universal de los derechos de los usuarios; en este estado de cosas, destaca la Comunicación sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) de 2007 que realizó la Comisión al Parlamento Europeo (30), y por la cual se recomienda la tutela de los derechos de protección de datos e intimidad de los usuarios, mediante herramientas tecnológicas denominadas «PET». Se trata de sistemas tecnológicos destinados a reducir y, en su caso, eliminar la incidencia de las nuevas tecnologías de la información sobre los derechos de protección de datos e intimidad de los usuarios.

Entre otras destacan como medidas la disociación o «anonimización» automática de los datos, que serán almacenados en un formato que permita identificar al interesado únicamente durante el tiempo necesario para la consecución de las finalidades para las que fueron obtenidos inicialmente, el uso de instrumentos de cifrado que impidan el acceso no autorizado a la información transmitida a través de Internet, el uso de anuladores de «cookies», que impiden que el sitio web pueda instalar en los equipos de los usuarios ficheros que, de forma automática y sin que

(28) GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 5/2009 sobre las redes sociales en línea, adoptado el 12 de junio de 2009, Doc. WP 163.

(29) 31.º CONFERENCIA DE AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD, Propuesta conjunta para la redacción de Estándares Internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal, Madrid, 2009. https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf (Fecha de consulta: 21/03/2010).

(30) COMISION DE LAS COMUNIDADES EUROPEAS, Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad, COM (2007) 228 final, de 2 de mayo de 2007.

el usuario lo conozca, recopile toda la información estadística y relativa a los accesos que el usuario lleva a cabo durante su navegación, la Plataforma de Preferencias de Privacidad (P3P), que permite a los usuarios analizar y comparar políticas de privacidad de los sitios web que visita, mediante un informe sobre la adecuación de éstas a la normativa aplicable, y finalmente, los sistemas de gestión de identidad, que permiten el control por parte de los usuarios de los datos que revelan sobre sí mismos en cada transacción, como los promovidos por el proyecto PRIME (Privacy and Identity Management for Europe).

En el ámbito de las redes sociales, el Memorando de Roma de 2008 (31) constituye una referencia fundamental para comprender la necesidad de adaptar las normativas nacionales al fenómeno de las redes sociales; y así, se definen las obligaciones para los prestadores de servicios y un conjunto de recomendaciones a los legisladores, entre las que destacan:

- Derecho a uso del seudónimo.
- Asegurar que los proveedores de servicios de redes sociales son honestos y transparentes en la información que ofrecen al usuario.
- Establecer la obligación de notificar cualquier riesgo para la protección de datos personales.
- Proveer una mayor responsabilidad a los proveedores sobre el tratamiento de datos en la red.
- Introducir en la educación y formación de los más jóvenes una mayor conciencia sobre la privacidad y su protección.

Por otra parte, en su Dictamen 5/2009 sobre las redes sociales el Grupo de Trabajo del Artículo 29 reflexiona a propósito de la exención doméstica en el tratamiento de datos personales de terceros, situación habitual entre los usuarios de las redes sociales (32). A este respecto, se señala en el citado Dictamen que no es posible aplicar esta exención, por ejemplo, en el caso de plataformas con fines comerciales, políticos o sociales, tampoco cuando se accede a un gran número de contactos, o cuando los datos son indexados por motores de búsqueda. Abundando en lo expresado, se considera que la aplicación de la exención doméstica se halla limitada por la necesidad de garantizar los derechos de los terceros, especialmente en lo que se refiere a los datos sensibles, y en cualquier caso, el usuario podrá ser responsable en virtud de las disposiciones generales del derecho civil o penal nacional de que se trate.

(31) International Working Group on Data Protection in Telecommunications, Report and Guidance on Privacy in Social Network Services «Rome Memorandum», 43rd meeting, 3-4 March 2008, Rome (Italy).

(32) GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 5/2009 sobre las redes sociales en línea, adoptado el 12 de junio de 2009, Doc. WP 163.

Por último, especiales dificultades plantea el ejercicio de los derechos de protección de datos personales por quienes no son usuarios de los servicios de redes sociales, en estos supuestos resulta esencial garantizar los derechos de acceso, rectificación o cancelación de los datos, por ello, se apunta desde el Dictamen 5/2009 del Grupo de Trabajo del Artículo 29 que los servicios de redes sociales deben disponer en su página de inicio de información sobre la existencia de una «oficina de reclamación» que permita gestionar los conflictos relativos a la protección de datos y la intimidad, así como las denuncias de usuarios y no usuarios ante actuaciones ilícitas o abusivas.

Claro que como se anunciaba desde la Comisión Europea, queda mucha labor por delante, y si bien se reconocían los avances, igualmente se apuntaban carencias significativas en la seguridad de las redes sociales, de suerte que algunas medidas importantes en relación con los menores aún no han sido aplicadas por las redes sociales. Se denunciaba que menos de la mitad de las entidades firmantes del Acuerdo Europeo para mejorar la seguridad de los menores que utilizan redes sociales, establece por defecto para los menores perfiles visibles sólo para sus amigos, y únicamente la mitad de los sitios evaluados garantiza que los menores no son objeto de indexación a través de los motores de búsqueda, en tanto que 9 de los 22 sitios de redes sociales ofrecía respuesta a las denuncias presentadas por menores de pedir ayuda (33).

2. Normativa española de protección de datos personales y su aplicación a las redes sociales

No siempre el derecho a la protección de datos personales gozó en el ordenamiento jurídico español de la consideración que como derecho fundamental en la actualidad ningún jurista cuestiona. En efecto, no será hasta la célebre STC 202/2000 cuando el Tribunal Constitucional español ponga fin a un dilema que hasta entonces había ocasionado una encendida y permanente polémica entre la doctrina española, y delimite la estrecha línea que separa y diferencia el derecho a la intimidad y el derecho a la protección de datos personales, estableciendo explícitamente su configuración como un derecho fundamental. Y así, de acuerdo con las consideraciones del Alto Tribunal expresadas en la citada sentencia, la protección de datos personales «[...] alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado, porque así lo ga-

(33) Así se expresaba desde la Comisión Europea el 2 de febrero de 2010, Día de internet segura. http://ec.europa.eu/information_society/activities/sip/index_en.htm (Fecha de consulta: 12/03/2010).

rantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo».

A tenor de lo expresado por el TC, cabe recordar que de acuerdo con las previsiones legales, se considera dato de carácter personal «cualquier información concerniente a personas físicas identificadas o identificables», sea esta información «numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas», tal y como se desprende del artículo 5.1.º del RD 1720/2007 de 21 de diciembre.

En el ámbito de las redes sociales, la identificación de la persona es un proceso sencillo, a la considerable información personal que el propio usuario comparte al abrir la cuenta y generar su perfil, se suma la dirección IP como dato personal, que permite segmentar y contextualizar la publicidad que se ofrece a cada tipo de usuario. A este respecto, el informe 327/03 de la AEPD concluyó que la dirección IP constituye dato de carácter personal, al que hay que aplicar medidas de seguridad de nivel básico. Ha alcanzado la AEPD esta conclusión a partir de las siguientes consideraciones: en primer lugar, los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios a los que han asignado direcciones IP; en segundo lugar, con la asistencia de terceras partes responsables de la asignación de la dirección IP se puede identificar a un usuario de Internet por medios razonables; y en tercer lugar, existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo (34).

Ahora bien, son numerosos y significativos los datos personales que en ocasiones voluntariamente, y en otras, inconscientemente, los usuarios transfieren a las plataformas para su tratamiento y cesión. Es por ello, que debe exigirse a la red social la redacción de pautas claras y principios concretos que permitan a los ciudadanos, antes de registrarse

(34) De este modo lo ha interpretado también el Grupo de Trabajo del Artículo 29, al afirmar que «los proveedores de acceso a internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de internet a los que han asignado direcciones IP pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de internet», GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DE DATOS DEL ARTÍCULO 29, Dictamen 4/2007 sobre el concepto de datos personales, de 20 de junio, Doc. 1248/07/ES WP 136. Véase Informe AEPD 327/2003 en https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Caracter-de-dato-personal-de-la-direcci-oo-n-IP.pdf (Fecha de consulta: 07/03/2010).

como usuarios, identificar su política de privacidad y valorar su acomodación a la normativa vigente en protección de datos personales. Así lo vienen demandando las diferentes instituciones y Autoridades de control, que como en el caso de la AEPD, mantienen contactos periódicos con los responsables de las redes sociales, y se esfuerzan por impulsar acuerdos y compromisos que garanticen la adopción de medidas de control y protocolos de actuación en defensa de los derechos de los usuarios, y aseguren la acomodación de su funcionamiento a la normativa española.

En España, la regulación sobre protección de datos de carácter personal en el sector privado se configura a partir de dos normas principalmente: la citada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RDLOPD); ello no obstante, también resultan aplicables a las redes sociales la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico (en adelante LSSI-CE), la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y la Ley 25/2007, de 18 de octubre, de Conservación de Datos relativos a las Comunicaciones electrónicas y a las Redes Públicas de Comunicaciones.

Significar en primer lugar que de acuerdo con lo dispuesto en el artículo 4 de la LSSI-CE se exige el cumplimiento de las obligaciones establecidas en la propia Ley, para todo prestador de servicios de la sociedad de la información:

- Que se encuentre establecido en España, entendiéndose por tal cuando su residencia o domicilio social se localice en territorio español, y siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios
- Que aunque se encuentre establecido en otro Estado, ofrezca sus servicios a través de un establecimiento permanente situado en España, considerándose a tal efecto que así opera cuando se dispone en territorio español de forma continuada o habitual, de instalaciones o lugares de trabajo en los que se realice toda o parte de su actividad
- Que aunque se aloje y pertenezca a servidores externos a la Unión Europea, oriente sus servicios específicamente al territorio español, siempre que ello no sea contrario a los convenios internacionales aplicables. En este sentido, se ha manifestado la AEPD que ha afirmado su competencia para aplicar esta normativa a prestadores de servicios establecidos fuera de la Unión Europea en la prestación del servicio del correo electrónico gratuito (35).

(35) Doc. Expediente E/01544/2007.

- Que aunque se encuentren establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo, se les aplicará la LSSI-CE a efectos de la libre prestación de los servicios y sobre colaboración de los prestadores de servicios de intermediación para interrumpir el servicio o retirar determinados contenidos cuando lo haya declarado un órgano español competente.

Determinadas las circunstancias legales por las cuales un prestador de servicios de la sociedad de la información se someterá a la normativa española, debe llamarse la atención sobre una circunstancia que ha provocado no pocos conflictos y suspicacias jurídicas entre los responsables de las redes sociales y las instituciones, a saber: alguna de las redes sociales con mayor expansión en España radica en Estados Unidos, y no dispone de relación con nuestro país, lo que complica la aplicación de la normativa nacional vigente a dichas redes sociales en España y despierta el recelo de las Instituciones que les reclaman, como en el caso de la AEPD, el cumplimiento de la normativa española. Por ello, hemos de felicitarlos por algunos de los avances que en las últimas fechas se vienen produciendo en el entorno de las redes sociales y su marco legal, y que han llevado, por ejemplo, a Facebook a elevar la edad para acceder a sus servicios y acomodarla a las normas españolas, o que han significado el establecimiento de protocolos o controles de verificación de edad de los usuarios de redes sociales.

Desde la perspectiva de la legislación española de protección de datos personales, todo tratamiento de datos de carácter personal debe atender a unos fundamentos generales, que pueden resumirse en los siguientes principios:

- A) Los datos personales objeto de tratamiento deben ser adecuados, pertinentes y no excesivos, en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, no pudiendo usarse para finalidades incompatibles con aquellas para las que los datos se recabaron. Los datos deberán responder a la situación actual del interesado, siendo rectificados si se constatan errores. Podrá prohibirse la recogida de datos por medios fraudulentos, desleales o ilícitos, y sólo se podrán conservar los datos personales mientras subsista la finalidad por la que se recabaron.
- B) Se informará al usuario previamente a la obtención del consentimiento para el tratamiento de los datos personales, consentimiento que deberá ser libre, inequívoco, específico e informado.
- C) Quienes procedan a almacenar, tratar y acceder a ficheros de datos de carácter personal, se hallan obligados a adoptar medidas de seguridad técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información.

- D) Los datos personales objeto del tratamiento sólo podrán ser comunicados a un tercero, para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario previo consentimiento del interesado.

En la disyuntiva que enfrenta a las redes sociales y la protección de datos personales de sus usuarios, ha diferenciado la AEPD tres momentos críticos para la tutela de la información personal, a saber: un primer momento, en el registro para el acceso a la red social; un segundo momento, cuando el usuario despliega su actividad en la plataforma y utiliza las aplicaciones y servicios que se le ofrecen; y por último, un tercer momento cuando el usuario decide cancelar su cuenta y darse de baja del servicio de la red social. Siguiendo este esquema propuesto por la AEPD e INTECO en el citado Estudio sobre privacidad de los datos personales, procederemos a realizar un análisis de los aspectos más controvertidos de la protección de datos personales en las redes sociales.

En un primer momento, el del registro de acceso del usuario, la exigencia legal impone a los prestadores de servicios de redes sociales el principio de calidad de los datos personales que se solicitan, que no deben ser excesivos ni desproporcionados. Ahora bien, conforme a lo dispuesto en el art. 7 LOPD se reclama la prestación de un consentimiento expreso y por escrito para la obtención de datos personales relativos a ideología, religión o creencias, y expreso en el caso de datos personales de salud, origen racial y vida sexual. Por ello, no se podrán tratar datos sensibles sin consentimiento explícito de los interesados, y si en un formulario de registro se introducen cuestiones relativas a datos sensibles se debe indicar claramente que la respuesta es totalmente libre y voluntaria.

En este momento, tiene un protagonismo esencial la política de privacidad diseñada desde la red social, que ha de ser clara, legible y comprensible por el usuario y que debe delimitar, según exigencias legales, las finalidades para las que se recaban y tratan los datos personales. En este sentido, resultan de especial interés las conclusiones de la Encuesta del CIS sobre protección de datos personales, en la que un 35% de los encuestados manifestaba que nunca leía dicha política, un 27% reconocía que raramente lo hacía, y finalmente, un 5% de usuarios confesaba no saber cómo hacerlo (36). Igualmente, deberá informarse de posibles cesiones de datos personales a terceros y de cuantas transferencias internacionales estén previstas, así como de la finalidad de las mismas, y del derecho del interesado a oponerse.

En un segundo momento, cuando el usuario despliega su actividad en la plataforma y utiliza las aplicaciones y servicios que se le ofrecen ad-

(36) CIS. Encuesta 2009 sobre protección de datos. Véase http://datos.cis.es/pdf/Es28/2mar_A.pdf

quiere especial relevancia el tratamiento de datos personales ajenos, lo que puede significar en algunos casos tratamiento y difusión pública de datos personales de terceros que no han prestado su consentimiento. Siguiendo en este punto las reflexiones de ACED FELEZ, además del proveedor también quien introduce los datos personales deberá actuar con la suficiente prudencia para contrastar que la persona no se molestará o bien estará de acuerdo con dicho tratamiento. Coincidimos con el autor en afirmar que será difícil que pueda calificarse este uso como uso doméstico de la información personal, porque ésta no se comparte sólo ni exclusivamente con una comunidad cerrada de antemano conocida y excluyente, máxime si se considera la posibilidad de indexación de los perfiles personales por motores de búsqueda (37).

Claro que es frecuente también que los servicios de redes sociales permitan a los usuarios proporcionar datos sobre terceros no usuarios de la red social, si bien como señala el Grupo de Trabajo del Artículo 29 el tratamiento de estos datos personales sólo será lícito si se cumplen los criterios previstos en el artículo 7 de la Directiva de protección de datos; rechaza el Dictamen 5/2009 la posibilidad de que sea lícito este tratamiento aun cuando desde la red social se comunicasen con el no usuario para informarle de dicho tratamiento e invitarle a adherirse a la red social, no en vano mediante esta práctica se vulneraría lo dispuesto en el artículo 13.4 de la Directiva sobre privacidad y comunicaciones electrónicas relativo al envío de comunicaciones no solicitadas con fines publicitarios.

Así mismo, la instalación de cookies y otros dispositivos para almacenar información del usuario y su navegación son prácticas habituales en las redes sociales. Estos sistemas permiten que pueda obtenerse de forma automática información relativa al lugar del acceso, al dispositivo empleado para dicho acceso, al tipo de contenidos a los que se accede, así como al tiempo empleado en el acceso. Las políticas de privacidad de las plataformas si bien informan sobre su utilización y el derecho a eliminarlas, los términos que emplean no son siempre claros ni precisos, e intencionadamente en ocasiones inducen al usuario a estimarlas imprescindibles para la óptima utilización de los servicios, por lo que en la práctica el usuario no se aventurará a bloquear ni eliminar las cookies (38). En este sentido, tal y como se ha puesto de manifiesto, resulta

(37) ACED FÉLEZ, Emilio, «Las redes sociales: nueva frontera para la privacidad de los *digital babies*», en *Seminario Seguridad en redes sociales: ¿están nuestros datos protegidos?*, Escuela Universitaria de Ingeniería Técnica de Telecomunicaciones, Universidad Politécnica de Madrid, 2009.

(38) «Utilizamos “cookies” (datos que almacenamos en tu ordenador, teléfono móvil u otro dispositivo Durante un período de tiempo prolongado) para que sea más fácil de usar en Facebook, para que nuestra publicidad sea mejor y para Proteger tanto a ti como a Facebook. Por ejemplo, las empleamos para guardar tu nombre de usuario (pero nunca tu contraseña) de modo que te resulte más sencillo iniciar sesión cada vez que quieras entrar en Facebook. También Utilizamos las

de especial utilidad la dirección IP desde la que el usuario se conecta, y que ha sido considerada por la AEPD dato de carácter personal, habida cuenta que puede vincularse a una persona identificable (39).

A propósito de la conservación de datos personales, a tenor de lo dispuesto en el artículo 2 de la Ley 25/2007, cuando los proveedores de servicios de redes sociales ofrezcan servicios de comunicación electrónica tales servicios quedarán sujetos a las normas de la citada Ley sobre conservación de datos personales.

En otro orden de consideraciones, las redes sociales, como ya ha sido apuntado, presentan un sistema viral de expansión, de suerte que el acceso y registro como usuario suele venir precedido de invitaciones previas que se cursan a determinados contactos, bien personalmente por el propio usuario o bien automáticamente a través de la propia plataforma. Y este proceso, en el que se sustenta el crecimiento de la red social, constituye una cuestión especialmente polémica a propósito del tratamiento y utilización de datos personales de terceros sin su consentimiento para el envío de comunicaciones comerciales no solicitadas. Claro que la prohibición de utilizar el correo electrónico con fines de comercialización no resultará aplicable a las comunicaciones personales, si bien para que esta excepción sea aplicable no se debe incentivar al remitente ni al destinatario desde la propia red social, no debe seleccionar el proveedor a los destinatarios del envío, la identidad del remitente debe quedar claramente identificada, el remitente debe conocer el contenido total del mensaje que se enviará en su nombre y no pueden enviarse invitaciones de forma indiscriminada a toda la relación de contactos de un usuario.

Así también se desprende de las consideraciones recogidas en una reciente Resolución de la AEPD, en la que esta institución se pronuncia a propósito del envío masivo de correos electrónicos de promoción con ocasión de un sorteo de entradas para asistir a un evento, en el que el usuario debía introducir su correo electrónico y el de sus contactos personales para participar (40). Siguiendo las argumentaciones de la AEPD puede concluirse que:

- 1.º Los correos electrónicos tienen la consideración de comunicación comercial recogida en el Anexo f) de la LSSI-CE, cuando mediante los mismos se promociona un producto, un evento o un servicio.

“cookies” para confirmar que estás conectado a Facebook, y para saber cuándo estás interactuando con aplicaciones y sitios web de la plataforma de Facebook, nuestros reproductores, de botones y compartir nuestros anuncios. Puedes eliminar o bloquear las cookies mediante la configuración de tu navegador, pero en algunos casos puede influir en tu capacidad de uso de Facebook». Véase <http://www.facebook.com/policy.php>

(39) Así lo expresa la AEPD en su Informe 327/2003. Carácter de dato personal de la dirección IP.

(40) RESOLUCIÓN AEPD R/01719/2009, de 14 de septiembre de 2009.

- 2.º Si bien la obtención de las reseñadas direcciones de correo electrónico se produce a partir de terceros ello no habilita para usarlas en la remisión de comunicaciones promocionales si no se da cumplimiento a lo previsto en el artículo 21 de la LSSI.
- 3.º Si la LSSI-CE ha querido imponer una formalidad específica que permita a los destinatarios de los envíos oponerse al tratamiento de sus datos para el envío de mensajes publicitarios por correo electrónico, a fin de garantizar su derecho a no recibir comunicaciones de naturaleza comercial, que el prestador de servicios no ofrezca un procedimiento sencillo y gratuito para ello conculca la obligación legal establecida en la LSSI.
- 4.º Se exige una especial diligencia a las entidades prestadoras de los servicios cuando se envían comunicaciones comerciales por medios de comunicación electrónica, y dicha diligencia falta desde el momento en que se remiten a una multitud de destinatarios un mismo mensaje comercial de contenido publicitario sin comprobar, por un lado, que los destinatarios del mismo hubieran solicitado la publicidad remitida o hubieran consentido la utilización de su correo electrónico para dicho fin ni constatar, por otro lado, si tenían la condición de clientes de la entidad en los términos recogidos en el artículo 21.2 de la LSSI-CE.
- 5.º El hecho de que no se reciban quejas por el envío de los mensajes promocionales, tanto durante como después de la campaña, ni que a la denuncia se acompañe el soporte de alguna reclamación concreta, o la falta de interposición de denuncia ante la Agencia por alguno de los destinatarios de los correos comerciales no anula la obligación de dar cumplimiento al requisito previsto en el artículo 21 de la LSSI-CE.

Recapitulando, constituye un importante riesgo para los usuarios la recepción de comunicaciones comerciales no solicitadas; y así, se indican en el Informe de INTECO y la AEPD sobre la privacidad de los datos personales dos prácticas usuales de las redes sociales: por un lado, cuando el propio usuario decide enviar invitaciones a sus contactos para que se registren en las aplicaciones o grupos de la red social y, segundo, cuando se permite que la herramienta o la red social acceda a la libreta de contactos para remitir a todos ellos un correo electrónico animando a que se registren en la red, lo que a juicio de la AEPD, a pesar de la mediación de un usuario, podrá considerarse comunicación electrónica no deseada (41).

(41) Ha declarado la AEPD que: «El envío publicitario que el denunciante manifiesta haber recibido, corresponde a una campaña continua de captación de clientes que promueve el demandado. Dicha campaña consiste en ofrecer a los clientes registrados la posibilidad de recomendar a sus familiares y amigos los servicios de Iniciativas Virtuales a través de la página web, para lo cual existe en

Otro importante riesgo para los usuarios de redes sociales es la indexación automática por motores de búsqueda de sus perfiles, de suerte que los datos y la información personal de los usuarios disponible en la red social puede ser accesible de forma pública en internet. En general, dicha publicidad representa información personal del usuario, su nombre, aficiones, intereses, fotografías, así como el nombre y fotografías de sus amigos o contactos en la red social, de suerte que dichas informaciones no se mantienen de forma cerrada accesibles sólo desde la red social, sino abiertas al conocimiento de terceros. En este contexto, la AEPD ha reconocido a los afectados el derecho de oposición a que sus datos personales sean accesibles desde los buscadores, por entender que constituye un tratamiento de datos personales, que debe respetar la normativa vigente y por tanto, «debe estimarse la procedencia de evitar mediante la estimación de la oposición al tratamiento de los datos, en el caso que así lo solicite el afectado, como en el presente, que el tratamiento por parte de un buscador tenga efectos no deseados con carácter permanente en contra de la voluntad del afectado» (42). Así, lo ha declarado recientemente el Director de la AEPD, al referirse a los efectos multiplicadores de internet en relación con la información personal que los buscadores de internet recuperan de medios de información digitales, y ha instado a estos últimos a reflexionar sobre la trascendencia de mantener de manera permanente una accesibilidad plena de los datos identificativos de personas contenidos en noticias irrelevantes, por lo que ha aconsejado a los medios que empleen medias técnicas que impidan la indexación de noticias por los buscadores de internet, advirtiéndole que ningún ciudadano que no sea persona conocida de relevancia pública «deba resignarse a soportar que sus datos de carácter personal circulen por la red sin poder reaccionar ni corregir la inclusión de los mismos en un sistema de comunicación universal como internet» (43).

Otra conducta cada vez más habitual en las redes sociales es la suplantación de la identidad de los usuarios; y así, personajes populares, políticos nacionales, cantantes o actores han visto circular por las redes sociales falsos perfiles con su identidad, creados en unas ocasiones por enemigos, y en otras, por personas que persiguen un beneficio económico. Además de esta práctica, puede señalarse otra forma de suplanta-

dicha página web una facilidad que permite remitir a una dirección de correo electrónico un mensaje informativo invitando al destinatario a registrarse en ella» (Resolución R/00139/2008, de 20 de febrero de 2008).

(42) Entre otras Resoluciones de la AEPD, Procedimiento TD/00444/2008, de 4 de noviembre de 2008.

(43) ASOCIACIÓN DE PRENSA DE MADRID, Foro «Libertad de expresión vs. Ley de protección de datos», 2010.

ción, que consiste en apoderarse del perfil de una persona e introducir en ella información que la pueda comprometer. Esta última conducta tiene lugar generalmente entre personas del mismo entorno, y se pretende hacer una gracia o burla, o comprometer y exponer a situaciones violentas o incómodas a ex amigos, ex compañeros de trabajo y ex parejas. En el ordenamiento español, la suplantación de identidad está sancionada en el CP en el artículo 401, si bien como señala FERNÁNDEZ BURGUENO, la suplantación de personalidad únicamente es delito si la conducta encaja perfectamente en el tipo penal del citado precepto, esto es, si lo que se usurpa es el estado civil de otro. En este caso, la conducta puede ser castigada con la pena de prisión de seis meses a tres años. Si, por el contrario, lo que se hace es crear un perfil inventado o con datos falsos, la conducta no encajaría en el tipo penal y no podría ser considerada delito; por tanto, el hecho de idear datos falsos para participar en una red social no es constitutivo de delito de usurpación de estado civil. Ahora bien, que la usurpación de identidad hubiera sido o no una broma no exime de responsabilidad criminal a su autor, según dispone el artículo 20 del Código Penal, si bien podría llegar a ser considerada como circunstancia atenuante, en virtud del apartado 6 del artículo 21 del CP (44).

En palabras del citado autor, la forma idónea de defenderse de este tipo de prácticas es mediante acciones preventivas tanto desde un ámbito técnico como desde la actitud del usuario. En este sentido, se lanzan tres recomendaciones básicas al usuario: primera, adoptar contraseñas seguras, alfanuméricas de al menos ocho dígitos y que contengan mayúsculas y minúsculas; segunda, mantener el sistema operativo actualizado para evitar vulnerabilidades y agujeros de seguridad; y tercera, contar con soluciones antivirus activas y actualizadas para evitar la instalación o ejecución de troyanos u otros programas maliciosos que vigilan al usuario y le sustraen sus datos y contraseñas.

Propone FERNÁNDEZ BURGUENO una definición de usurpación de estado civil que la identifica con «hacerse pasar por otro». Y así, señala que usar el nick o el apodo de otra persona podría no ser considerado usurpación del estado civil si no induce a error a terceros, en tanto que usurpar el nick y actuar como esa persona, contactando con sus amistades y haciendo uso del resto de características personales del afectado sí constituye una usurpación de personalidad de acuerdo con lo establecido en las leyes penales.

El tercer y último momento de riesgo para la protección de datos aparece cuando el usuario pretende darse de baja del servicio. Por ello, es

(44) Así lo ha expresado FERNÁNDEZ BURGUENO, Pablo, «Identidades falsas y usurpación de estado civil. El Delito del artículo 401 del Código Penal», en <http://www.pabloburgueno.com> (Fecha de consulta: 23/03/2010).

habitual que se encuentren importantes dificultades para darse de baja del servicio o bien esta baja no resulte plenamente efectiva. Por ello, el derecho de cancelación de los datos personales adquiere en las redes sociales una nueva dimensión que se sustenta en la propia configuración y funcionamiento de estos servicios. Con frecuencia la suspensión de un usuario implicará la conservación por la red social de sus datos personales con el propósito de evitar que pueda registrarse de nuevo, por lo que deberá informarse al usuario sobre esta posibilidad y la finalidad por la cual se conservan los datos. Así lo ha expresado el Grupo de Trabajo de Protección de Datos del Art. 29, estableciendo el plazo de un año para la conservación de dicha información. Del mismo modo, se advierte que la información cancelada por el usuario al actualizar la cuenta no debería conservarse. En cualquier caso, cuando la conservación de la información personal esté justificada para impedir actuaciones maliciosas como usurpación de identidad u otras conductas delictivas también deberá informarse al usuario. A propósito de la conservación de los datos personales, se propone por el citado Grupo de Trabajo desactivar el perfil de usuario cuando no se utiliza el servicio por un período determinado, y suprimir finalmente, tras un período de inactividad la cuenta llegado el caso, ofreciendo cumplida información al usuario de estos trámites y períodos (45).

Sin embargo, lo cierto es que como ha denunciado la AEPD en su Estudio sobre la privacidad de los datos y la seguridad de la información, después del análisis de las más importantes redes sociales, y como criterio general, si bien estas plataformas colaborativas disponen de avisos legales, condiciones de uso y políticas de privacidad, su complicada y extensa redacción las convierte en textos inútiles y de difícil comprensión para el usuario. De esta forma, y a pesar de hallarse recogidas en el sitio web, no alcanzan su finalidad última, a saber: que el usuario comprenda el objeto, la finalidad y el plazo para el que son recabados y tratados sus datos personales, incumpliendo así la normativa sobre protección de datos.

Como con acierto concluye ROIG, la protección de la privacidad en las redes sociales se halla condicionada porque el marco regulador es inexistente o limitado, las tecnologías garantes de la privacidad se consideran un gasto extraordinario desde las empresas y los usuarios demuestran escasa conciencia y preocupación ante esta situación (46).

El éxito y la eficacia en la protección de la privacidad en una red social debe conjugar, a nuestro juicio, dos elementos; por un lado, la responsa-

(45) GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 5/2009 sobre las redes sociales en línea, adoptado el 12 de junio de 2009, Doc. WP 163.

(46) ROIG, Antoni, «E-privacidad y redes sociales», *Revista de Internet, Derecho y Política*, n.º 9, 2009, pp. 50-51.

bilidad y conciencia del propio usuario al utilizar las herramientas y servicios de la plataforma, y por otro lado, el compromiso de la red social con sus usuarios a través de una política de privacidad y unas condiciones de uso claras y ajustadas a la legalidad vigente y un soporte humano y técnico que atienda las necesidades y reclamaciones de los usuarios.

V. El acceso de los menores a las redes sociales

Quienes nos fuimos paulatinamente incorporando al avance de las nuevas tecnologías, y las hemos asumido como una revolución en nuestra vida cotidiana, vivimos rodeados de una nueva generación de jóvenes que han nacido en un universo digital y que no imaginan el mundo sin internet, son los conocidos como *generación interactiva*. Se trata de jóvenes nacidos en la primera década de los años noventa, que disponen en la propia habitación de ordenador y que en su mayoría han sido autodidactas en el uso de las nuevas tecnologías (47). Además, nos hallamos ante una generación de jóvenes, en palabras de TRONCOSO REIGADA, que no sólo utilizan las nuevas tecnologías, sino que viven en ellas y comparten ahí novedades, experiencias y vivencias personales (48).

Cuando PRENSKY acuñó las expresiones «nativo digital» e «inmigrante digital», reflejó de manera certera las importantes y palpables diferencias que separaban a varias generaciones de ciudadanos en el disfrute y manejo de las nuevas tecnologías. Diferencias que determinan la posición de los menores ante las tecnologías y explican la denominada «brecha digital» que permite comprender las dificultades de sus padres para entender, encauzar y educar en un uso responsable y prudente de estas nuevas herramientas tecnológicas (49). Sin embargo, más recientemente este mismo autor ha publicado un interesante trabajo en el que considera superados estos conceptos, e introduce un nuevo término, la «sabiduría digital», concepto que se aplica a aquellas personas que: por

(47) GARCÍA FERNÁNDEZ, Fernando, *Nativos interactivos. Los adolescentes y sus pantallas: reflexiones educativas*, Foro generaciones interactivas, Madrid, 2009. p. 16.ss.

(48) TRONCOSO REIGADA, Antonio, «Las redes sociales y la APDCM», *Revista datospersonales.org*, n.º 43, 2010.

(49) Así, quienes no nacimos en un mundo digital pero adaptamos nuestras vidas en algún momento a las nuevas tecnologías, en expresión de Prensky, somos «inmigrantes digitales», que en ningún caso renunciaremos a nuestra esencia como seres no digitales, y que a pesar del interés y fascinación que despiertan en nosotros las nuevas tecnologías, seguimos manteniendo aspectos que nos identifican y delatan como recién llegados al mundo digital. Enumeraba el autor entre otras situaciones la necesidad de imprimir el correo electrónico o la de confirmar todo envío o comunicación digital telefónicamente. Véase PRENSKY, Marc, «Digital natives, digital immigrants», *On The Horizon*, MCB University, vol. 9, n.º 5, 2001. Véase [http://www.marcprensky.com/writing/Prensky-Digital Immigrants-Part1.pdf](http://www.marcprensky.com/writing/Prensky-Digital%20Immigrants-Part1.pdf) (Fecha de consulta: 25/0372010).

un lado, utilizan de forma habitual y natural las nuevas tecnologías; y por otro lado, realizan además un uso prudente y beneficioso de estas herramientas como instrumento para reforzar sus opiniones, aspiraciones o deseos (50).

En verdad, la problemática y las dificultades a las que se enfrentan los menores en el uso de internet y las diferentes aplicaciones propias de la web 2.0 se hallan marcadas por una realidad que debe analizarse para valorar acertadamente los riesgos que esperan al menor en su acceso a internet. En primer lugar, los menores encuentran un amplio repertorio de herramientas tecnológicas que, salvo excepciones, nadie les ha enseñado a utilizar de manera responsable y prudente; además, son escasas las ocasiones en que reciben formación tecnológica y en protección de sus derechos, por lo que la autoprotección no resulta un medio eficaz de tutela; por otra parte, son mayoría los menores que navegan solos, a edad cada vez más temprana y sin la compañía ni la orientación de sus padres o profesores, las propias herramientas así lo facilitan y permiten. En la actualidad, los menores disponen de teléfono móvil, de un portátil, e incluso de ordenador en su propia habitación. Y por último, el control de los menores en su acceso a Internet, que corresponde a los padres no siempre se ejerce, y pueden citarse varios factores que así lo condicionan: la falta de tiempo, la desidia parental, y principalmente, la evidente brecha digital que separa a ambas generaciones, tal y como hemos apuntado anteriormente (51).

Como reconoce la Decisión del Parlamento Europeo y del Consejo por la que se establece un programa comunitario plurianual sobre la protección de los niños en el uso de internet y de otras tecnologías (52):

«La evolución de la tecnología, la transformación de la manera en que niños y adultos utilizan internet y las demás tecnologías de la comunicación y la modificación de los comportamientos sociales crean nuevos riesgos para los niños [...] Resulta necesario combinar varias medidas y acciones de forma polifacética y complementaria, por ejemplo, me-

(50) Y así, nos sorprende este autor con una nueva expresión, la de *homo sapiens digital*, que se identifica con aquellos usuarios que aceptan la mejora digital como parte de la existencia humana, y que utilizan con normalidad las aplicaciones tecnológicas y las ponen a su servicio. Véase PRENSKY, Marc, «H Sapiens Digital: From digital immigrants and digital natives to digital wisdom», *Innovate*, n.º 5, 2009. Véase http://innovateonline.info/pdf/vol5_issue3/H._Sapiens_Digital-From_Digital_Immigrants_and_Digital_Natives_to_Digital_Wisdom.pdf (Fecha de consulta: 25/03/2010),

(51) ABA CATOIRA, Ana, «Los menores ante internet», *Congreso Internacional de Derecho y Nuevas tecnologías*, Universidad de Deusto, Bilbao, 2009.

(52) Decisión N.º 1351/2008/CE del Parlamento Europeo y del Consejo, por la que se establece un programa comunitario plurianual sobre la protección de los niños en el uso de internet y de otras tecnologías de la comunicación, DO L 348/118, de 24 de diciembre de 2008.

diante la adopción de media que fomenten el uso seguro y responsable de internet, la prosecución del desarrollo de tecnologías de apoyo, el fomento de las mejores prácticas para elaborar códigos de conducta que incluyan unos cánones de comportamiento que cuenten con la aprobación general o la cooperación con la industria sobre objetivos concertados» (Considerando 9).

Así mismo, y siguiendo con las consideraciones de la citada Decisión, confluyen en relación con los menores y su acceso a internet importantes factores, como la desinformación de los padres respecto a sus relaciones online, el exceso de confianza, o la falta de conciencia de los jóvenes sobre la necesidad de reservar su información personal, lo que favorece prácticas abusivas desde los servicios de redes sociales, y exige establecer las necesarias acciones para garantizar la protección de los menores en estas redes.

Desde el ámbito jurídico, en materia de protección de la intimidad, honor y propia imagen de los menores, la Ley orgánica 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen dispone que «el consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil». Bien entendido que cuando el menor no disponga de capacidad suficiente para consentir aquello que afecte a su honor, intimidad o propia imagen, el consentimiento deberá otorgarse mediante escrito por su representante legal, que estará obligado a informar previamente al Ministerio Fiscal, que si en plazo de ocho días se opone, deberá resolver el Juez. Así las cosas, parece evidente que estos principios deben interpretarse conforme a la realidad de las redes sociales, y el fenómeno de internet, tal y como se viene argumentado por la más diversa doctrina (53).

Otro aspecto controvertido del acceso de los menores a la red es el relativo al tratamiento de sus datos personales, no en vano las redes sociales obtienen y tratan numerosa información personal de los menores que también resulta accesible a efectos de contextualizar la publicidad, de suerte que las preferencias, intereses, accesos, aficiones de los menores se obtienen para orientar y personalizar la publicidad que se les dirige (54).

(53) PANIZA FULLANA, Antonia, «Problemática jurídica del menor como consumidor/usuario en la sociedad de la información». *Congreso Derecho y Nuevas Tecnologías*, Universidad de Deusto, Bilbao, 2009.

(54) Véase la interesante aportación de PÉREZ-LUÑO, Antonio Enrique, «La protección de los datos personales del menor en Internet», *Anuario de la Facultad de Derecho de la Universidad de Alcalá de Henares*, n.º 2, 2009, pp. 145-177.

En el ordenamiento jurídico español, el RD 1720/2007 de 21 de diciembre prevé, no sin cierta polémica doctrinal, en su artículo 13 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 la patria potestad o tutela. En el caso de menores de 14 años se requerirá el consentimiento de los padres o tutores». Coincide en señalar la doctrina la falta de coherencia de la norma reglamentaria, por cuanto que antes ninguna otra norma con rango de ley ha determinado la concreta edad a la que se entiende lícitamente prestado el consentimiento por los menores (55). Siguiendo la interpretación de GRIMALT SERVERA que califica a esta norma como regla orientadora, nos hallamos ante una presunción legal de madurez suficiente, si bien, como con acierto sugiere el autor, no deberían ser los catorce años los que determinen la capacidad del menor para otorgar un consentimiento válido, por el contrario, de acuerdo con el resto del ordenamiento jurídico español, se deberá atender a las condiciones de madurez del menor (56).

Así lo ha interpretado también el Grupo de Protección de Datos del Artículo 29 cuando en su Dictamen 2/2009 subraya que las normas de protección de datos de los menores han de tener en cuenta dos aspectos importantes. En primer lugar, los diversos grados de madurez que determinan el momento a partir del cual los niños pueden empezar a ocuparse de sus propios datos y, en segundo lugar, hasta qué punto los representantes tienen derecho a representar a los menores en los casos en que la divulgación de datos personales pueda ser perjudicial para los intereses del niño (57).

En el ámbito autonómico, destaca la Ley 12/2008, de 3 de julio de Protección de la Infancia y la Adolescencia de la Comunidad Valenciana, que en su artículo 16 presenta una solución distinta a la prevista en la norma estatal, y por la que «se reconoce al menor el derecho de protección de sus propios datos y a impedir el tratamiento o la cesión de los mismos sin el consentimiento del representante del menor, salvo en el caso del menor emancipado, que podrá consentir por sí mismo» (58). Doble re-

(55) Por todos, PANIZA FULLANA, Antonia, «Problemática jurídica del menor como consumidor/usuario en la sociedad de la información». *Congreso Derecho y Nuevas Tecnologías*, Universidad de Deusto, Bilbao, 2009,

(56) GRIMALT SERVERA, P. y CAVANILLAS MÚGICA, S. «Servicios de la sociedad de la información y protección de datos personales», en *Derecho de la empresa y protección de datos*, Ed. Aranzadi: Cizur Menor, 2008, pp. 336-338.

(57) GRUPO PROTECCIÓN DE DATOS ART. 29, Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas), Doc. 398/09/ES WP 160, de 11 de febrero de 2009.

(58) Ley 12/2008, de 3 de julio de Protección de la Infancia y la Adolescencia de la Comunidad Valenciana, BOE n.º 200, de 19 de agosto de 2008.

sulta, a nuestro juicio, el acierto de esta previsión normativa que, por una parte, sigue la línea apuntada por la legislación general en la prestación válida del consentimiento de menores, y por otra, presenta un claro efecto extensivo, en el que el consentimiento se otorga para el tratamiento y la cesión; conviene recordar, no obstante, que su aplicación se halla circunscrita al ámbito autonómico al que la norma se refiere, y por el cual será aplicable únicamente a los ficheros de titularidad pública de dicha Comunidad Autónoma.

Así mismo, señala el artículo 13 del citado RD 1720/2007 que no pueden recabarse del menor datos personales de la familia o de los padres, a excepción de aquellos que sean necesarios para recabar su consentimiento, cuando éste sea preciso. En todo caso, exige este precepto, que cuando el tratamiento de datos esté referido a menores de edad, la información deberá expresarse en lenguaje comprensible y adaptado para ellos, siendo obligación del responsable del fichero arbitrar los mecanismos y controles precisos para comprobar de modo efectivo la edad del menor.

Corresponde a las redes sociales configurar un entorno seguro para aquellos usuarios que como los menores de edad resultan especialmente vulnerables; por ello, además de evitar la indexación de la información personal de los menores, determinar una publicidad restringida para el perfil personal de estos usuarios, establecer el acceso por invitación, o actuar frente a la denuncia de actuaciones ofensivas o perjudiciales, se deben reforzar las medidas de seguridad, especialmente en lo que afecta al control de edad, con la implantación de protocolos de control de la edad de los usuarios, con ágiles botones de denuncia de actuaciones abusivas o irrespetuosas, o con el diseño y redacción de políticas de privacidad adoptadas a la edad de los usuarios, cada vez más jóvenes, de estas plataformas de servicios. En este contexto, destaca la actuación y el compromiso de Tuenti, la plataforma española de mayor éxito, que el año pasado presentó a la AEPD las medidas adoptadas para eliminar de esta red social a usuarios menores de catorce años (59).

Para concluir, es interesante reseñar las reflexiones y recomendaciones que en el marco del Seminario Derechos, Adolescentes y Redes sociales en internet, se adoptaron en el denominado Memorandum de Montevideo sobre la protección de datos personales y la vida privada en

(59) Tuenti implantó en abril de 2009 un proceso de depuración de los perfiles de menores de catorce años, por el cual en los casos de perfiles que aparentan ser de menores de 14 años se les envía desde la red social una solicitud para que aporten fotocopia del DNI o pasaporte en un plazo inferior a 92 horas, y en el caso de no recibir respuesta, se advierte al usuario que su perfil será borrado. Así mismo, Tuenti ha realizado un cambio en la configuración de los perfiles de menores de 18 años, que por defecto tendrán el grado de privacidad máximo. Así se anuncia por la AEPD en <http://www.agpd.es>

las redes sociales en internet, del que destacamos las tres consideraciones fundamentales que se señalan en su Preámbulo, a saber: el especial protagonismo de la familia y el entorno de los menores en el proceso de educación sobre un uso seguro y responsable de internet y las redes sociales; la necesidad de que cuantas medidas se adopten tengan presente el principio del interés superior del menor, garantizando un equilibrio entre las necesidades de protección contra la vulneración de sus derechos y el uso responsable de estas herramientas, y por último, la responsabilidad de los prestadores de servicios de redes sociales por los servicios que proveen, y que como tales deben asumir su compromiso en los conflictos y la problemática que su uso genera (60). A estas acertadas consideraciones, debe sumarse la necesidad de que desde las instituciones públicas se arbitren mecanismos y herramientas para la protección de los usuarios en internet, así como corresponde a las administraciones fomentar la autoprotección del usuario, mediante la preparación y difusión de documentos, en forma de Guías, y recomendaciones a los usuarios que alerten sobre los peligros y la necesidad de proceder a una navegación segura.

Por último, según revelan los autores de un interesante Estudio sobre los hábitos de los jóvenes en internet (61), se confirma que entre las actividades de los jóvenes no se detecta prácticamente ninguna acción solidaria, ciudadana y/o política realizada a través de Internet; se asegura que los padres españoles usan muy pocos medios técnicos, básicamente programas de filtrado o uso de filtros del Internet Explores o el Windows Vista, para el control de las actividades de sus hijos en la Red y que son escasas las ocasiones en las que los menores acuden a sus padres o tutores ante situaciones comprometidas o graves en internet, y se señala como riesgo que en mayor medida preocupa a los jóvenes en internet los posibles virus. Ante esta realidad, fácilmente se comprende la tarea que deben abordar instituciones públicas y educativas, así como el entorno familiar de los menores para concienciar y sensibilizar a los jóvenes en la necesidad de protegerse como usuarios de internet. Y ciertamente, es mucho lo avanzado, así lo demuestran los estudios y las actuaciones públicas desarrolladas en este ámbito, pero no es menos cierto que todavía son muchas las carencias y conflictos a los que los menores deben enfrentarse como usuarios de internet.

(60) Memorando sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes, Montevideo, 2009. <http://www.iijusticia.org/Memo.htm> (Fecha de consulta: 17/03/2010)

(61) GARITAONANDIA, Carmelo y GARMENDIA, Maialen, «Cómo usan Internet los jóvenes: hábitos, riesgos y control parental», *Programa «Safer Internet Plus Programme»*. <http://www.ehu.eukidsonline/INFORME%20FINAL-INTERNET.pdf> (Fecha de consulta: 27/03/2010).

VI. Actuaciones públicas en defensa del usuario

Según revela un Estudio del Observatorio de Seguridad de la Información un 83.4% de los encuestados afirmaba que la Administración debe implicarse más en mejorar la seguridad en internet; de ellos, un 26.8% consideraba necesario que se desarrollaran y ofrecieran desde la administración herramientas de seguridad gratuitas, frente al 24% que estimaba necesaria una mayor vigilancia de lo que sucede en internet, y tan sólo un 7% apostaba por el deber de las instituciones de velar por un uso adecuado de los datos personales en internet (62).

En 2008 se alcanzaron en Estados Unidos una serie de acuerdos entre Myspace y Facebook con Fiscales generales estatales, *Joint Statement on Key Principles of Social Networking Safety*, que recogen varios principios para la protección de los usuarios de redes sociales, entre los que destacan, por ejemplo, el carácter privado de los perfiles de menores de 14 años, la política de bloqueo de edad para los perfiles ya existentes a esa fecha, y la restricción a menores del acceso a contenidos y links para adultos, así como la implantación de un servicio de atención a padres con herramientas y aplicaciones gratuitas de control parental (63).

A iniciativa de la Comisión Europea, se logra en 2009 un Acuerdo Europeo para mejorar la seguridad de los menores que utilizan redes sociales, entre las principales empresas de la web que operan como redes sociales, y que permite valorar la magnitud del problema (64), y dar cuenta de la necesidad de establecer medidas de control y cautela que faciliten el acceso seguro a estas redes sociales de comunicación, utilizadas principalmente por los sectores más jóvenes de la sociedad. El citado Acuerdo, que agrupa y compromete a empresas como Facebook, Google, YouTube, Myspace, Yahoo Europa o Microsoft Europa, y al que posteriormente se han adherido otras plataformas como Tuenti, es un ejemplo de la importancia de la autorregulación en este sector, que intenta a través de este acuerdo poner límites a los riesgos más significativos a los que los menores quedan expuestos con la utilización de las redes sociales.

Más recientemente, ENISA, la Agencia Europea para la Seguridad de las Redes y la Información, ha publicado un Informe en el que alerta sobre las redes sociales y su uso indebido, especialmente cuando se accede

(62) OBSERVATORIO DE SEGURIDAD DE LA INFORMACIÓN (INTECO), *Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles (10.ª Oleada) Tercer Trimestre*, 2009.

(63) Véase en <http://www.ag.state.mn.us/PDF/PressRelease/SocialNetworkingSitesSafety.pdf>

(64) Se puede acceder al documento íntegro y a las actividades de difusión del mismo, así como las empresas adheridas en http://ec.europa.eu/information_society/activities/social_networking/index-en.html (Fecha de consulta: 20/02/2010).

mediante teléfono móvil (65), en dicho informe incorpora las denominadas «Reglas de oro», concebidas como consejos de seguridad y recomendaciones para aumentar la conciencia sobre los riesgos y las amenazas relacionadas con el uso indebido de las redes sociales, en particular cuando se accede a través de teléfono móvil. Mediante la redacción de unas sencillas normas sobre la forma de evitar consecuencias no deseadas, se recomienda con carácter general, al usuario:

- Considerar cuidadosamente las imágenes, los vídeos y la información que opta por publicar, con especial atención a la información sensible.
- Utilizar un seudónimo o apodo que le ayude a proteger su identidad y privacidad frente a terceros
- Ser selectivo sobre las personas a quienes acepta como amigos en la red social. Debe asegurarse de la identidad real de las personas con quienes contacta
- Registrar el correo electrónico personal al acceder a la red social, y no el de la empresa donde trabaja. Deberá ser prudente y cauteloso con los comentarios o materiales que publique de su empresa
- Actuar con responsabilidad cuando se publique información de terceros, y asegurarse del consentimiento de la persona.
- Leer cuidadosamente y de forma íntegra la política de privacidad y las condiciones de uso de la red social antes de registrarse.
- Adecuar correctamente el nivel de privacidad de su perfil, evitando la puesta a disposición del mismo de forma indiscriminada
- Ser especialmente cauteloso si se accede a la red social través del teléfono móvil. Informando de su pérdida o robo inmediatamente, no guardando en él la contraseña de acceso.

En el ámbito nacional, destacan los diferentes estudios presentados por INTECO, algunos en colaboración con otras Instituciones. Así, en el citado Estudio sobre la privacidad de los datos personales se señalan aspectos a mejorar por las empresas de redes sociales y se establecen propuestas desde una doble perspectiva: desde el punto de vista jurídico, se insiste en la necesidad de hacer transparentes y sencillas las condiciones de uso; y desde el ámbito tecnológico, se señala la necesidad de reforzar la privacidad del usuario, controlando la indexación de los perfiles, estableciendo el grado máximo por defecto de privacidad de los datos, o implementando sistemas de identificación de edad y de identificación remota de los usuarios mediante sistemas de firma electrónica reconocida.

(65) ENISA, «Online as soon as it happens», 2010. <http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens> (Fecha de consulta: 17/03/2010).

Un elemento importante a subrayar de las actuaciones públicas es la elaboración y difusión de Guías y recomendaciones para la protección de los usuarios. En este contexto, INTECO conjuntamente con la iniciativa PantallasAmigas ha desarrollado el proyecto SecuKid, en el que mediante un sencillo y gratuito juego educativo para móviles dirigido a todos los públicos, especialmente niños y adolescentes a partir de los 11 años, se pretende que este colectivo identifique mejor algunos riesgos de Internet, sus efectos y cómo prevenirlos (66).

En febrero de 2010 INTECO ha publicado un conjunto de Guías de ayuda para la configuración de la privacidad y seguridad de las redes sociales, con las que pretende asistir a los usuarios cuando acceden y se registran en las diferentes redes sociales, ofreciendo pautas y normas de actuación a los usuarios, y en las que se analiza la política de privacidad y las condiciones de uso de cada red social (67).

Debemos llamar la atención sobre los esfuerzos que viene desarrollando en este ámbito la AEPD, que ha publicado numerosas guías y recomendaciones para usuarios de internet. Así, en 2006 las Recomendaciones a usuarios de internet, y posteriormente, en 2008 una Guía sobre Derechos de niñas y niños y deberes de los padres y madres. A ello, debe sumarse la incorporación en la propia página web de esta institución de materiales específicos para los menores, donde se incluyen vídeos, guías, estudios y enlaces de interés para los menores. Especialmente intenso está resultando el seguimiento que la AEPD viene realizando a las redes sociales, y que se materializa en encuentros periódicos con los responsables de estas plataformas, para promover la adecuación de su funcionamiento a la normativa española, y trasladar la inquietud con que desde las instituciones se percibe el crecimiento de estas comunidades virtuales, principalmente entre los más jóvenes.

A tales efectos, se han puesto en funcionamiento un conjunto de medidas y buenas prácticas que impidan tales riesgos, como la implantación de un «botón de denuncia de abusos» sencillo de utilizar y que permita al usuario denunciar en un clic contactos o comportamientos inadecuados, o bien medidas que aseguren que los perfiles privados de los usuarios menores de edad no puedan buscarse, o en su caso, técnicas que garanticen que las opciones de privacidad están destacadas y sean accesibles en todo momento, en definitiva, se establecen límites para el acceso de menores a redes dirigidas a mayores de edad.

Desde las instituciones autonómicas, la Agencia Vasca de Protección de Datos ha impulsado un Portal para adolescentes y educadores ubicado

(66) Véase <http://secukid.es/index.html> (Fecha de consulta: 12/03/2010).

(67) http://www.inteco.es/Seguridad/Observatorio/manuales_es/guia_ayuda_redes_sociales (Fecha de consulta: 28/03/2010).

en su propia página web en el que se incluye la campaña juvenil «Kontuzdatos... Decides Tú», y se presentan vídeos formativos, dibujos animados que ilustran a los menores sobre la importancia de proteger la información personal, y un Manual de uso de tecnologías para jóvenes de 9 a 11 años (68).

Tal y como se anuncia por la Agencia Catalana de Protección de Datos, las escuelas y los institutos de Cataluña disponen de material educativo para ayudar a los menores a construir una cultura de protección de su privacidad en Internet. El objetivo es promover un uso adecuado de los datos de carácter personal y de las tecnologías de la información (TI) entre los niños y jóvenes de 9 a 17 años. Para ello, la Agencia Catalana de Protección de Datos (APDCAT), la Comisión de Libertades e Informática (CLI) y el Departamento de Educación presentaron tres nuevos manuales prácticos dirigidos a menores, con la finalidad de concienciarles sobre la amenaza a la intimidad y la privacidad que representa la publicación de sus datos personales en Internet, así como proporcionarles recomendaciones prácticas para evitar situaciones de riesgo y hacer un buen uso de las tecnologías de la información. Estas guías van dirigidas a jóvenes de entre 9 y 17 años, y se incluirán en el plan de acción tutorial de las escuelas e institutos catalanes, ya que podrán descargarse de la página web del Departamento de Educación (www.gencat.cat/educacio). Se han editado tres versiones adaptadas a las necesidades de cada uno de los ciclos educativos a los que se dirigen: Educación Primaria (de 9 a 11 años), Educación Secundaria (12 a 14 años) y Bachillerato o Formación Profesional (15 a 17 años) (69). Además, incorpora en su propia página web la campaña para menores «Privacidad para niños y jóvenes. Navega seguro», en la que se propone a los menores mediante un sencillo juego de preguntas que avancen en el conocimiento de la protección de datos personales y valoren la importancia de navegar seguros por la red.

Por su parte, la Agencia de Protección de Datos de la Comunidad de Madrid (en adelante, APDCM), ha colaborado desarrollando importantes y extensas campañas de sensibilización de los más jóvenes, alertando sobre los riesgos y amenazas de las redes sociales. Para ello, bajo el lema «Hay cosas que no contarías a un extraño, ¿por qué hacerlo en Internet?», la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM) ha editado dos vídeos destinados a los menores y que pueden descargarse en Tuenti y en YouTube, colaboradores de esta campaña, así como en el propio sitio web de la APDCM. Otra de las acciones destacadas de esta campaña ha sido la celebración de una sesión informativa sobre pro-

(68) Véase <http://www.avpd.euskadi.net/sO4-Kontuzdt/es> (Fecha de consulta: 03/03/2010).

(69) Véase <http://www.apdcat.net/ca/index.php> (Fecha de consulta: 03/03/2010).

tección de datos personales en el ámbito de las nuevas tecnologías en todos los Institutos públicos de la Comunidad de Madrid a comienzos de 2010. Una iniciativa de la APDCM que contó con el apoyo de la Consejería de Educación de la Comunidad de Madrid, en la que participaron un total de 404 Institutos de Enseñanza Secundaria madrileños y que formó a unos 80.000 escolares de segundo y tercero de la ESO (70).

También en la Comunidad de Madrid, el Defensor del Menor, alcanzó en 2007 con las principales operadoras de telecomunicaciones un Protocolo para el uso adecuado y seguro de las Tics por niños y adolescentes (71), tendente a articular un marco común que favorezca un uso adecuado y saludable de estas aplicaciones, y por el que se acuerda reforzar las iniciativas y medidas de apoyo que ayuden a la formación tecnológica saludable de los menores, fomenten el desarrollo de actividades de educación e información de padres y jóvenes, y divulguen la existencia de medidas técnicas y de seguridad que permitan personalizar las necesidades de protección por los padres y educadores para los menores en su acceso a internet.

Recientemente esta institución se ha visto inmersa en una fuerte polémica, cuando el actual Defensor del Menor de esta Comunidad Autónoma confesó que disponía de un perfil personal falso para poder controlar el uso que sus hijos hacen de la red, al tiempo que animó a los padres a que adopten estas medidas como forma de ejercer la patria potestad en un mundo virtual (72). Sin entrar a calificar esta conducta, lo cierto es que esta experiencia permite denunciar y llamar la atención sobre la alarmante facilidad con la que los adultos pueden acceder mediante engaño a las redes sociales y crear un perfil falso que les ampare para actuar en la red social.

Corresponde a las instituciones y a las redes sociales facilitar y promover espacios seguros de relación, mediante la implantación de medidas que contribuyan a que los usuarios puedan disfrutar y servirse de cuantos avances tecnológicos vayan abriéndose paso en la sociedad de la información. Y en este sentido, adquieren especial relevancia cuantas

(70) Véase <http://www.madrid.org> (Fecha de consulta: 29/03/2010).

(71) http://www.defensordelmenor.org/documentacion/informes_anuales.php (Fecha de consulta: 29/03/2010).

(72) El Defensor del Menor de la Comunidad de Madrid aseguró que fue su hija quien cursó la invitación para facilitar su acceso a la red social, y estuvo de acuerdo en dicho control, que por otra parte estima necesario, por lo que anima a los padres a que accedan a las redes sociales para poder conocer qué comparten sus hijos y con quién se relacionan. Al mismo tiempo, sugirió a las redes sociales que arbitren medios que habiliten el acceso de los padres y tutores sin necesidad de invitación como medida de control parental. http://www.elpais.com/articulo/madrid/Defensor/Menor/tiene/perfil/falso/Tuenti/controlar/usan/hijos/elpepusoc/20100313elpmad_8/Tes (Fecha de consulta: 28/03/2010).

iniciativas se impulsen desde las administraciones como garantes de los derechos de los ciudadanos, por ello cabe esperar que al tiempo que se estimula e incentiva el acceso a los servicios tecnológicos que la sociedad de la información nos procura, se afiancen y garanticen desde las instituciones el reconocimiento y el ejercicio de los derechos a los que como usuario de estos servicios no debe renunciar el ciudadano.

VII. Conclusiones

Como seres humanos somos seres sociables, necesitamos de los demás para vivir y relacionarnos, y esa necesidad nos mueve y anima a entablar contactos, relaciones y experiencias con otras personas. Las redes sociales constituyen en la actualidad la máxima expresión de esta sociabilidad y de ese anhelo de relación que todos llevamos dentro. Ahora bien, no puede afirmarse, sin incurrir en una imprecisión, que las redes sociales son un fenómeno reciente y actual, que nace con el desarrollo de la sociedad de la información, no en vano las redes sociales convencionales han existido desde que el hombre siente la necesidad de unirse a otros y constituir una comunidad social. Bien es verdad que el avance y desarrollo de las nuevas tecnologías y la irrupción de internet han facilitado la aparición de una nueva realidad, las redes sociales digitales, que amparadas en la condición social de las personas, han revolucionado las formas de relación humana hasta establecer un mundo paralelo y virtual, donde los ciudadanos se reúnen, contactan y comparten sus más personales vivencias y experiencias con otros. Claro que si las redes sociales se definen como el modo en que se construye nuestra identidad on line, el cauce por el que se agrega y comparte nuestra actividad en la red, y la nueva forma de representación de nuestra vida social será sencillo explicar y comprender el éxito y el interés que este fenómeno despierta socialmente.

Este nuevo espacio tecnológico, cuya expansión y crecimiento no parece tener límites, se nos presenta como una oportunidad única para que el ser humano se abra a los demás y participe en la creación de un espacio virtual, en el que además se manifiesta como el auténtico protagonista. Como usuarios de redes sociales digitales no sólo buscamos información, la creamos, generamos y compartimos. En una sociedad como la actual, en la que la imagen que se proyecta resulta tan importante, nada parece preocupar tanto al ser humano como poder gestionar y controlar su propia identidad ante los demás; por tanto, en estas comunidades virtuales, en las que cada usuario compone su imagen o perfil personal, las personas parecen sentirse seguras y confiadas frente a los demás. Y seguramente por ello, nunca antes se había cedido ni compartido tanto es-

pacio personal y privado por el ser humano, y nunca antes se había confiado a terceros tanta información personal y familiar.

Pero lo cierto es que esta sensación de seguridad y control que comparten los usuarios no pasa de ser una ilusión o ficción, de la que se ven obligados a salir forzados en ocasiones por la negligente o ilícita actuación de terceros, o por la abusiva o irresponsable actitud de las propias redes sociales. En efecto, sin desconocer las indudables posibilidades y virtudes que pueden encontrarse en las redes sociales, acompañan al uso de estos servicios importantes y significativos riesgos que el usuario debe identificar y conocer para poder actuar con la responsabilidad y prudencia que estas herramientas digitales demandan. En verdad, las redes sociales plantean un nuevo esquema de relación humana, que se caracteriza por la interactividad y por conferir a nuestras relaciones sociales y a nuestras experiencias y vivencias una visibilidad y difusión hasta ahora imposible. Hacemos partícipes a otros usuarios de nuestros contactos, actividades, gustos, aficiones, logros o decepciones con una facilidad y una confianza hasta ahora impensables. Por ello no debe extrañar que se advierta desde las más diversas instancias a los ciudadanos, ante la pérdida y renuncia a la privacidad que en sí mismas encierran estas acciones. Y así, no sólo nuestros datos personales, nuestra intimidad, imagen u honor pueden resentirse como consecuencia de una irresponsable o imprudente actuación en estos entornos virtuales, también debemos valorar los derechos de los demás a su intimidad, a su imagen, y a la protección de sus datos personales, sin ignorar que deben respetarse igualmente los derechos de propiedad intelectual e industrial de los contenidos que se comparten. Los ciudadanos no deben olvidar que nada hay más real que internet, que su pretendida virtualidad es sólo aparente, y que nuestra actividad en la red nos delata y tiene consecuencias y efectos en el mundo real que debemos valorar y medir en nuestro comportamiento online.

Por otro lado, no pueden esconder su responsabilidad las redes sociales, a quienes la normativa vigente, en el ámbito comunitario y en el nacional, les impone importantes deberes y exigencias para la tutela de los derechos de sus usuarios. Así, debemos confiar en que el empeño y la tenacidad de las instituciones, finalmente dé sus frutos, y desde las redes sociales se avance en la implantación de medidas y protocolos de actuación necesarios para crear un entorno virtual seguro para los usuarios. Debemos felicitarnos por algunos de los logros alcanzados, y como usuarios, conscientes de nuestra fuerza y poder, nos corresponde demandar cuantos avances y garantías sean precisas para la tutela efectiva de nuestros derechos.

La normativa exige que la política de privacidad de las redes sociales sea legible, comprensible para el usuario, se establece también el de-

ber de informar del tratamiento de datos personales y de las finalidades de uso de los mismos, se debe obtener nuestro consentimiento expreso para el tratamiento de determinados datos sensibles, desde la legislación se prohíbe el envío de comunicaciones comerciales no deseadas, y se garantiza que nuestros datos personales se cancelarán cuando no seamos ya usuarios de la red social.

Ahora bien, se espera y confía en que como usuarios de redes sociales desarrollemos un comportamiento responsable que no exponga gratuitamente nuestra vida privada y la de terceros, y que asegure una respuesta eficaz ante posibles conflictos. Así, en primer lugar, se insiste en que el usuario lea y respete las condiciones de uso del servicio de las redes sociales, que configure las opciones de privacidad de los datos personales adecuadamente, que seleccione con cautela a quienes acepta como amigos, y que finalmente, evite conductas de riesgo tales como la publicación de fotos íntimas o comprometidas, la revelación de datos de contacto a desconocidos o la aceptación de encuentros personales con usuarios conocidos sólo en la red.

Si hay que señalar un colectivo especialmente sensible y vulnerable ante las redes sociales, es el de los menores, considerados «nativos digitales», han nacido en un entorno tecnológico, se caracterizan por vivir las nuevas tecnologías como un fenómeno natural, pero al mismo tiempo carecen de la formación necesaria para un uso seguro de internet, se muestran excesivamente confiados ante los riesgos y amenazas que las aplicaciones tecnológicas implican, y con frecuencia, tropiezan con la palpable «brecha digital» que les separa de sus padres y educadores, y que explica, en buena medida, su actitud y comportamiento en las redes sociales. Es una realidad reciente que las nuevas tecnologías y el uso de Internet se están fomentando en los centros educativos, y ello debe ir acompañado de recomendaciones y consejos sobre los riesgos de uso de la propia red; consejos que no sólo deben proporcionarse en los círculos educativos, sino, fundamentalmente, en el ámbito familiar. La protección de la esfera privada de los más jóvenes requiere la incorporación de una cultura de protección de datos de carácter personal y de la privacidad que promueva las actuaciones preventivas como medio más efectivo y seguro de respuesta ante posibles conflictos. Y en este ámbito, deben poner especial cuidado y atención las redes sociales y las instituciones, impulsando medidas que protejan a los menores ante actuaciones abusivas e ilícitas, implementando cuantos avances técnicos garanticen un uso seguro de estas herramientas y aplicaciones, y advirtiendo claramente de los riesgos y amenazas de la red. En efecto, los perfiles de menores de edad deben ser por defecto cerrados, sin posibilidad de indexación por motores de búsqueda, deben establecerse medidas de control y verificación de la edad, se deben introducir «ventanas de denuncia» ante actua-

ciones abusivas, y deben arbitrarse medios que faciliten el ejercicio de derechos por personas ajenas a la propia red social.

Es innegable que en este sentido han sido importantes los avances, especialmente en la seguridad de los menores ante internet, si bien, tal y como se insiste desde las instituciones europeas, todavía son numerosos los compromisos y acuerdos que deben suscribir las redes sociales, para la construcción de un entorno seguro de relación.

Por todo ello, se espera que los responsables de redes sociales configuren plataformas que se adapten a cada usuario, siendo particularmente protectores con los menores de edad; y se confía en que los usuarios actúen con cautela, y valoren adecuadamente los datos que revelan en estos servicios web, con una especial llamada de atención a padres y educadores, para que no descuiden su obligación de seguir la actuación de los menores en la red y puedan advertirlos de los peligros de estas redes para que realicen un uso seguro y prudente de las nuevas tecnologías.

En definitiva, en una sociedad dominada por el uso de la tecnología, en la que las instituciones despliegan decididos esfuerzos de promoción de la sociedad de la información no resultaría razonable ni coherente dar la espalda a las redes sociales. Verdaderamente, no se podrá avanzar negando una realidad que, como las redes sociales, favorece la comunicación y la interactividad social, por el contrario, corresponde a la familia, las instituciones y los educadores orientar hacia un uso responsable y seguro de estas herramientas, conscientes de su imparable avance y crecimiento y de su configuración como un instrumento imprescindible para la comunicación y la relación entre los seres humanos.

VIII. Reseña bibliográfica

ABA CATOIRA, Ana, «Los menores ante internet», *Congreso Internacional de Derecho y Nuevas tecnologías*, Universidad de Deusto, Bilbao, 2009.

ABRIL I ABRIL, Amadeu, «Redes sociales, Web 2.0 y la desaparición del espacio privado», en *Redes sociales: ¿autocontrol o descontrol de la privacidad en internet?*, Barcelona, 6-10 de julio de 2009.

ACED FÉLEZ, Emilio, «Las redes sociales: nueva frontera para la privacidad de los *digital babies*», en *Seminario Seguridad en redes sociales: ¿están nuestros datos protegidos?*, Escuela Universitaria de Ingeniería Técnica de Telecomunicaciones, Universidad Politécnica de Madrid, 2009.

CACHIA, Romina, «Los sitios de creación de redes. Aspectos sociales», *Cuadernos de Comunicación e Innovación*, n.º 16, 2008, pp. 72-ss.

- DUMORTIER, Franck, «Facebook y los riesgos de la «descontextualización» de la información», *Revista de Internet, Derecho y Política*, n.º 9, 2009, pp. 25-41.
- FERNÁNDEZ BURGUEÑO, Pablo, «Identidades falsas y usurpación de estado civil. El Delito del artículo 401 del Código Penal», en <http://www.pabloburgueno.com>
- GARCÍA FERNÁNDEZ, Fernando, *Nativos interactivos. Los adolescentes y sus pantallas: reflexiones educativas*, Foro generaciones interactivas, Madrid, 2009, pp. 16-ss.
- GRIMALT SERVERA, P. y CAVANILLAS MÚGICA, S. «Servicios de la sociedad de la información y protección de datos personales», en *Derecho de la empresa y protección de datos*, Ed. Aranzadi: Cizur Menor, 2008, pp. 336-338.
- MIRALLES, Ramón, «Uso y abuso de las redes sociales», en *Redes sociales: ¿autocontrol o descontrol de la privacidad en internet?*, Barcelona, 6-10 de julio de 2009.
- ORIHUELA, José Luis, «Internet: la hora de las redes sociales», *Nueva Revista*, n.º 119, 2008, pp. 57-ss.
- PANIZA FULLANA, Antonia, «Problemática jurídica del menor como consumidor /usuario en la sociedad de la información». *Congreso Derecho y Nuevas Tecnologías*, Universidad de Deusto, Bilbao, 2009.
- SANDOVAL MARTÍN, María Teresa, «La red: el nuevo mercado de la vida privada», *Ambitos*, n.º 5, 2000, pp. 154-155.
- PÉREZ-LUÑO, Antonio Enrique, «La protección de los datos personales del menor en Internet», *Anuario de la Facultad de Derecho de la Universidad de Alcalá de Henares*, n.º 2, 2009, pp. 145-177.
- PÉREZ SAN JOSÉ, Pablo, «La autorregulación como instrumento para la protección de la privacidad y de la seguridad en las redes sociales», *Revista Datospersonales.org*, n.º 43, 2010.
- PRENSKY, Marc, «Digital natives, digital immigrants», *On The Horizon*, MCB University, vol. 9, n.º 5, 2001.
- PRENSKY, Marc, «Homo Sapiens Digital: From digital inmigrants and digital natives to digital wisdom», *Innovate*, n.º 5, 2009.
- ROIG, Antoni, «E-privacidad y redes sociales», *Revista de Internet, Derecho y Política*, n.º 9, 2009, pp. 42-53.
- TRONCOSO REIGADA, Antonio, «Las redes sociales y la APDCM», *Revista Datospersonales.org*, n.º 43, 2010.

LABURPENA: Gizakiak hurkoek aintzat har dezatela behar du, harremanak izateko beharra dauka eta besteek berari buruz duten iritzia kudeatu eta kontrolatzeko beharra ere bai. Hortxe dago gizarte-sareen arrakastaren koska. Sare horien bidez, identitate digitala eratu nahi da, eta identitate hori beste batzuei zabaltzen zaie, norberaren bizipen pertsonalenak ere erakutsita, norberak hala erabakita. Horregatik, orain harreman sozialak eta profesionalak oso agerikoak eta interaktiboak dira, inoiz ez bezala. Izan ere, gaur egun, gizakiak uko egiten die bere bizitza pribatuaren alde askori, askatasunez eta nahita; lehendik ez da inoiz halakorik gertatu. Ez da harritzekoa, horrenbestez, oso erakunde desberdinak gizarte-sareen erabiltzaileak babesteko esparru juridikoa ezartzeko ahaleginetan ibiltzea, batez ere adingabekoen babesa sendotze aldera, erabiltzailerik ahulenak direla-eta.

HITZ GAKOAK: Funtsezko eskubideak. Adingabekoak. Gizarte-sareak.

RESUMEN: Las redes sociales centran su éxito en la consideración social del ser humano, en su necesidad de relación y en el intento de las personas por gestionar y controlar la impresión que causan en los demás. Se pretende construir una identidad digital, que se comparte voluntariamente con terceros, a quienes se desea hacer partícipes también de las vivencias más personales. Por ello, nunca antes las relaciones sociales y profesionales fueron tan visibles e interactivas. Nunca antes el ser humano había renunciado de manera libre y voluntaria a tantas parcelas de su vida privada. No debe sorprender, por tanto, el esfuerzo de las más diversas instituciones por establecer un marco jurídico de tutela para los usuarios de las redes sociales y, por reforzar de forma especial, la protección los menores como usuarios mas vulnerables.

PALABRAS CLAVE: Derechos fundamentales. Menores. Redes sociales.

ABSTRACT: Social networks get their success from the social consideration attributed by the human being, from their need to interact and from people trying to manage and control the impression they make upon others. A digital identity can be construed, and it is volutarily shared with third parties whom with we want to share our most personal experiences. Thus, social and professional relationships were never so exposed and interactive. Human beings did never renounce to so many life parcels in such a free and voluntary way. It is not surprising, then, the effort by several institutions to set a legal framework for the protection of users of social networks and specially to strenghten the protection of minors as the most vulnerable users.

KEYWORDS: Fundamental rights. Minors. Social networks.