Revista de Derecho UNED, núm. 10, 2012

EL FENÓMENO DE LAS REDES SOCIALES Y LOS CAMBIOS EN LA VIGENCIA DE LOS DERECHOS FUNDAMENTALES

Ana María Gil Antón

Profesora Asociada de Derecho Civil de la UCM
Doctoranda del Departamento de Derecho Constitucional de la UNED

«Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas, ni entiendes la tecnología.»

Bruce Schneier

Resumen: Este trabajo aborda, de manera sintética, uno de los problemas más relevantes con los que nos estamos encontrando en el Siglo XXI resultado del fenómeno de Internet, el de las redes sociales que constituyen vías consolidadas de relación e interacción cotidianas, no sólo de las nuevas generaciones de adolescentes y jóvenes, sino también de todo el conjunto de nuestra sociedad. Y pese a que la utilización de las nuevas Tecnologías de la Información y Comunicación ofrece grandes oportunidades y ventajas, no puede obviarse igualmente que éstas nos pueden situar en la sociedad del riesgo, por cuanto que pueden entrañar múltiples peligros, entre los que cobra una especial relevancia la posibilidad de conculcación de los derechos fundamentales a la intimidad, al honor, a la propia imagen y a la protección de datos personales, bien individualmente considerados o, bien de forma conjunta, acrecentándose los citados riesgos entre jóvenes y adolescentes, en cuanto usuarios indiscriminados. Pero, a éstos se añaden además otros riesgos por conductas delictivas, como el denominado Ciberacoso.

Abstract: This research recollects in a synthetic way, one of the most relevant problems the society is facing today, as a consequence of the Internet phenomenon. The routes of social Networks in the daily relations and interactions are consolidating in such a way that is not only affecting the young teenagers and the new generation, but also the whole of our society. In spite of the fact that, the utilization of new Technology of Information and Communication offer great opportunities and have many advantages, however, one should not ignore that this situation is putting the society at risk.

This phenomenon contains many dangers, as well as the possibility of violating the fundamental laws to intimacy, to the honor, to one's own image and to the personal data protection, being individually considered or as a whole form in conjunction of the mentioned risks between the youth and adults users. Moreover, there will be an increase of this risk, because of criminal behaviors as Ciber bullying.

Palabras Clave: Niños o nativos digitales, generación digital, en línea, fuera de línea, pulsar un click, privacidad, intimidad, redes sociales, sobrenombre, red de relaciones, acoso escolar y sexual en la red, cookies.

Key Words: *Digital babies o digital natives, native generation, on line, off line, click, privacy, intimacy, SRS, nick, networking, Ciberbullying, Grooming, nick, cookies*.

I. INTERNET Y LAS REDES SOCIALES: NUEVOS MEDIOS DE CIVILIZACIÓN

El profesor TRONCOSO REIGADA, en su intervención sobre redes sociales en la Conferencia Europea de Protección de Datos, cele-

brada en Edimburgo el 24 de abril de 2009[1] afirmaba que «todas aquellas personas nacidas después de 1995 son conocidas como *digital babies o digital natives*[2], o pertenecientes a la *digital generation,* un término que acuñó el tecnólogo Marc Prenssky en 2001 para definir aquellas personas que no han conocido –ni conciben– un mundo sin Internet y sin telefonía móvil. Desde que tiene uso de razón, esta generación de adolescentes y jóvenes, una gran mayoría de ellos menores de edad, se ha acostumbrado a la presencia constante de las modernas tecnologías de la información y de la comunicación, fenómeno éste que no nos es desconocido simplemente si miramos en nuestro entorno. Una de sus señas de identidad es que no sólo emplean las nuevas tecnologías, sino «que viven dentro de las redes sociales», donde pasan el tiempo compartiendo novedades y vivencias personales, segundo a segundo.

Tanto es así que según un estudio sobre Privacidad y Seguridad de la Información en las redes sociales *on line*, elaborado en España por el Instituto Nacional de Tecnologías de la Comunicación (INTECO)[3] y publicado junto con la Agencia Española de Protección de Datos el 12 de febrero de 2009, pone de relieve este fenómeno, ya que en España en 2008, 7 de cada 10 usuarios eran menores de 35 años; el 32,5 % entre 24 a 35 años, y el 36,5 % por ciento entre 15 a 24 años. Las redes son mayoritariamente utilizadas para compartir o subir fotos (70,9%), enviar mensajes privados (62,1 %) o comentar las fotos de los amigos (55 %). En un estudio elaborado en el Reino Unido se concluye que el 27 % de los niños de 8 a 11 años dicen pertenecer a una red social, aunque todas en principio, prohíben la entrada a los menores de 13 años e indica que del total de jóvenes entre 14 y 18 años, cuando se despiertan por la noche, un 29 %, lo primero que hace es mirar y hablar por las redes sociales, y el 37 % de estos jóvenes cuando se levantan por la mañana, la primera acción es la de comunicarse a través de la red social. Y es que el objetivo primordial en el ámbito de las redes sociales para adolescentes y jóvenes, no es otro que facilitar las relaciones personales, la comunicación instantánea, así como fomentar el ocio entre los usuarios que las componen, o inclu-

[1] TRONCOSO REIGADA, A.; *La protección de datos personales. En busca del equilibrio*. Valencia 2010, pag.1687.

[2] Sobre el concepto de *digital natives*, ver MARKBAUERLEIN, The *Dumbest Generation: How the Digital Age Stupefies Young Americans and Jeopardizes Our Future (Or, Don't Thust anyone under 30*.Tarcher.2008.; La George Lucas Foundation está desarrollando un interesante proyecto sobre la generación digital. *Vid.* http://www.edutopia.org/digityal-generation.

[3] www.inteco.es.

so en el ámbito profesional, siendo un punto de encuentro entre los miembros de las mismas. A dichos extremos, se refiere PIÑAR MAÑAS[4], cuando además indica que según ha comprobado el *Information Commisioner* de Reino Unido tras una encuesta a más de 2000 menores realizada en 2009, casi el 60 % de los preguntados no han considerado nunca que la información que colocan en Internet puede en el futuro permanecer *on line* disponible para terceras personas. Los conceptos de la privacidad y la intimidad entre los nativos digitales están cambiando, y sin embargo hemos de ser conscientes de que son requisitos necesarios para mantener una mínima calidad de vida[5].

Y es que la red social, en cuanto tal, es esencialmente una aplicación *on line* que está permitiendo a los menores y jóvenes usuarios de la misma generar un perfil con sus datos en páginas personales y compartirlo con otros, donde además se hace pública esta información, lo que facilita la interrelación entre todos ellos, sin que existan fronteras ni espaciales, ni temporales. Como además cuando se inscriben en una red social, ésta te anima a invitar a las personas con las que ya tienes una relación, incorporando el listado de personas a los contactos de correo electrónico, ese conjunto de datos fluye por la Red, podríamos afirmar que «sin control», por una parte consecuencia de que la gran mayoría de usuarios no tiene pudor alguno en introducir todo tipo de datos personales, incluidas fotografías para que toda esa información pueda ser compartida, y por otra, porque todavía no se aplican sistemas reales de seguimiento, control y supervisión de esa información.

Si bien es verdad que, inicialmente los contactos de una red social estarían compuestos únicamente por aquellas personas con las que ya se dispone de una relación *off line*, ello no es óbice, para que esta red de contactos posteriormente se vaya progresivamente ampliando. Resulta incuestionable, que las redes sociales cuentan con pocas restricciones preestablecidas, con la finalidad de fomentar un libre acceso a los perfiles que se van ampliando progresivamente con el incremento del número de contactos de cada usuario, de tal manera que se permite que los usuarios accedan no sólo a la lista de contac-

[4] PIÑAR MAÑAS, J. L.; Capítulo El Derecho Fundamental a la protección de datos y la privacidad de los menores en las Redes sociales de la Obra colectiva *Redes Sociales y Privacidad del Menor*. Madrid 2011. Págs. 63-65.

[5] TRONCOSO REIGADA, A.; Opera citada pág.1693. Nnp. 16, recuerda que «Carecer de privacidad-que toda la información personal sea pública-afecta a la propia identidad y a la libertad ya que la actuación tiende a ajustarse a unas pautas previamente esperadas». Se distinguen los círculos de intimidad y privacidad.

tos amigos, sino también a aquellas de los amigos, y de los amigos de éstos. A través de la utilización de las redes sociales, se facilita a los usuarios no sólo buscar, sino ser buscados por otras personas, de tal manera que el usuario puede agregarlas a su grupo de conocidos, dando a su vez, la posibilidad también a éstos de conocer a personas con las que se ha entrado en contacto. A mayor abundamiento, las redes sociales permiten generar grupos de interés, en virtud de los datos personales contenidos en los perfiles de usuarios. De esta forma, se aprovecha la red social para contactar con personas que ya conocemos, pero también para ampliar el circulo de personas de contacto, iniciando vínculos con personas desconocidas. Tal es la profusión en el uso de estas redes sociales que permiten que sus usuarios estén constantemente compartiendo aficiones, fotografías, vivencias personales, de tal manera que entre los adolescentes fundamentalmente, se haya llegado a sustituir mediante los *chats* tanto el correo electrónico, como incluso la televisión. Este fenómeno llega al extremo de producir la circunstancia de que los jóvenes dejan, incluso, de ver la televisión porque les aburre –les parece algo estático– y, prefieren la red social que les permite estar con contacto con mucha gente y saber qué pasa, por ejemplo, con las fotos que se van colgando y compartiendo. Desde este planteamiento, hay que reconocer que una persona está más aislada frente a un televisor que delante de un ordenador de mesa o de un portátil.

1. Estado de la cuestión

La Comisión Europea ha señalado que en el 2012 serán 120 millones los europeos que tengan un espacio en Internet. Las redes sociales tienen ya más de 270 millones de usuarios en todo el mundo, indicando los estudios más recientes que, algo más de nueve de cada diez jóvenes, dicen haber participado o accedido a una de estas redes sociales *on line* y, ocho de cada diez jóvenes afirman tener su propio perfil en alguna de estas comunidades digitales. El Informe de la Fundación Pfizer sobre «La juventud y las Redes Sociales en Internet» de Septiembre de 2009, señala que un 92 % de los jóvenes españoles entre 11 y 20 años son usuarios de redes sociales[6].

El impacto de las tecnologías de la interrelación y de la comunicación, en todos los órdenes de la sociedad actual, ha venido a configurar una serie de escenarios imprevisibles hace tan sólo unas déca-

[6] TRONCOSO REIGADA, A.; Opera citada pág. 1689 Nnp. 6.

das. Una de sus consecuencias es la denominada sociedad del riesgo. Internet, baluarte de la Sociedad de la Información, es una herramienta impresionante para tratar datos personales, y entre ellos los referentes a imágenes, sonidos y otros datos identificativos de las personas. Esta vía permite facilitar dichos datos, pero además igualmente recabarlos subrepticiamente. La popularización de uso y el fácil acceso a ella, sin controles reales, su gratuidad y sus múltiples usuarios, entre los que destacan los adolescentes y jóvenes, han traído como resultado además de múltiples ventajas en el ámbito del conocimiento y el incremento de las relaciones interpersonales, también agresiones a los derechos fundamentales a la imagen y protección de datos, sin perjuicio de la existencia de lesiones también a otros derechos. Como mantiene CASTELLS[7] «la evolución de la red favorece la generación de comunidades, tanto por medio del traslado del mundo virtual de grupos sociales preexistentes, como mediante la creación de grupos de interés de ámbito global».

En efecto, la Web 2.0, en cuanto estructura colaborativa, comporta el nacimiento de un universo social propio, poblado de comunidades que pueden ir de lo más cercano a cualquier grupo horizontal –grupos profesionales o sociales–, como verticales–, espacios de trabajo en grupo, e incluso el informar sin límites de espacio o tiempo». Y es que según señala RATZINGER «el hombre no puede ser privado de su dimensión relacional, que es parte de él mismo, y que necesita para llegar a ser él mismo»[8]. En esta misma línea, mantiene TRONCOSO REIGADA «aislar a un hijo de las redes sociales, prohibírselas, es posiblemente, condenarle al desarraigo. El acceso a Internet es un derecho fundamental de la persona, lo que no quiere decir que no tenga que estar sometido a límites, que requieren de una regulación legal y un control judicial, sin perjuicio de la posible intervención en el ámbito de autoridades administrativas independientes»[9].

Y una de las cuestiones más relevantes que nos estamos encontrando, es precisamente, la que se produce respecto de las imágenes como consecuencia de la prestación de determinados servicios que son ofrecidos por los prestadores de servicios de las redes sociales y, en la mayoría de los casos de forma gratuita y fácilmente accesibles, siendo estos en multitud de ocasiones contrarios a la dignidad de la persona, la juventud y la infancia, y sin embargo cada día más utilizados.

[7] CASTELLS, M.; *La galaxia Internet*. Barcelona 2001. Pág. 139.
[8] RATZINGER, J.; *La sal de la tierra*, Madrid, 5º ed. 2005, pág. 178.
[9] TRONCOSO REIGADA, A.; Opera citada, pág. 1691.

A nivel de la Comunidad Internacional, existen una serie de Recomendaciones elaboradas por diferentes instituciones en relación al uso de Internet por menores, como el Programa Comunitario del Parlamento Europeo para reforzar la protección de los niños en Internet, a través de la reducción de los contenidos ilícitos; el Proyecto *Dadus* en Portugal; el Proyecto *Prometeo*, que ha contado con distintas Agencias de Protección de datos españolas.

Las propuestas tanto de Directiva del Parlamento Europeo y del Consejo ambas de 25 de enero de 2012, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de datos, así como la de Reglamento de protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de Protección de datos) establecen con carácter general, no sólo mayores obligaciones de control para los Estados, sino además mecanismos de coherencia para esa cooperación entre las autoridades de control, creando incluso un nuevo órgano denominado Consejo Europeo de Protección de Datos, entre cuyas tareas se incluirá la del examen, bien a iniciativa propia, como de cualquiera de sus miembros o de la Comisión, no sólo de cuestiones relativas a la aplicación del Reglamento, sino la emisión de directrices, recomendaciones y mejores prácticas dirigidas a las autoridades de control, a fin de proceder a la aplicación coherente del mismo, así como la promoción de la cooperación e intercambio bilateral y multilateral efectivo de información y de prácticas entre las autoridades de control.

A mayor abundamiento, la propuesta de Reglamento introduce el artículo 8 específicamente en relación con el tratamiento de datos personales de los niños, en el que se distingue el tratamiento de los datos personales relativos a los menores de 13 años, indicando que éste sólo será lícito si el consentimiento ha sido dado o autorizado por el padre o tutor del niño, así como fijando la obligación del responsable del tratamiento de efectuar esfuerzos razonables para obtener un consentimiento verificable, teniendo en cuenta la tecnología disponible, junto con otra serie de mecanismos y atribuciones a la Comisión de la Unión Europea, en adelante UE, para establecer formularios normalizados para los métodos específicos de obtención de un consentimiento verificable, así como obligaciones de efectuar evaluaciones de impacto relativas a la protección de datos, especialmente cuando entrañan riesgos específicos como es el su-

puesto de los tratamientos de datos personales a gran escala relativos a los niños, al tiempo que el de datos genéticos o biométricos[10], fomentando además la confección de códigos de conducta para la debida aplicación de todo lo dispuesto en el Reglamento futuro.

No obstante lo indicado, a nivel nacional, en el ámbito normativo el legislador español promulgó la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, previéndose en su Art. 8.1 que, cuando un determinado servicio ofrecido en la red sea contrario a la dignidad de la persona, la juventud o la infancia, podrá ser interrumpida la prestación del servicio o eliminados de él los datos que vulneren dichos principios. Es decir, la Ley establece una serie de medidas que son de utilidad para preservar la privacidad del ciudadano, y por supuesto el interés del menor ante la posibilidad de vulneración de los derechos fundamentales del menor de edad a través de la Red.

La circunstancia de que las imágenes se incluyan como datos de carácter personal, determina la existencia de una importante relación entre propia imagen, protección de datos personales y el derecho a la identidad de uno mismo y en definitiva, de la privacidad, tal como ésta es concebida en el ordenamiento jurídico de los Estados de nuestro entorno. No solo es que estos derechos fundamentales compartan en muchos casos sede constitucional, como es el supuesto de nuestro ordenamiento, sino también el objetivo de ofrecer una eficaz protección constitucional a la propia imagen y el tratamiento de ésta como un dato de carácter personal, y máxime considerando la especial protección que debe dispensarse a la infancia y la adolescencia, en el ámbito de las redes sociales que este colectivo utiliza habitualmente como forma de relación.

Y el hecho es que se requiere la creación de un entorno más seguro en Internet para garantizar la privacidad a nivel mundial, entorno que habrá de ser compatible con la constitución y regulación de las redes europeas, a través de centros que permitan la localización y denuncia ágil de la existencia de contenidos ilícitos, como ocurre en Bélgica, donde la policía judicial posee una línea directa para la denuncia de situaciones o páginas de contenidos pornográficos, al igual que ocurre en nuestro país con las líneas de la Guardia Civil y la Policía Nacional.

[10] Propuesta de Reglamento de 25 de enero 2012, artículo 33.

2. Privacidad e Internet

No nos resulta extraño que «una foto puede acabar con una exitosa carrera», así concluía una noticia relativa al mundo del fútbol femenino. Esto es lo que ocurrió con una de las jugadoras más emblemáticas de un club español de fútbol, que sufrió las consecuencias del hecho de que una foto suya se colgara en *Facebook*, y pese a que la borró enseguida, ya fue tarde. La foto empezó a circular por Internet y, generó como consecuencia última, la resolución del contrato que tenía con su equipo de fútbol, por entender los directivos del equipo que la foto atentaba a su sensibilidad y la de los seguidores del club. Esta y otras muchas consecuencias se pueden derivar de esta circunstancia, inicialmente sin importancia. VILASEU SOLANA[11] se refiere, precisamente, a este hecho, e «incide en que se muestra como una circunstancia tan banal e insignificante como una determinada fotografía de una persona en determinada actitud o circunstancias, al acceder a Internet y a una red social cobra relevancia y adquiere unas dimensiones totalmente inesperadas».

Sobre el surgimiento de las redes sociales, hemos de indicar que las primeras redes sociales hicieron su aparición a finales de los años 90, fueron consolidándose entre 1997 y 2001 y, se consagraron a partir de 2002, *Friéndster* hizo su aparición en 2002 y *My space* en 2003[12], afluyendo los adolescentes de forma masiva a esta última red a partir de 2004. *Facebook* inició su actividad en 2004, originariamente como una red exclusivamente para estudiantes de Harvard, y posteriormente poco a poco, *Facebook* empezó a abrirse a otras Universidades para, a principios de 2005, expandirse para incluir profesionales dentro de redes corporativas, y finalmente a partir del 2006, se abrió a todo el mundo. Ni tan siquiera, el joven creador de *Facebook* pensó nunca que las consecuencias de su innovación alcanzaran las cotas que con el tiempo ha ocupado, máxime en los países anglosajones. No obstante, existen otras redes como *Orkut* –con mayor presencia en la India y Brasil–, o en España es la red nacional *Tuenti* la que goza de un mayor número de usuarios.

Sobre lo que no existe discusión es que se trata de un fenómeno social que crece exponencialmente y resulta ser imparable, que pre-

[11] VILASEU SOLANA, M.; *Privacidad, redes sociales y el factor humano*, en la obra coordinada por RALLO LOMBARTE, A. y MARTÍNEZ MARTÍNEZ, R. *Derecho y redes sociales*. Reus 2010. Pág. 55.

[12] D. BOYD y N. ELLINSON, «Social Networks sites: Definition History and Scholarship», *Journal of computer mediated communication,*13, article 11, http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

cisa de regulaciones ante los múltiples peligros que entraña, principalmente en el ámbito de la privacidad del individuo y de los derechos fundamentales del Art. 18.1 y 18.4 CE. Y a ello se ha de añadir que siendo una cuestión especialmente compleja se ha de tomar en serio, por cuanto que encierra amenazas para la privacidad y la seguridad que en absoluto se pueden desconocer, pues además según el Cisco 2010 *Annual Security Report,* las redes sociales son utilizadas cada vez más como instrumento por el cibercrimen que busca extender sus operaciones por todo el mundo[13].

Ahora bien, tampoco hemos de obviar el hecho, de que el concepto de privacidad está variando, fundamentalmente en el ámbito de los denominados *digital natives,* que anteponen la comunicación y la interrelación, a la intromisión en su propia privacidad. Se trata de un colectivo que ha nacido en la era de la Web 2.0, compuesto por los jóvenes y adolescentes para los que los móviles, ordenadores, *Smartphone, iphone,* etc., son ya herramientas de comunicación y de interrelación, que proporcionan un mundo similar al mundo real, y que en múltiples ocasiones no ha alcanzado el grado de madurez necesario para la comprensión de las consecuencias que genera el uso de las redes sociales y de la información personal que discurre por las mismas. De ahí la necesidad de reforzar la educación y formación en estos ámbitos entre los menores.

No obstante lo anterior, VILASEU SOLANA[14] opina «considero que no debe abandonarse este terreno pero soy un tanto escéptica respecto de la eficacia de la formación. Por ejemplo, en el caso de España, a pesar de que la población declara sentirse preocupada por la privacidad, parece que esta inquietud se diluye un poco cuando el sujeto accede a un entorno virtual»[15]. En concreto, después de manifestar la preocupación por la privacidad, gran parte de los internautas reconocen que no leen las políticas de privacidad de las páginas Web que visitan[16].

---

[13] Pág.11 del Informe. Puede consultarse en http//mikemeikle.com/wp-content/uploads/2011/02/Cisco-Annual-Security-Report.2010.pkf.

[14] VILASEU SOLANA, M.; *Privacidad, redes sociales y el factor humano*, en la obra coordinada por RALLO LOMBARTE, A. y MARTÍNEZ MARTÍNEZ, R. *Derecho y redes sociales*. Reus 2010. Pág. 74.

[15] Así se desprende del Barómetro del CIS de Septiembre de 2009. Estudio un.2812 (http://www.cis.es/cis/opencms/ES/Novedades//Documentación_2812.html).

[16] En el citado Barómetro del CIS, la pregunta 16.f hace referencia a la frecuencia con la que se leen las políticas de privacidad de las páginas de internet que se visitan. El 21,7 % de los usuarios de Internet declaran hacerlo *algunas veces,* el 26,2 % declaran que *raramente* y el 35,6% dicen que *nunca* (Téngase en cuenta que esta cuestión se plantea sólo a los encuestados que han declarado haber hecho uso de Internet durante los últimos 12 meses, que son el 55,8 % del total de encuestados).

De alguna manera parece que al acceder a Internet y a una plataforma social, surgen otras prioridades y la privacidad pasa a un segundo plano. La persona tiene otras motivaciones; principalmente comunicarse –y hacerlo de forma rápida– y poder acceder a determinado contenido. Impaciencia y avidez de información serían las características de esta forma de comunicarse.

La conclusión como veremos a lo largo de este estudio, es que existen grandes retos a la privacidad del menor en las redes sociales: nos encontramos ante un mundo que se ha montado hace tan solo unos años y en el que sin embargo todos somos intérpretes, mucho más los menores, pese a que no siempre conozcan el papel que representan, y sobre esta necesidad de una adecuada formación de los jóvenes y adolescentes, resultan muy interesantes las observaciones y recomendaciones que realiza DANAH BOYD en «*Social* network sites: Public, Private or What?», cuando indica que «más que proporcionar reglas o normas se trata de interpelar a los jóvenes, plantearles cuestiones relativas al uso de las redes sociales y a las consecuencias que pueden comportar utilizarlas»[17].

«También es imprescindible que las agencias de protección de datos, desde su independencia, especialización y autoridad, tutelen el derecho a la privacidad de los menores no siempre fácil en el marco globalizado en el que operan las redes sociales», tal como mantiene PIÑAR MAÑAS[18].

II. LA DEFINICIÓN DE RED SOCIAL, REGULACIÓN LEGAL Y TIPOS

Las redes sociales *on line* son hoy un ejemplo más de la Web 2.0 o de la denominada Web colaborativa, en la que Internet deja de ser un foco de información, para convertirse en un espacio virtual retroalimentado en el que los usuarios consumen, pero también aportan múltiple información.

Podemos pues definir de una forma genérica, una red social *on line* como aquellos servicios de la sociedad de la información que ofrecen a los usuarios una plataforma de comunicación a través de

[17] VILASEU SOLANA, M.; *Privacidad, redes sociales y el factor humano*, en la obra coordinada por RALLO LOMBARTE, A. y MARTÍNEZ MARTÍNEZ, R., *Derecho y redes sociales*. Reus 2010. Pág. 74 Npp (52).

[18] PIÑAR MAÑAS, J. L.; «*Redes Sociales y Privacidad del menor*». Fundación Solventia. Madrid 2011, pág. 23.

Internet para que estos generen un perfil con sus datos personales, facilitando la creación de redes en base a criterios comunes y permitiendo la conexión de unos usuarios con otros y su interacción. De esta forma, se crea el fenómeno más relevante que es el de las vinculaciones entre usuarios miembros de las redes. Estas se miden en grados, donde el primer grado sería los contactos directos, el segundo grado el contacto de los contactos y así sucesivamente, de tal manera que a mayor número de usuarios mayor número de vinculaciones, y por tanto incremento de la Red. Y sobre este fenómeno se crea la teoría de los 6 grados de separación, es decir que el número de enlaces crece exponencialmente con el número de enlaces de la cadena.

Además, otro hecho reseñable es que el acceso a las redes sociales se viene incrementando con la aparición de nuevos herramientas y dispositivos de acceso a Internet, como los *Smartphone* que permiten la conexión en cualquier momento y lugar, fenómeno éste que además acrecienta aún más los posibles riesgos a la privacidad.

Desde el ámbito jurídico se entiende por red social, a tenor de lo preceptuado por el Grupo de Trabajo sobre Protección de Datos del artículo 29 el 12 de junio de 2009[19], en su Dictamen 5/2009 sobre redes sociales en línea: «*Los SRS pueden definirse generalmente como plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes. En sentido jurídico, las redes sociales son servicios de la sociedad de la información, según se definen en el Art. 1, apartado 2 de la Directiva 98/34/CE, modificada por la Directiva 98/48/CE. Las SRS comparten determinadas características: –los usuarios deben proporcionar datos personales para generar su descripción o perfil; –Los SRS proporcionan también herramientas que permiten a los usuarios por sí propio contenido en línea. (Fotografías, comentarios, videos, etc.); –las redes sociales funcionan gracias a la utilización de herramientas que proporcionan una lista de contactos para cada usuario, con las que los usuarios pueden interactuar. Los SRS generan la mayoría de sus ingresos con la publicidad que se difunde en las páginas Web que los usuarios crean y a las que acceden. Los usuarios que publican en sus perfiles mucha información sobre sus intereses ofrecen un mercado depurado a los publicitarios que desean difundir publicidad específica y basada en la información. Es por tanto importante que los SRS funcionen respetando los derechos y libertades de los usuarios, que tienen la expectativa legítima de que los datos personales que revelan sean tratados de acuerdo con la*

[19] Pues ha sido instituido por el Grupo del artículo 29 de la Directiva 95/46/CE de protección de datos.

legislación europea y nacional relativa a la protección de datos y la intimidad».

Y desde esta definición, se extrae que las redes sociales en línea son nuevos entornos de comunicación y de relación *on line*, que por sus especiales funcionalidades, han tenido un enorme éxito.

Si pensamos en los distintos y variados servicios que prestan al usuario las distintas redes sociales *on line*, comprobamos como pueden tener finalidades diferentes, lo que genera una multiplicidad de ellas, que a su vez se pueden clasificar en distintos tipos:

— Redes sociales de comunicación, entre otras *Facebook, Tuenti, Myspace*, etc. Siendo estas plataformas en las que el usuario se puede dar de alta en el servicio libremente, o a través de invitación y encontrar conocidos o invitarles a formar parte de su comunidad. Este tipo de redes permiten la vinculación entre los usuarios con contactos de segundo o tercer grado o gente que pertenece a los mismos grupos, como pueden ser miembros de colegios, universidades, etc. En estas redes se suelen publicar fotografías, videos, reflexiones, aficiones y preferencias de todo tipo.

— Redes sociales especializadas, cuya finalidad suele unir a colectivos con unos mismos intereses, como la de niños, *mi cueva.com*; *virtualtourism.com* para viajeros, *flickr.com* para compartir fotografías, *Twister.com* para recibir y enviar mensajes breves, para encontrar pareja como *Meetic*, etc.

— Redes sociales profesionales, como *Linkedln*, *Xing*, que permiten a los individuos de todo el mundo buscar oportunidades de empleo, hacer *networking* con compañeros de trabajo, con gente del ámbito profesional. Estas tienen un público más especializado, y su modelo de financiación está basado en venta de servicios Premium o en la realización de campañas de publicidad personalizada.

Si mencionamos la regulación legal a la que se encuentran sometidas las citadas redes sociales, indicar que a pesar de las diferencias entre las distintas redes y su singular configuración en el ámbito de la UE, sin embargo todas ellas se someten al mismo marco jurídico general, recogido en la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, de protección de las personas frente al tratamiento de sus datos personales y de su libre circulación, encontrándose en tramitación tanto la Propuesta de nuevo Reglamento que lleva fecha de 25 de enero de 2012, ya mencionado ante-

riormente, como la de Directiva de protección de datos de igual fecha, tratando ambas disposiciones en curso de establecer una normativa que se adapte con mayor rigor a las transformaciones, nuevas circunstancias y presupuestos de hecho que realmente genera el mundo de las TIC en el ámbito de la protección de los datos de las personas.

No obstante, muchas de las citadas cuestiones han sido objeto de pronunciamiento en la 30ª Conferencia Internacional de Privacidad, celebrada en Estrasburgo[20] en octubre de 2008, que aprobó la Resolución sobre Protección de la Privacidad en las Redes Sociales. También en el Memorándum de Roma, del Grupo internacional de Berlín sobre Protección de Datos de las Telecomunicaciones, de marzo de 2008. Y especialmente el Dictamen 5/2009 del Grupo de Trabajo sobre Protección de Datos del Art. 29, de 12 de junio de 2009, sobre las redes sociales en línea.

Por su parte, la Agencia Europea de Seguridad de las Redes y de la Información, ENISA[21], ha elaborado toda una lista de riesgos potenciales del uso de las redes sociales en 2007, agrupado en «*Security Issues and Recomendation for on line Social Networks*»[22]. Durante los días 26 al 28 de mayo de 2009 se celebró el I Seminario Euro-Iberoamericano de Protección de Datos en la ciudad de Cartagena de Indias (Colombia) que tuvo el tema la Protección de los menores, y en la que se analizaron entre otros temas el de los menores y la sociedad de la información, los menores y las telecomunicaciones y los menores e Internet, con especial referencia a las redes sociales. En su Informe Anual publicado en 2007 por Ipsos Insight «The Face of the Web»[23], se señalaba que las redes sociales iban a convertirse rápidamente en el fenómeno global dominante en la Red.

Uno de los mayores problemas que se plantean, por la propia naturaleza de Internet –y de estas redes sociales– que facilita las relaciones con personas de ámbitos geográficos muy alejados, es precisamente la Ley aplicable cuando algunas redes sociales tienen su sede fuera del ámbito por ejemplo de la UE, máxime considerando la multitud de datos personales que se tratan, lo que genera dudas muy relevantes respecto de la determinación de la misma, en un escenario en que la legislación se mueve en términos de territorialidad, existiendo respecto de los actores verdadera ausencia de límites espacia-

[20] www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_en.pdf.
[21] www.enisa.europa.eu.
[22] TRONCOSO REIGADA, A.; Opera citada pág. 1693 Nnp.17.
[23] http://www.ipsosinsight.com/.

les. En efecto, si nos referimos al marco jurídico que soporta la regulación de las redes sociales, podríamos mantener que, a pesar de contarse con iniciativas nacionales e internacionales sobre la protección de datos de los menores en el ámbito de las redes sociales, sin embargo tanto éstas, como los resultados alcanzados han sido hasta la fecha claramente insuficientes para garantizar la adecuada protección, y seguridad jurídica.

Es cierto, que han existido esfuerzos y contribuciones importantes en estas materias, como el relativo al Primer Encuentro Euro-Iberoamericano de Protección de Datos que tuvo lugar en Cartagena de Indias en mayo de 2009, ya mencionado, en el que se analizó la cuestión de la protección de datos de los menores. También cabe destacar el llamado Memorándum de Roma, aprobado en marzo del 2008 por el Grupo de Berlín, el grupo de Telecomunicaciones (*International Working Group*), sobre la protección de datos en el ámbito de las telecomunicaciones, o la Resolución sobre la protección de la privacidad en los Servicios de las Redes Sociales adoptado en la 30ª Conferencia de Protección de Datos y Privacidad, celebrada en Estrasburgo en octubre de 2008, o el Memorándum sobre la protección de los datos personales y la vida privada en las redes sociales en Internet en particular, de niños, niñas y adolescentes, conocido como Memorándum de Montevideo, pues fue elaborado por los asistentes al *Seminario Derechos, Adolescentes y Redes sociales en Internet* realizado en Montevideo Uruguay, los días 27 y 28 de julio de 2009.

No obstante, se puede constatar que, como consecuencia del alto riesgo que este mundo virtual conlleva, y de la falta de percepción de estos peligros para los menores, a lo que se añade la carencia de regulación, se va tomando conciencia de la necesidad de regulación y mayor control, no sólo vía de normativas estatales, sino también a través de sistemas y procedimientos de autorregulación y de Códigos de Conducta, que como hemos señalado también se contemplan en las propuestas de Directiva y nuevo Reglamento de Protección de datos, ambos de fecha 25 de enero de 2012.

Tanto ello es así, que las propias redes sociales en sus normas de regulación, existentes ya en Internet, están dando pasos en aras de la salvaguarda de la privacidad, así como de controlar una forma de operar con respecto a los menores, y en particular, en lo referente al aseguramiento del otorgamiento del consentimiento y de su validez, o el de sus padres o tutores, poniendo el acento en la acreditación de su veracidad, con el fin de evitar riesgos como los derivados de la suplantación de identidad. Existe, por consiguiente un compromiso

cada vez mayor con la protección de datos personales y los menores. No obstante, a pesar de estos pasos sobre la autorregulación por las propias plataformas de servicios *on line*, se requiere de la elaboración de Códigos de Conducta y/o políticas claras y accesibles respecto de las cuales se exija su cumplimiento, acorde con las disposiciones de la legislación sobre protección de datos personales, que faciliten y garanticen su aplicación efectiva.

En el contexto de las varias veces citadas Propuestas de Directiva y Reglamento de la UE respecto de la protección de datos personales, conviene además resaltar el fortalecimiento de las vías de cooperación, control, seguimiento y coordinación entre las distintas autoridades de control de los estados de la Unión, precisamente para tratar de solventar los problemas que se derivan tanto de la globalización de este mundo virtual, como de la extraterritorialidad en que se mueven las redes sociales.

Con independencia de la aplicación de lo expuesto, si concretamos el escenario español, a nivel de las autoridades nacionales cabe destacar la preocupación de todas las Agencias de Protección de Datos existentes, tanto estatal como autonómicas, por establecer medidas de actuación. Las autoridades de protección de datos han elaborado múltiples materiales a fin de implementar las políticas de educación e información dirigidas a la población más joven y vulnerable. Recordar que la propia Agencia Española de Protección de Datos, en adelante la AEPD, creó una sección especial en su página web dedicada a los menores, con material diverso: guías, recomendaciones, videos y estudios para facilitar y potenciar la educación de los menores en relación con la privacidad y los riesgos a la misma[24].

A mayor abundamiento, en relación con nuestra propia normativa, podemos mantener que la legislación que se utiliza con carácter general la Ley Sobre los Servicios Información mencionada y, con carácter particular, la siguiente normativa en función de la materia:

En el ámbito de la privacidad:

— Ley Orgánica 15/1999, de 15 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo, aprobado por el R.D. 1720/2007, de 21 de diciembre.

— La Ley Orgánica 1/1982, de 5 de mayo, de Protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen.

[24] http*://www.agpd.es/portalweb/canalciudadano/menores/index-ides-idphp.php*.

— Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

— Así como aquellas otras de ámbito autonómico igualmente referida a los menores.

En el ámbito de los delitos y faltas:

— La Ley Orgánica 10/1995, de 23 de noviembre, de Código Penal.

En el ámbito de la propiedad intelectual e industrial:

— La Ley 23/2006, de 7 de julio, por la que se modifica el Texto Refundido de la Ley de Propiedad Industrial, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril.

— La Ley 17/2001, de 17 de diciembre, de marcas.

Y para el resto de asuntos que puedan surgir se utiliza el resto de normas vigentes como la Ley General de Publicidad, la de Competencia Desleal, la normativa sobre comercio minorista o contratación a distancia, o incluso la Ley de Comercio electrónico, o la aplicable para un sector regulado como es el de las telecomunicaciones.

Por tanto, en una primera aproximación, podríamos entender que existiría una regulación suficiente a nivel nacional, completada además, a nivel de la Unión Europea, con «Los Principios de Redes Sociales Seguras», redactados con la colaboración de la industria de las SRS, siendo la pretensión de los mismos principalmente la mejora de la protección de la privacidad, de los datos personales, de la concienciación de los usuarios así como información sobre seguridad que todo SRS ha de tener. A estos Principios se han adherido ya más de 20 SRS en Europa. Y, por último, otro tercer bloque de normativa sería el de «Las Condiciones de Uso y Políticas de Privacidad» de cada una de las redes sociales, a las que se tendrán que ir incorporando los diversos Códigos de Conducta que se vayan estableciendo y siendo aplicables de forma efectiva.

Ahora bien, de toda la citada normativa podríamos llegar a considerar que se encuentran plenamente garantizados los derechos de los usuarios y, sin embargo, constatamos que la realidad, es muy otra, pues nos sitúa ante situaciones conflictivas o de vulneración de derechos fundamentales, e ilícitos penales que se incrementan cada día, determinando este panorama la necesidad de ahondar sobre la problemática que éstas plataformas generan, respecto de los usuarios y sus derechos.

Téngase en cuenta que el Grupo de Trabajo del artículo 29, en el Dictamen 5/2009, señala que las disposiciones de la Directiva 95/46/CE relativa a la Protección de datos personales se aplican en la mayoría de los casos a los proveedores de servicios de redes sociales, aunque su sede se encuentre fuera de la Unión Europea, y ya en la Propuesta de Reglamento de 25 de enero de 2012 sobre protección de datos personales se incorporan disposiciones especificas tendentes a una mayor regulación y control efectivo y coordinado.

En tal sentido, señala el Art. 4 de la Propuesta de Directiva de 25 de enero de 2012 que, serán de aplicación las disposiciones nacionales que traspongan la Directiva a todo tratamiento de datos cuando el responsable esté establecido en la Unión europea, pero que recurra para el tratamiento de datos personales, a medios situados en el territorio de dicho Estado, salvo que tales medios se utilicen únicamente con fines de tránsito.

La realidad es que las redes sociales disponen tanto de medios ubicados dentro de la Unión Europea, como fuera no sólo por la utilización de *cookies o banners*, sino porque la recogida de datos se produce en parte dentro de la Unión Europea y claro está en parte en terceros estados. En este sentido, el Grupo de Trabajo del Art. 29 estima de acuerdo con lo establecido en el Dictamen 5/2009, y dictámenes anteriores, que existen cuestiones en materia de establecimiento y utilización de equipos, que son determinantes para la aplicabilidad de esta Directiva 46/95/CE, resultando muchos de dichos tratamientos excluidos del régimen de protección de datos al tratarse de «ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas». Y este es uno de los aspectos que vienen a ser tratados en la Propuesta de Directiva sobre Protección de datos de fecha 25 de enero de 2012.

Lo cierto es que la recogida de datos personales, incluidas las fotografías, por el proveedor del servicio de la red social de que se trate, así como las posibles cesiones tienen que hacerse mediante el correspondiente consentimiento, libre, inequívoco, especifico e informado del interesado; reseñando la Propuesta de Reglamento de protección de datos en diversos preceptos, aspectos claves como todo lo relativo a las condiciones del consentimiento (artículo 7), el tratamiento de los datos personales relativos a los niños (artículo 8), la licitud del tratamiento de datos (artículo 9) así como el tratamiento de datos que no permita identificación (artículo 10), en cuyo caso se establece expresamente, que en dicho supuesto el responsable del tratamiento no estará obligado a hacerse con información adicional

con vistas a identificar al interesado, en orden a cumplir lo determinado en el Reglamento. A ello se añade todo un capítulo entero, el III sobre los Derechos del interesado.

En definitiva, debe ser el usuario el que dé su consentimiento, estableciendo el nivel de acceso a su perfil personal –a sus amigos, a los amigos de sus amigos, a toda la red social o fuera de ella permitiendo o no la indexación por motores de búsqueda. Y este consentimiento se ejerce habitualmente aceptando la política de de privacidad establecida por defecto. Pero como veremos no siempre el consentimiento resulta ser un derecho del usuario, ni está libre de dificultades, ante por ejemplo cesiones de datos –fotografías– que se pudieren entender que se hacen para fines personales, familiares o domésticos y que estarían excluidos de la Directiva 95/46/CE, cual es el supuesto de imágenes de grupos de personas sin el preceptivo consentimiento de cada una de ellas.

Y lo expuesto, se ha de poner en relación con otra de las cuestiones que se plantean con respecto a las redes sociales y el ámbito de su regulación, es el gran número de contactos que se establecen, muchos de ellos realizados de forma indiscriminada, en cuanto petición de amistad sin que realmente exista una relación personal, cuestión ésta que además se incrementa en el ámbito de los menores, por lo que se viene efectuando una interpretación limitada del concepto de tratamiento personal o domestico. Este planteamiento se ha venido entendiendo como una exigencia del respeto debido a los derechos de las personas en las redes sociales, pues no tendría ningún sentido que no se pudiesen aplicar el derecho fundamental a la protección de la información personal, a tratamientos que suponen una cesión indiscriminada de datos, de terceras personas a un número muy amplio de usuarios.

Y es que la publicación de datos personales por el usuario de una red social, debe suponer la asunción de la responsabilidad del tratamiento, en relación con las personas cuyos datos o fotografías aparecen publicados en el perfil, lo que le está obligando al cumplimiento de los principios de la información y del consentimiento. En este sentido, el usuario será responsable en el ámbito jurisdiccional de las vulneraciones de los derechos de las personas que se deriven de la información incorporada a una red social. De ahí, que la recogida de datos personales por el proveedor del servicio de la red social, y sus posibles cesiones de datos requerirá el consentimiento libre, inequívoco, informado y especifico del interesado. Y este consentimiento, ha de ejercerse habitualmente aceptando la política de privacidad estable-

cida por defecto, cuando se opera a través de una red social. También sobre dichos extremos se establecen una serie de medidas en la Propuesta de Reglamento, en orden a garantizar la transparencia en los procedimientos y mecanismos para el tratamiento de datos y el ejercicio de los derechos por los usuarios, así como las destinadas a lo concerniente a la elaboración de perfiles de personas físicas, al igual que otras tendentes a evitar la suplantación de identidad, así como lo relativo al Derecho al olvido y a la supresión de los datos.

III. LA PROBLEMÁTICA DEL CONSENTIMIENTO EN LAS REDES SOCIALES *ON LINE*

En relación con la vida privada, uno de los mayores cambios que ha provocado el uso de las redes sociales, es el hecho de que la mayoría de la información personal que se publica en estos servicios se hace a iniciativa de los propios usuarios, con su propio consentimiento. Y es que, como venimos reiterando, tanto la normativa europea, como la española sobre protección de datos determinan que para la realización de tratamientos de datos de forma legítima se debe de cumplir con el principio relativo a la prestación del consentimiento, requisito indispensable y vertebrador de la protección de datos de carácter personal. Esta exigencia es recalcada incluso en la Propuesta de Reglamento de protección de datos de 25 de enero de 2012, donde se señalan de forma detallada tanto los Principios que han de presidir el tratamiento de datos personales, como las condiciones para el consentimiento, siendo interesante la referencia a que es el responsable del tratamiento el que asumirá la carga de la prueba respecto a que el interesado ha dado su consentimiento para el tratamiento de sus datos personales para determinados fines, tal como se dispone en el artículo 7. Se fijan asimismo determinados requerimientos específicos respecto del consentimiento de los menores de edad de 13 años, y de aquellos que sean mayores de dicha edad, distinguiendo además medidas en atención al tratamiento de determinadas categorías especiales de datos.

No obstante a pesar de los esfuerzos de regulación, se constata, que uno de los mayores problemas y peligros de las redes sociales, como luego señalaremos, se producen respecto de la intromisión ilegítima en la privacidad de los sujetos, incluido el derecho a ser uno mismo. Dar protección a la privacidad en el ámbito de las redes sociales, y en general, en el ámbito de la Sociedad de la Información, conlleva la necesidad de reinterpretar, adecuar y fortalecer el con-

cepto de protección existente hasta el momento. Es por ello que el requisito del consentimiento inequívoco como principio legitimador de todo tratamiento de datos personales, incluidas las imágenes, haya de adaptarse a los cambios que la tecnología y los nuevos servicios ofrecen.

Si mencionamos el concepto que la Ley Orgánica de Protección de Datos, en adelante LOPD, exige respeto del consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa, en cuanto «*toda manifestación de voluntad libre, inequívoca, especifica e informada*», tal como se define en el Art. 3 h) de la citada LOPD y, Art. 5.1 d) del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, en adelante RLOPD, disponiendo el Art. 2 h) de la Directiva 95/46/CE como «*toda manifestación de voluntad libre, especifica e informada, mediante la que el interesado consiente el tratamiento de datos que le concierne*». No obstante, el citado último precepto no se refiere, sin embargo, al término inequívoco con respecto al consentimiento. Pero lo cierto, es que alguna de las características formalmente exigidas del consentimiento plantea más de un problema en el ámbito de las redes sociales. En efecto, el consentimiento es libre cuando se presta por el usuario de la Red, el problema es que éste cuando lo presta, lo hace porque piensa que está en una red privada de amigos, entre otras cosas precisamente por los conceptos que se utilizan para denominar la «comunidad», o los «amigos».

En este sentido en la Declaración de la AEPD sobre buscadores de Internet de 1 de diciembre de 2007, se determina «*que las personas cuyos datos se tratan estén informadas de qué datos se van a utilizar, por quién, con qué finalidad y a quienes se pueden ceder sus datos*». La obligación incumbe a los proveedores o prestadores de servicios, si bien también está cambiando la tradicional forma de prestación del consentimiento por parte del usuario, que en las redes sociales se hace vía la formula de enlaces como «aviso legal» o «política de privacidad», a través del simple «*clic*», por lo que en muchas ocasiones el usuario ni tan siquiera ha leído realmente dicha normativa a su disposición, ni es consciente de la prestación de ese consentimiento. Y a estas dificultades se añade otra, esto es que el mayor número de usuarios que cada día se incorporan a las redes sociales, principalmente adolescentes o jóvenes, menores de edad en la mayoría de los casos, por lo que se requiere una mayor claridad y fácil accesibilidad a esa información, mediante la existencia de un lenguaje sencillo, al tiempo que sea ineludible para poder continuar con el uso del servicio, al margen lógicamente de las necesarias autorizaciones correspondientes por padres o representantes, en función de la edad del usuario.

Por la existencia de toda esta problemática mencionada, es por lo que no solo es necesario el consentimiento especifico, sino que además se debe dar un plazo más amplio para que el afectado pueda claramente tener conocimiento del tratamiento que, en su caso se está efectuando sobre su fotografía o resto de datos personales subidos a la Red. Y a mayor abundamiento, con respecto a los datos sensibles, lo aconsejable será no admitir por tanto, consentimientos tácitos, debiéndose exigir por parte de los responsables de los tratamientos, la existencia de un consentimiento expreso e inequívoco, requiriéndose en todo caso, para los menores el de los padres o tutores, en función de la edad y que éste pudiese ser claramente verificable.

Para concluir, podemos afirmar que, por regla general, dado que en los servicios de las redes sociales, la recogida de datos se producirá en el momento en que el usuario se da de alta vía web que, el consentimiento haya de recabarse de tal forma que resulte imposible la introducción de dato alguno sin que previamente el afectado haya conocido la advertencia que contenga las menciones a las que nos hemos referido, pudiendo servir como prueba del otorgamiento de ese consentimiento, la acreditación de que el programa impide introducir los datos sin antes haber aceptado el aviso legal, correspondiendo al prestador de servicios la prueba de la acreditación de la obtención.

Es a través de dichas medidas, como se podrá asegurar que la prestación del consentimiento de los afectados es realmente específica e inequívoca, tal como se indica en el Informe jurídico de la AEPD 93/2008, sobre «Formas de obtener el consentimiento mediante Web. Consentimientos tácitos».

En el caso de los menores, se exigirá como ya se prevé en la Propuesta de Reglamento de 25 de enero de 2012 de protección de datos, que el tratamiento de los datos personales relativo a los niños menores de 13 años sólo será lícito si el consentimiento ha sido dado o autorizado por el padre o tutor del niño. Es por ello que, al responsable del tratamiento será al que incumbirá la carga de la prueba en el supuesto de no ser éste verificable, y de ahí que habrá de hacer los esfuerzos razonables para la obtención de ese consentimiento verificable, teniendo en cuenta la tecnología disponible. No obstante, dichos extremos habrán de ser objeto de una regulación específica por parte de la Comisión de la UE, a fin de que se determinen los métodos de obtención del consentimiento verificable contemplado respecto a los menores de 13 años, pudiendo además disponer la elaboración de formularios normalizados para los métodos específicos de obtención del consentimiento verificable en el supuesto de dichos menores.

Con lo reseñado en relación al consentimiento lícito respecto de los menores de 13 años, y de las medidas que se podrán ir desarrollando, posiblemente se pueda ampliar el nivel de garantía y seguridad exigibles para el otorgamiento y verificación de dicho consentimiento, cuando se dé el mismo en el entorno de las redes sociales.

Una de las cuestiones que se ha venido planteando en el Dictamen 5/2009 del Grupo de Trabajo del Art. 29, es la de la implementación de herramientas que mejoren el consentimiento entre los usuarios miembros de una red social. Se habla así de la «introducción de herramientas de gestión de etiquetas de la información en los sitios de redes sociales en particular, creando espacios en un perfil personal para indicar la presencia de un nombre de usuario en imágenes o vídeos con etiquetas que estén a la espera del consentimiento del usuario en cuestión, o fijando plazos de expiración para las etiquetas que no hayan recibido el consentimiento de la persona señalada». Como veremos ya hay algunas redes sociales en las que se han introducido ciertos mecanismos entre sus «condiciones de uso».

1. Peligros que entrañan las redes sociales *on line*

Es un hecho incontrovertido que la participación en las redes sociales *on line* implica una serie de riesgos y peligros para los usuarios, que son aún mayores si se trata de menores de edad, tanto en el momento de registrarse en la Red, como mientras se interactúa y forma parte de la misma, así como en el momento en que se decide darse de baja.

Aunque pudiera parecer que los protagonistas de las redes sociales son los usuarios, sin embargo lo cierto es que lo son los prestadores de servicios. Si nos centramos en su funcionamiento, vemos como al darse de alta el usuario proporciona una gran cantidad de datos personales, muchos de los cuales pueden calificarse de sensibles, no proporcionándolos el usuario voluntariamente, aunque puede dar esta impresión, sino compelido por el sistema, con el fin de poder acceder a determinados servicios o aplicaciones, produciéndose lo que por ejemplo GONZALEZ FUSTER califica «como divulgación no espontánea de datos»[25].

Esta captación de datos tiene transcendencia respecto de la privacidad, ya que las plataformas disponen de potentes herramientas de

[25] GONZÁLEZ FUSTER, G.; «*Privacy 2.0?*«» *Rue du droit des Tecnologies de línformation*», nº 32, Septiembre 2008. Págs. *vid.* Pág. 352.

procesamiento y análisis de los datos facilitados por los usuarios. Además, a ello se añade la circunstancia de que en múltiples redes, los perfiles de los usuarios aparecen indexados en determinados buscadores de Internet, así como que se detecta, en términos generales, una ausencia de mecanismos que permitan controlar la edad de las personas que se conecta a las redes y evitar que accedan los menores de 14 años, sin el preceptivo consentimiento o autorización de los padres o tutores, tal como determina el Art. 13.1 y 13.4 del RLOPD. Los citados aspectos serán reforzados, una vez que resulte de aplicación el futuro Reglamento sobre protección de datos, en los términos señalados anteriormente en relación con la licitud del consentimiento y la verificación.

Y aunque puede haber redes sociales como el caso de *Tuenti* que, se implicó en una política de protección de datos que, tiene como objetivo impedir que los menores de 14 años puedan ser usuarios de la red social, lo cierto es que la experiencia de cada uno de nosotros, nos dice que eso en la realidad no se produce de forma generalizada. No es menos cierto que puede existir el mecanismo correspondiente de verificación de la edad, y de la posibilidad ante una duda de solicitar el DNI al usuario para la comprobación de la edad, pero este proceso resulta harto complicado[26] habida cuenta el volumen de usuarios. Y por ejemplo, *Facebook* también se implicó elevando la edad para ser usuario de esta red de los 13 años a los 14 años, con objeto de mejorar la privacidad y el control de la información por parte de los usuarios, según nota informativa de la AEPD de 20 de julio de 2009.

Pero a pesar de todos estos intentos en aras a una mayor protección de la privacidad de los menores, lo cierto es que la política de privacidad de estas redes es poco clara, y no se detalla con suficiente especificidad el uso que se puede hacer de datos personales, ni por supuesto de las imágenes, con las consecuencias de conductas lesivas a la privacidad que se pueden producir, una vez introducidos esos datos en la red «sin control».

2. Algunos ejemplos de conductas lesivas

A) Situación de partida

La sociedad de hoy en día, Sociedad de la Información ya no se

[26] MARTOS DÍAZ, N.; «Redes sociales y privacidad». Madrid. Opinión de expertos Revista digital Datos personales. Org. Madrid. AEPD, de 31 de enero de 2010, nº 43.

entiende sin la existencia y utilización de las nuevas tecnologías, éstas han aportado mejoras significativas y sustanciales que han modificado el estilo de nuestra vida y de la forma de relación entre las personas, permitiéndonos llevar a cabo actividades inimaginables hasta hace unos cuantos años, que presentan un futuro de progreso, y sin embargo no impiden la existencia de situaciones de riesgo a las que nos vemos abocados. Los retos a los que se enfrenta el mundo a comienzos del siglo XXI requieren del desarrollo y uso generalizado de las Tecnologías de la Información y Comunicación (TIC), como instrumento imprescindible para generar riqueza y mejorar las condiciones de vida de las personas, al ser los avances introducidos por la electrónica elementos que, sin duda, contribuyen a mejorar el nivel de vida y bienestar de la sociedad actual. En este sentido la Asociación Española de Empresas de Electrónica, Tecnología de la Información y Telecomunicaciones (AETIC)[27], en su informe sobre recomendaciones de gobierno para la legislatura del 2008 al 2012 presentó ya una serie de medidas a cumplir, de entre las que merece la pena reseñar las siguientes:

— La necesidad de promover que los ciudadanos accedan habitualmente a Internet en banda ancha,

— Priorizar la alfabetización digital y la accesibilidad de aquellos grupos de género y edad más desfavorecidos,

— Incrementar la sensibilidad del público hacia los nuevos medios audiovisuales e impulsar proyectos de digitalización, para el incremento del patrimonio cultural,

— Conocer los beneficios de la utilización del software legal e incentivar la puesta en práctica de las adecuadas políticas que permitan asegurar, controlar y auditar con un nivel adecuado la protección de los datos, y en consecuencia de la privacidad.

A pesar de que según los datos disponibles, el fenómeno de Internet se ha convertido en un supuesto de utilización masiva que ocupa el 50 por ciento de la población española, sin embargo todavía es necesaria una labor de difusión de la cultura de la protección de la seguridad de la información y la sensibilización entre los usuarios de una correcta utilización de Internet y, de las redes sociales. Si acudimos a las estadísticas, se constata la tendencia al crecimiento. Tan

[27] AETIC «La electrónica, la tecnología de la información y las telecomunicaciones» Propuestas de AETIC para la Legislatura 2008-2012.Asociación de Empresas de electrónica, Tecnologías de la Información y Telecomunicaciones de España Diciembre 2007.

sólo en 6 trimestres durante el año 2005-2006, la evolución de la utilización del ciudadano en el uso de Internet se incrementó desde los 16.426 millones de personas en el 2005 hasta los 20.097 millones en el 2006. Del estudio realizado por INTECO se constata como las actividades mayoritariamente realizadas por la población no solo se centran entorno a los usos sociales de utilización de Internet, sino en otra clase como chats, correo electrónico, blog, la banca electrónica, el comercio electrónico o los juegos. El envío de archivos P2P, punto a punto o de un ordenador a otro, se ha convertido en regla general, tanto es así que 6 de cada 10 usuarios lo utilizan habitualmente para el envío de todo tipo de información, incluyendo los archivos de fotografías y videos, y otros más. Sin embargo no se nos escapa que dicho tratamiento masivo, también es utilizado de forma malintencionada, pudiendo quedar vulnerados los derechos fundamentales de la personalidad, sin perjuicio de que un gran número de estas actuaciones estén en muchos supuestos vinculadas con otras delictivas, por lo que es necesario estar especialmente atentos a las mismas, y aún con más intensidad con respecto a los adolescentes y jóvenes, estableciendo en la medida en la que se nos permita, mecanismos y herramientas que determinen la fijación de medidas necesarias para una protección básica frente a este tipo de problemas.

Conviene añadir que el concepto de red social en Internet supone una nueva forma de relación humana que se ha ido posicionando como uno de los medios de comunicación *on line* más populares de la Red, llegando a superar en muchos casos los 132 millones de usuarios recurrentes[28], que las utilizan como principal medio de comunicación. Este método es uno de los más utilizados en Internet y prueba de ello es que entre las palabras más buscadas en Internet está precisamente, la denominación de algunas de las redes sociales existentes, como por ejemplo *Facebook, Badoo* logrando un número de visitantes durante 2007 que superaron los 500 millones anuales[29]. Especial trascendencia tiene el hecho de que los menores de edad sean según recientes estudios los principales usuarios de este tipo de plataformas. Existe por ello la necesidad de una estrecha supervisión para una mayor seguridad de las personas, haciéndose imprescindible una evolución de la legislación vigente, que contribuya a aumentar el grado de protección con el objetivo de intentar reducir los efectos negativos derivados del uso de estas.

[28] COMSCORE WORD METRIX, Agosto de 2008.

[29] COMSCORE, Inc. «Facebook,Hi5 more than doublé visión global Visitor bases during past year«2008.http:wwwcomscore.com/press/release.asp?.

La red social permite a su usuario crear un perfil público, compartir información, colaborar con la generación de contenidos y participar de forma fácil en movimientos sociales y corrientes de opinión. Permite gracias a la facilidad y rapidez de interconexión, aumentar las relaciones sociales entre los usuarios, lo cual genera un aspecto sociológico interesante que atrae, engancha y que cada vez más, incide en el ámbito de esas relaciones humanas, ya que las personas se hacen más individualistas y solitarias, al tiempo que cada vez esas relaciones «*on line*» se multiplican.

Ahora bien, existen paralelamente determinadas actuaciones sospechosas o al menos actos que se están llevando a cabo sin cumplir los principios básicos de la normativa de protección de datos de carácter personal, la protección de la intimidad, la publicidad y la protección intelectual e industrial respecto de los contenidos creados y alojados por los propios usuarios en sus perfiles. Aunque, como se ha señalado, hay muy distintos tipos de redes sociales, una diferenciación a tener en cuenta entre las mismas, se refiere al ámbito de actividad, por cuanto se pueden clasificar entre aquellas profesionales y, aquellas otras más generalistas o dedicadas al ocio. Este tipo de plataformas en los últimos años han llegado a experimentar crecimientos muy importantes, tanto a nivel social como tecnológico llegando a constituirse en plataformas multitudinarias internacionales, como es el caso de *Facebook* que pueden llegar a alcanzar los 100 millones de usuarios. Se ofrecen plataformas que integran multitud de herramientas en una misma pantalla pudiendo prescindir de otras aplicaciones de comunicación externa. Además resulta relevante señalar que dicha plataforma sirve para convocar y organizar otros aspectos de la vida *offline*. También se pone a disposición del usuario, parte del código abierto mediante el cual la plataforma se ha programado, para que los usuarios puedan desarrollar aplicaciones propias y personalizar la interfaz de usuario.

El principal problema que se genera es que los propios usuarios no sólo exponen sus datos, sino que además hacen públicas sus vivencias, por lo que el ámbito de la privacidad se abre de forma exponencial, con la consecuencia lógica del aumento del riesgo de atentados contra los derechos de la personalidad, entre otras cosas incrementándose incluso los ilícitos penales.

En efecto, si entramos en cualquier perfil de una red social, fundamentalmente las de ocio, los usuarios exponen en muchas ocasiones, no sólo datos personales, sino incluso datos como los de la orientación sexual, o religiosa o ideología política que pueden ser utilizados por ter-

ceros de forma maliciosa, siendo un ejemplo muy habitual el volcado en la red de informaciones falsas que se difunden, elementos audiovisuales privados, fotos o videos principalmente, sin ningún tipo de autorización y en ocasiones, con la única intención de perjudicar, siendo atentatorios contra los derechos de la personalidad, ya se trate del honor, la intimidad o nuestra imagen o los propios datos personales.

Si ahondamos en los supuestos de intromisiones ilegítimas en el ámbito de la privacidad, constatamos como los casos más habituales de conductas intrusivas que se producen en las redes sociales se manifiestan en alguno de los aspectos a los que nos referimos a continuación:

B) Suplantación de identidad

Al darse de alta en una red social podemos descubrir que otro usuario ha asumido nuestra identidad, y este comportamiento es más habitual sobre todo en las redes que buscan relaciones negóciales o profesionales. Ello sin olvidar que uno de los fenómenos más problemáticos que hoy día existen es el del acoso a menores, en los que se suele suplantar la identidad de otro menor por parte del acosador, para ganar la confianza de la víctima, y posteriormente fundamentalmente a través de la utilización de imágenes de contenido pornográfico, obtener satisfacción sexual. Es el denominado *Grooming*, conducta ésta penalmente castigada.

En este ámbito, es de interés destacar que precisamente la AEPD ya ha sancionado, a un usuario de Internet que se hacía pasar por otro en redes sociales, imponiéndole una sanción por la citada suplantación de identidad. Es verdad que ya existían resoluciones anteriores de órganos judiciales que, de una u otra forma, condenaban este tipo de conductas, pero fundamentalmente en el ámbito penal, orden que había dado acomodo a la suplantación de identidad como la suplantación de estado civil del artículo 401 o el delito de vejaciones del artículo 620.2 ambos del Código Penal.

La disparidad en el tratamiento efectuado por el Derecho, lejos de dar seguridad jurídica, otorga una inseguridad precisamente por esa ausencia de regulación específica en cuanto a la conducta atípica de la suplantación de identidad. Y es que no existe como tal un tipo penal o una infracción civil que permita su sencillo encaje en el ordenamiento jurídico vigente. Así las cosas, aunque este tipo de acciones podrían tener un mejor encaje dentro de las figuras penales, su ubicación con-

creta en la normativa sobre protección de datos, resulta complicada, por cuanto si bien se sanciona a un usuario que suplanta la identidad de otro, el ordenamiento jurídico no le sanciona por tal hecho, sino por el tratamiento in consentido de datos de carácter personal de la persona suplantada, de conformidad con lo dispuesto en el artículo 6 de la Ley Orgánica de Protección de Datos de carácter personal. Precisamente, posteriormente al criterio mantenido por la AEPD respecto a la suplantación de identidad, en el sentido de considerarse una conducta ilegítima objeto de sanción, se plantea si dicho encaje jurídico es el adecuado para enjuiciar estos hechos de suplantación de identidad, o si por el contrario se debería sancionar de acuerdo con el ordenamiento penal, para que la AEPD, en caso de tener conocimiento de unos hechos presuntamente delictivos, deba ponerlo en conocimiento de la Fiscalía o de los Juzgados para que sean éstos los que enjuicien una causa cuya competencia parece más natural.

Y esto es lo que acontece en el ámbito de nuestro ordenamiento jurídico que, hoy por hoy, no se adapta a los distintos supuestos que son una realidad en Internet, y que exigen acudir a figuras forzadas para castigar conductas claramente contrarias a la buena fe y la legalidad.

C) Difusión no consentida de fotografías

Se trata de un supuesto habitual en el que, por inexperiencia y falta de conocimiento de los usuarios, incluyen en su espacio fotografías de amigos o conocidos, y las etiquetan, sin su consentimiento.

Las consecuencias de esta publicación pueden ser del más variado signo, aunque las más difundidas son las que se refieren, en el caso de menores de edad, a supuestos de acoso escolar; no se deben obviar igualmente, otros casos de acceso por las empresas a fotografías, que pueden generar consecuencias muy distintas, no sólo desde el ámbito de la vulneración del derecho a la propia imagen, sino también en el ámbito penal, del derecho al honor, a la intimidad personal o familiar o a la protección de datos. Y es que no podemos ser ajenos a la existencia de fotografías que se publican con la clara intención de hacer daño, y ese daño se multiplica exponencialmente si se trata en la Red.

En efecto, si nos referimos al ámbito de los menores no nos resulta extraño que en ambientes escolares este tipo de supuestos de etiquetado de fotografías o su manipulación suele ser utilizado para ri-

diculizar a compañeros o profesores Pero además, son cada vez más habituales los supuestos de *ciberbullying* o acoso escolar por vía telemática, y en muchos de los casos se utilizan fotografías o el denominado *happy slapping*, conducta consistente en la grabación de imágenes o videos a través de los móviles para posteriormente incluirlas en plataformas de contenidos como *Youtube, Myspace*, y cuyo fin no es otro que ridiculizar o vejar a la víctima, cuando ésta se sitúa en determinadas actitudes, al verse sorprendida o agredida por un conjunto de estudiantes, ya sean o no menores, y ser grabadas estas imágenes.

También suele ser habitual la utilización de imágenes en la red con fines de pretendido periodismo ciudadano, pero sin respetar los límites que el ejercicio del derecho a la información impone en muchos casos.

Difusión de imágenes en Youtube ya sea con fines vejatorios, o con fines informativos

Como nos recuerda MARTÍNEZ MARTÍNEZ[30] en el ámbito de los servicios de la «Web 2.0 se pueden identificar distintos tipos de conductas relevantes desde el punto de vista de la protección de datos personales…, el supuesto de hecho principal va a consistir en algún tipo de publicación de datos personales –datos de identificación alfanuméricos, imágenes o audio videos– o de documentos o archivos que los contengan. A su vez desde la perspectiva de su repercusión en los derechos de los afectados», y han de considerarse además los distintos escenarios alternativos en función de la configuración del espacio en Internet, esto es si el espacio únicamente facilita acceso a usuarios autorizados o, si por el contrario, el espacio se encuentra abierto a todo el público.

Todo este conjunto de problemas que se plantean en relación con los posibles derechos fundamentales de la personalidad de los usuarios afectados o no, y en particular con el de la protección de datos de imágenes viene siendo objeto de preocupación por el Grupo de Trabajo del artículo 29 de la Directiva 95/46/ CE, que con posterioridad a la Sentencia del Tribunal de Justicia de 6 de noviembre de 2003 en el asunto Bodil Lindqvist[31] que constituye una referencia de primer orden cuando se trata de establecer con claridad criterios a aplicar so-

[30] MARTÍNEZ MARTÍNEZ, R.; Capítulo IV en la obra coordinada por. RALLO LOMBARTE, A. y MARTÍNEZ MARTÍNEZ, R.; *Derecho y redes sociales*. Reus 2010. Pág. 97.

[31] Sentencia del Tribunal de Justicia de 6 de noviembre de 2003 en el asunto C-101/01.Petición de decisión prejudicial planteada por el Gota Hovrätt. http://curia.europa.eu/.

bre la protección de datos personales en Internet, y por tanto de aplicación también a las fotografía e imágenes.

En efecto, se centra en considerar que el colgar una foto, o un video o un texto escrito en una red social no difiere en términos materiales de lo acaecido en el caso Bodil Lindqvist, pues se entiende que los extremos distintos de los diferentes supuestos de hecho que se pueden producir, son como consecuencia del avance de la tecnología, pero que concierne a tratamientos de datos inconsentidos, si bien a través de un entorno cooperativo, como es una red social.

Como se recordará la Sra. Lindqvist era una catequista sueca que, a finales de 1998, creó con su ordenador personal varias páginas web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieren obtener fácilmente la información que pudiera resultarles útil. Dichas páginas contenían información sobre la Sra. Lindqvist y dieciocho de sus compañeros de parroquia, incluido su nombre de pila, acompañado en ocasiones, del nombre completo. Además la Sra. Lindqvist describía en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros, así como sus aficiones. En varios casos se mencionaba la situación familiar, el número de teléfono e información adicional. Así mismo, señaló que una de sus compañeras se había lesionado un pie y que se encontraba en situación de baja parcial por enfermedad. Tras ser sancionada y recurrir, el Tribunal sueco consulto al Tribunal de Justicia[32] sobre las condiciones de aplicación de la Directiva 95/46/CE, y una vez analizadas todas las cuestiones que el Hovrätt formula en un total de siete, y pronunciándose dicho Tribunal sobre las mismas, se concluye en la Resolución dictada de 6 de noviembre de 2003 tanto que la conducta efectuada por la Sra. Lindqvist de incluir en una página web datos relativos a diversas personas e identificarlas por su nombre y otros medios, así como que dicho tratamiento lo es de datos personales, y es más relativos algunos de ellos a la salud, sin que las disposiciones de la Directiva se entienda que suponen una restricción contraria al principio de la libertad de expresión o a otros derechos y libertades vigentes en la UE, así como que la citada Directiva que resulta de aplicación a determinados supuestos, pueda ser ampliada su aplicación por los estados miembros en su propia normativa nacional tendente a adaptar el Derecho interno a la citada Directiva 95/46/CEE, tal

[32] Véase nota de prensa publicada al efecto por el propio Tribunal en la pagina http://curia.europa.eu//es/actu/communiques/cp03/aff/cp0396es.htm.

como se hace constar en el análisis efectuado por REBOLLO DELGADO[33].

Por tanto se estarían produciendo intromisiones ilegítimas en el derecho fundamental a la protección de datos, sin perjuicio de que también quedara afectado el derecho a la propia imagen, u otros derechos fundamentales, en función de las circunstancias en concreto que en cada caso se den.

De ahí que el citado Grupo de Trabajo del Artículo 29 se haya pronunciado sobre estos particulares en el Dictamen 5/2009 en relación con las redes sociales en línea y el etiquetado de fotografías, anteriormente citado.

En nuestro Estado, la AEPD también se ha centrado en el estudio de esta problemática, tal como nos señala MARTÍNEZ MARTÍNEZ[34] haciendo la citada Agencia una serie de recomendaciones especificas, entre las que merece la pena recordar la relativa a la necesidad de tener especial cuidado al publicar contenidos audiovisuales y gráficos en los perfiles, especialmente si se van a alojar imágenes de terceras personas; no etiquetar contenidos audiovisuales con la identidad real de sus protagonistas, ni ofrecer datos de terceros en su espacio sin el propio consentimiento; el respeto más escrupuloso de los derechos de terceros, incluso en el supuesto en que se publique una fotografía o se escriba en un blog, si se puede estar incluyendo algún tipo de información, aunque sea tangencial sobre otras personas.

Con respecto a los menores, ya se han efectuado iniciativas tendentes, entre otras medidas a la elaboración por la AEPD de documentos y otros recursos que se ponen a disposición de los padres o tutores y menores, con objeto de concienciar e informar sobre la privacidad en riesgo, que en la Memoria de 2008 se situaba precisamente en el ámbito de las redes sociales, considerando como un hecho el que «nuestros hijos nacen a la sociedad como niños digitales. La telefonía Móvil, la televisión digital, las PDA, los juegos digitales, o Internet son su medio natural y social pero no aprenden a protegerse», de ahí la importancia de la educación y de la concienciación.

Por último mencionar la existencia de tratamientos de informa-

[33] REBOLLO DELGADO, L.; «Comentario jurídico a la Sentencia del Tribunal de Justicia de la Unión Europea de 6 de noviembre de 2003». Revista de datos personales, número 9 de mayo de 2004.

[34] MARTÍNEZ MARTÍNEZ, R.; Capítulo IV «Protección de datos personales y Redes sociales, un cambio de paradigma» de la obra coordinada por RALLO LOMBARTE, A. y MARTÍNEZ; *Derecho..... Opera cit.* Pág. 101.

ción personal vinculados a espacios de ejercicio del derecho a la información en la denominada blogosfera, o en foros y lugares de debate público.

IV. UNA APROXIMACIÓN AL CIBERACOSO: *CIBERBULLYING, GROOMING* Y OTROS PELIGROS EN EL ÁMBITO DE INTERNET

1. Ciberbullying

Como consecuencia del fenómeno existente en nuestra realidad, respecto a que tanto Internet como el móvil están de forma *onmi* presentes en la vida de niños y jóvenes, y que el ciberespacio forma parte de su vida y de su proceso de socialización, el ejercicio de la violencia se ha instaurado en la red y ha encontrado en las redes sociales los recursos adecuados para abrir nuevos cauces de agresión.

Una de las manifestaciones de esa violencia es el acoso a través de las denominadas Nuevas Tecnologías, problema que genera una importante alarma social. Y es que hasta el 2,1% del alumnado de secundaria confirma haber sido a menudo victima de grabaciones o fotografías u otras formas de acoso a través de las nuevas tecnologías de la comunicación.

Desde el ámbito terminológico, debemos referirnos al termino en inglés de *Ciberbullying*[35] que se define como «*aquella conducta en que un adolescente o preadolescente, normalmente menor, es atormentado, amenazado, acosado o humillado y avergonzado por otra persona desde Internet utilizando los medios interactivos, tecnologías digitales y teléfonos móviles*»[36]. Se trata de determinado comportamiento que se lleva a cabo con el uso vejatorio de algunas tecnologías de la información y de la comunicación (correo electrónico, SMS, mensajería instantánea, sitios personales, redes sociales) por parte de un individuo o grupo, que deliberadamente y de forma repetitiva y hostil pretende dañar a otro. Se utilizan los medios telemáticos para ejercer el acoso psicológico entre iguales, es decir no entraría en el concepto la relación que se establece entre menores y adultos.

[35] PARDO ALBIACH, J. (Coord. Garcia Gonzalez, J.): Ciberacoso, la tutela penal de la intimidad, la integridad y libertad sexual en Internet. Valencia 2010. Pag.56.

[36] Guia.Juvenil.com(2008) «Qué es el Ciberbullying». El acoso en Internet. http://guiajuvenil.com/instituto/que.

Podríamos mencionar casos en los que un adulto engaña a un menor, haciéndose pasar por otro menor, precisamente siendo las redes sociales la vía más fácil y anónima, y por tanto impune, mediante el chantaje en la utilización de fotografías, en un gran número de supuestos, se trata de utilización de imágenes o conversaciones comprometidas fundamentalmente, aunque el porcentaje de estos casos parece ser bajo (INTECO, marzo 2009)[37].

El problema fundamental que se plantea en dichos supuestos es el desconocimiento del agresor, que magnifica el sentimiento de impotencia de la víctima. Ante esta situación, con independencia de la existencia de una mayor impunidad consecuencia del anonimato, es importante reseñar por ende, la dificultad de la identificación del agresor, y por tanto el desamparo legal que estas formas de acoso conllevan, pues aunque una web en concreto, donde se ha identificado el problema se pueda cerrar por mandato de las autoridades competentes, ello no es óbice para que a continuación se puedan abrir otras, por los mismos usuarios.

Como ejemplos concretos de este tipo de ciber intimidación, que se desarrolla sobre todo a través de Internet, mediante la utilización de imágenes comprometidas, previamente colgadas, o mediante la usurpación de la identidad de la víctima, tal como se ha señalado, en su nombre se efectúan comentarios ofensivos o participaciones inoportunas en chats, blogs, foros, entre otros, de tal forma que despierten reacciones adversas hacía quien de verdad es la víctima.

La inmortalización de determinadas imágenes, mediante la divulgación de las mismas en Internet, es un hecho más que habitual, siendo usual que se cuelguen en los «muros personales» (tal ha venido ocurriendo precisamente a finales del pasado año en *Facebook)*; se convierte así mismo en usual la posibilidad de entrar en el correo electrónico de la víctima accediendo a todos sus mensajes e incluso, evitando que los pueda leer el verdadero destinatario; se permite, igualmente hacer correr falsos rumores sobre un comportamiento reprochable atribuido a la víctima, de tal forma que quienes lo leen reaccionen y tomen represalias en contra de la misma.

Una característica importante que diferencia al ciber acoso, del acoso en la vida real, es que el uso del lenguaje resulta ser mucho más fuerte, más agresivo y por ende, más dañino debido posible-

[37] INTECO: «*La seguridad de la Información y la e-confianza de los hogares españoles*» II Semana Seguridad de Informática-Fundación Dédalo. Mesa Redonda Internet puerta abierta al mundo Tudela 10 de abril de 2008.

mente al anonimato del acosador. Es un tipo de actitud que puede ocasionar graves daños psicológicos, a la persona que sufre esta actividad ilícita. Se ha constatado, como venimos manteniendo, que la mayoría de estos comportamientos con respecto a los menores y adolescentes se producen por un menor contra otro menor, siendo aquellas actitudes más habituales, los mensajes de acoso de mensajería instantánea; robo de contraseñas de cuentas de correo y usuarios de la web; comentarios ofensivos en blogs y sitios web; envío de fotografías e imágenes a través de emails y teléfonos móviles, encuestas en Internet insultando o injuriando; juegos interactivos involucrando al acosado; envío de códigos maliciosos y virus al email de la víctima; envío de material pornográfico y emails basura y suplantaciones de identidad, en que el acosador asume la identidad de la víctima en Internet y comete actos delictivos o que denigran la imagen del acosado.

Con todo esto, se puede uno hacer una idea de lo que supone y de las consecuencias que ello conlleva para muchos menores, y de la importancia de proceder a una regulación contundente respecto de estas conductas, en las que las imágenes y videos, pueden constituir herramientas de gran relevancia. Y este es un problema de difícil resolución, precisamente por la necesidad de que los diversos ordenamientos jurídicos establezcan mecanismos para prevenirlos y evitarlos, requiriéndose una adecuada armonización legal y una mayor cooperación entre autoridades competentes de control.

2. Grooming

Otra de las practicas más habituales últimamente utilizadas en la red es la extorsión y chantaje a menores, curiosamente cometidas en un gran número de casos por menores de edad. Básicamente podemos decir que acaece, cuando se da una situación de extorsión, que se produce *on line* entre un individuo a un niño, para que bajo amenazas o coacciones, éste acceda a sus peticiones de connotación sexual principalmente, y que usualmente tienen lugar mediante la utilización de una *webcam* o, a través del programa de chat del ordenador, llegando incluso a concertar acuerdos para materializar el abuso.

En efecto, se ha constatado, no sin gran preocupación que, los acosadores de menores encuentran en Internet un lugar más accesible para desplegar una serie de actividades de abuso sexual a los mismos, amparados bajo la posibilidad de ocultación de su identidad.

Estos habitualmente mienten y muestran ser más jóvenes de lo que son, o de lo que indican en la web, encontrándose además en un ambiente impune que le facilita la Red, al actuar desde el anonimato.

Todo el proceso se inicia en la Red, cuando un adulto consigue, en base a esa primera confianza existente, que un menor le dé una fotografía o video comprometidos. Y es aquí donde comienza el chantaje, ya que el menor consigue ser convencido para que le remita más fotografías o imágenes comprometidas.

Posteriormente, si el coaccionado no quiere que dichas imágenes se envíen al resto de sus contactos, no existe ya solución, por cuanto lo habitual es que el delincuente ya se haya hecho, de forma engañosa, con las claves del correo de la víctima y, por tanto con la libreta de direcciones y contactos del mismo, pudiéndose proceder a la utilización in consentida y fraudulenta de la misma.

El menor pensando que el chantajista va a quedar satisfecho y, en consecuencia accederá a la no distribución de las fotografías remitidas de carácter comprometido, y con el fin de evitar su difusión, cede a los propósitos del delincuente. Pero posteriormente, lo habitual es que el delincuente no finalice con sus propósitos en este momento, sino que incide una y otra vez en las coacciones, y es entonces cuando se entra en una espiral de la que el menor ya no puede salir indemne y sin ayuda, constituyendose la red en la aliada del controlador.

Es a esta práctica a la que normalmente se la conoce como *Child Grooming,* término que hace referencia a la acción encaminada a establecer una relación y control emocional sobre el niño o niña, cuya finalidad última es la de abusar sexualmente del o de la menor.

El *modus operandi* de los acosadores internautas, no suele variar en exceso de unos supuestos a otros, pues lo usual es el ingreso en salones de chat públicos con nombres de usuario llamativos para los menores, con el fin de elegir a su potencial víctima que tiene un *nick* similar al suyo. Posteriormente, una vez elegida la víctima, se procede a establecer la conversación por chat, pidiendo a esa víctima que le dé su dirección de correo electrónico, para acto seguido comenzar el acosador con sus artimañas para tratar de seducirlo, diciéndole por ejemplo lo especial que es... (O por ejemplo que le permita ver si tiene una boca bonita, un bonito cuerpo, entre otros).

A continuación, prevaliéndose de esa confianza que ha hecho nacer en el menor, le puede hace adoptar frente a la *webcam* poses insinuantes que, va capturando como imágenes en su computador.

Así, si logra hacer que el menor le muestre alguna de sus partes íntimas, el abusador desvela entonces su verdadera identidad y amenaza a este con enviar esas fotos a sus padres o publicarlas, si no accede a lo que le va pidiendo. Ahí empieza el verdadero acoso con extorsión, que en su forma más repugnante puede terminar en encuentro personal y abuso físico.

Otra práctica habitual, que no conviene obviar, cuando nos referimos a la utilización de las propias imágenes o videos en la Red, es aquella que se produce cuando estos acosadores sexuales establecen una relación amistosa con los menores incluso por semanas o meses, haciéndose pasar por alguien de la misma edad y genero.

Al cabo de un tiempo, deciden presentarle otro amigo que podrá estar interesado en establecer una relación amorosa con él. Tras la presentación y luego un par de conversaciones, este nuevo amigo comienza a hacerle peticiones sexuales que hacen sentir incomodo al niño. Este recurre al primer amigo para contarle que la persona que le presentó está teniendo actitudes extrañas, tras lo cual el supuesto amigo pide al niño su cuenta de correo y clave para poder resolver el asunto inmediatamente. Una vez revelada esta información, el abusador deja al descubierto que es la misma persona tras las dos identidades. Y es así, como a continuación, se inicia la extorsión, con la amenaza de utilizar mal su correo electrónico, obligando al niño a posar frente a cámaras e incluso reunirse en persona.

Con dichos supuestos más que habituales de *cibergroomming,* se puede ofrecer una visión aunque limitada de lo relevante que resulta la buena utilización de las fotografías o imágenes, y la necesidad de su protección, no sólo en cuanto que pueden vulnerar el derecho a la propia imagen, sino desde la perspectiva de su condición de dato de carácter personal, puesto que éstas trascienden de estas esferas, haciéndose necesario en relación con las imágenes, videos y fotografías, la autorización de los padres y la supervisión que estos efectúen de esta actividad, así como una regulación legal, que genere una propia autorregulación de los propios prestadores de los servicios de las distintas redes sociales.

La privacidad y el derecho a la propia imagen y su dimensión de dato personal, se convierten en un problema a resolver, debiéndose resguardar tanto con prácticas sencillas derivadas del ordenamiento jurídico, como a través de otras que se pueden generar, así como con la instalación de barreras técnicas de protección. Todo lo anterior sin olvidar la posibilidad de las denuncias que siempre caben en este tipo de cuestiones.

V. LA PROTECCIÓN FRENTE A LAS CONDUCTAS DEL CIBERACOSO

El principal problema para la profusión de conductas de Ciberacoso, está constituido por los cambios acaecidos en el desenvolvimiento de la vida social en este Siglo XXI. En efecto, los usuarios, la gran mayoría menores, como venimos manteniendo, de forma consciente o inconsciente publican su vida al completo en la Red, denotando así un problema de falta de consciencia de que sus datos personales serán accesibles a cualquier persona y el valor que por ende, éstos pueden alcanzar en el mercado de la Red. A ello se añade la posibilidad de que se esté produciendo una transformación de la privacidad en el ámbito del las nuevas generaciones digitales.

Los usuarios de los que la gran mayoría son menores, hacen completamente públicos datos, imágenes, videos, etc., en que constan sus propias características personales que, en muchas ocasiones, no estarían dispuestos a exponer en su vida diaria, como pueden ser todo tipo de fotografías con posturas, gestos del rostro, signos identificativos en el cuerpo, así como otros, que pueden ser utilizados por terceros de forma ilícita con multitud de propósitos inconfesables.

Lo más relevante es que, en las nunca leídas condiciones de registro aceptadas por la gran mayoría de los usuarios menores de las redes sociales, éstos están cediendo derechos plenos e ilimitados sobre todos aquellos contenidos propios que se alojen en la plataforma, de manera que pueden ser explotados económicamente por parte de la red social, sin perjuicio del resto de consecuencias perniciosas indicadas.

Además conviene señalar, que una vez que un perfil se constituye en una red social, éste queda para el futuro, pues no existe hoy por hoy, posibilidad del control de los datos personales una vez introducidos, siendo realmente muy dificultosa la posibilidad de persecución legal, aunque exista la opción de «denunciar».

Sirva de ejemplo la política de privacidad de una de las redes sociales más utilizadas a nivel global, esto es *Facebook*.

En ella en primer lugar se puede apreciar que el domicilio social de la misma está en Lam arca –Chipre– lo cual sugiere una cierta cobertura legal. Pero más adelante se nos avisa que ciertos datos sensibles, podrían ser de alguna forma protegidos. Posteriormente se advierte al usuario de la publicación de fotos y videos, que por otro lado son de obligada aportación para poderse mover dentro de la red so-

cial, con lo cual se podrían llegar a revelar dichos datos sensibles, y por tanto permitir la utilización en la red social con total impunidad, siendo así que la publicación de material audiovisual puede servir incluso para la revelación de datos sensibles, como por ejemplo aquellos relacionados con la salud.

Y sobre este particular, sólo mencionar que como todo sitio en Internet, esta red social hace uso de las llamadas *cookies*. Estos son fragmentos de información que se almacenan en el disco duro del usuario cuando accede a una página web a través de un navegador, es decir supone el almacenamiento de información relativa al usuario para poder ser utilizada en posteriores visitas al mismo sitio web y, así conocer ciertas características y preferencias del mismo.

En la política de privacidad se informa a los menores vale las *cookies,* que la plataforma almacena tras la desconexión son destruidas, sin embargo las almacenadas por terceros, denominados como socios comerciales, no se encuentran bajo ningún control aunque dichos socios, sí estén autorizados para llevar a cabo esta recopilación oculta de información del propio usuario.

Si nos centramos en los datos de tipo personal introducidos en el perfil que, cada usuario introduce al darse de alta en la red social en cuestión, se avisa de que éstos están disponibles para cualquier socio de la red o de redes asociadas, no sabiendo en ningún momento a qué tipo de red o de redes asociadas estamos haciendo visibles datos de carácter personal, y entre ellos las imágenes. Además se advierte que dichos datos podrán ser utilizados con fines promocionales y como material publicitario de la red en cuestión.

En último caso, en cuanto a la seguridad de los datos que se almacenan, no se informa al usuario de si se tiene en cuenta algún tipo de estándar en seguridad de redes o si se atiene a algún tipo de legislación, como la Ley de Protección de datos de Carácter Personal, que pueda dar unas mínimas garantías de seguridad sobre los datos personales introducidos por los usuarios de las mismas.

En definitiva, lo que se extrae de todo ello, es una pérdida de control de los propios datos personales, entre ellas las imágenes una vez estos entran en la Red, lo que no genera más que el caldo de cultivo para el surgimiento de terceros malintencionados en la utilización de los mismos, que pueden derivar en conductas no sólo in consentidas, sino ilícitas.

El uso de las tecnologías de la comunicación y de la información y su evolución en el ciber acoso ofrecen tres nuevas dimensiones que

deben ser analizadas para comprender los posibles daños e identificar medidas que los eviten o los contrarresten, fundamentalmente para tratar de proteger a los menores:

— Los sistemas de utilización de Internet y las redes sociales, permiten que las personas que llevan a cabo los acosos, se benefician de un anonimato prácticamente absoluto proporcionado por las plataformas en línea, que no requieren una identificación sólida, ni tan siquiera un simple registro, ofreciendo a estos individuos una posición «inmune».

— Además se debería poder efectuar la trazabilidad sobre mensajes de los acosadores, determinar el que las plataformas de las distintas redes sociales, deban dar cumplimiento estricto a la Legislación de protección de datos, debiendo mantener un equilibrio con la necesidad de evitar bloqueos de los debates sociales, y de todos los datos que permiten la utilización efectiva de la publicidad, con los ingresos que de ello se genera.

— Las tecnologías de la información permiten a gran escala la comunicación del acoso, y ha de implicar cada día a un mayor número de personas, con el fin de prevenir y evitar estas situaciones de incremento de riesgo para los menores. A este respecto, los proveedores de estas plataformas, se encuentran con la posibilidad de limitar técnicamente determinadas capacidades que las mismas ofrecen en la actualidad, como la difusión de fotografías de personas que al ser colgadas y compartidas por los usuarios menores en Red, son de forma instantánea puestas en conocimiento del público en general.

— Otra nota que facilita la existencia de acosadores y la dificultad de la trazabilidad de sus actuaciones, es la memoria de datos que persiste en Internet en lo que se refiere a la información utilizada para el acoso. Actualmente, una vez que la información de un acosado consta en Internet, es muy difícil su supresión o su borrado, siendo la dificultad fundamental, para el reto que supone el ciber acoso en Internet. Por tales motivos, igualmente será necesario un escrupuloso respeto de la legislación sobre protección de datos personales, y la articulación de las herramientas técnicas necesarias.

Algunas otras formas en las que se puede usar la información volcadas en las redes sobre la que perdemos el control, es para hacer ataques o «spam» (correo no deseado), o «Malware» (software malicioso dirigido con datos reales para generar confianza en la posible

nueva víctima, es decir para hacer creer a esta que está contactando con el usuario real).

Lo cierto es que cuando por los usuarios se vuelca información sobre terceros, ya sean menores o no, con fotografías etiquetadas con comentarios sobre su apariencia o sobre su comportamiento, sin perjuicio de si es o no ofensiva o difamatoria dicha información, así como si las fotografías se encuentran protegidas por la legislación sobre protección de datos, ya sea europea o española, se exige el consentimiento de la persona antes de la publicación de una información personal o, con carácter previo a proceder a colgar una fotografía o video. Y es la citada Legislación sobre Protección de Datos la que habrá de ser respetada, sin perjuicio de la necesidad de que las redes sociales se involucren en el establecimiento de sistemas de control más potentes y efectivos, máxime en los supuestos de menores de edad.

Sin perjuicio de la necesaria información, educación y transmisión de valores, y conocimientos sobre aspectos técnicos, por parte de los responsables de los menores, ya se trate de los padres o tutores, así como sobre formas de actuar ante determinados tipos de mensajes, conductas de agresión, manipulación de fotografías o videos etc., uno de los aspectos más relevantes que habrán de ser tenidos en cuenta para evitar este tipo de conductas, será la necesaria información y comprensión sobre las condiciones de privacidad que se establecen en las distintas redes sociales, cuando los menores se dan de alta, al tiempo que es necesario que los menores comprendan que han de ser conscientes de los problemas que generan el uso indiscriminado de los datos personales en las redes, y la forma de utilización más segura.

Es decir los términos de la autorregulación de las redes, deberán estar al alcance de la comprensión de los usuarios a los que van destinados, y siendo menores una gran mayoría de estos usuarios, será necesario un análisis pormenorizado, en los distintos supuestos, sobre las condiciones de la autorregulación, que algunas de las principales redes sociales plantean, y en concreto de aquellas medidas que se encuentren, en su caso, previstas para la garantía de la protección de imágenes y fotografías, así como tener en cuenta lo que se vaya estableciendo en los diferentes Códigos de Conducta que se puedan elaborar.

Otra herramienta interesante, sobre todo cuando no sabemos quién estará al otro lado de Internet en contacto con los menores, es el denominado «*firewall*», que es una combinación de un dispositivo

hardware más uno software, que controla todo el trafico de Internet que entra y sale del ordenador.

Dicho dispositivo actúa como un agente que examina las credenciales de cada usuario antes de otorgarle acceso a la red o a nuestro propio ordenador. El «*firewall*» identifica nombres, direcciones IP, aplicaciones y otras características del trafico de red que entra y sale de la máquina, además evita las comunicaciones no autorizadas tanto al interior como hacia el exterior de la red en la que nos encontremos –como bien podría ser la red que por ejemplo haría referencia al conjunto de ordenadores que existen en un lugar concreto–.

Dicho software que, determinados prestadores de servicios ofrecen actualmente, otorga protección contra intrusiones que provienen del exterior, haciendo el equipo prácticamente invisible. Por otra parte, permite monitorizar y dejar constancia de datos referentes a todos aquellos usuarios de la red que de forma no autorizada están intentando acceder a ficheros, contraseñas y en general documentos privados que se encuentran en nuestros equipos, sin que el coste de la adquisición de este tipo de programas resulte excesivo, siendo así que es capaz de efectuar el análisis del estado del ordenador de forma diaria.

Por último, conviene recordar la importancia que tiene el que los proveedores de servicios de las distintas redes sociales estén atentos y sean diligentes en el cumplimiento de las Leyes sobre Protección de Datos Personales, no solamente respecto de los usuarios en general, pero de forma más estricta relación con los menores.

VI. A MODO DE CONCLUSIÓN

El cambio que supuso la Web 2.0 ha conllevado una serie de circunstancias y hechos nunca antes previsibles, que no sólo han generado ventajas indudables en el ámbito de las relaciones humanas, suprimiendo fronteras espaciales y temporales, sino también la existencia de peligros y amenazas para la privacidad del individuo, cuyo impacto de futuro todavía no se ha podido evaluar. Este entorno que para los adultos resulta preocupante, sin embargo entre los *nativos digitales* no preocupa sobremanera, pues han nacido con los medios y herramientas telemáticas necesarias para haberlos incorporado, como algo más, a su propio hábitat. Este fenómeno de transformación sociológico, y de cambio en el propio concepto de la privacidad, adquiere dimensiones muy distintas cuando nos referi-

mos a los menores, que no sólo no consideran los riesgos existentes cuando se facilitan todo tipo de datos personales, incluidas imágenes, fotografías y videos en la Red, sino que incorporan ese *modus operandi* consciente, o inconscientemente a su propio pensamiento y forma de relacionarse. A ello, debe unirse todo el conjunto de elementos de carácter técnico que confluyen en la Red, cuya influencia futura es a día de hoy impredecible, aunque sin duda producirá efectos respecto del tratamiento de la información personal, entre la que ocupa un lugar relevante las imágenes.

Ahora bien, como hemos venido manteniendo a lo largo del estudio, el avance de Internet es imparable tanto en la calidad técnica, como en la evolución de servicios y prestaciones para los usuarios, y si nos encontramos en la denominada blogosfera, donde se favorecen la generación de nuevas comunidades, y grupos nuevos ya sean de ocio, profesionales, de información, así como otros, se irán constituyendo nuevas plataformas de servicios en las que se enmarcan las denominadas redes sociales orientadas al ocio, o a incrementar aspectos directamente relacionadas con la vida personal o privada, como es el hecho de compartir fotografías[38] o imágenes, videos, cintas de voz, o escuchar música, o expresar opiniones sobre los temas más variados. Nacen todo tipo de redes sociales, entre las más conocidas *Facebook, Badoo, Twitter, Tuenti, Meetic*, y otras muchas.

En consecuencia, Internet se presenta como un espacio de libertad sin fronteras, espaciales o temporales, con apariencia de gratuidad, donde la personalidad pasa a ser una personalidad social, pero donde además de generarse ventajas, se incrementan exponencialmente los riesgos del nacimiento de conductas lesivas, no sólo respecto de la conculcación de los diversos derechos fundamentales a la intimidad, el honor, la propia imagen o la protección de datos personales, sino también respecto de conductas ilícitas como el *Ciberbullying, el Groomming, el Slapping,* y otras que suponen no únicamente intromisiones en la propia esencia de la persona y en su dignidad, sino que incluso pueden llegar a entrañar atentados a la propia integridad física o moral. De hecho, las suplantaciones de identidad, la difusión no consentida de fotografías con todo tipo de variantes, difusión de imágenes en *You Tube*, ya sea con fines vejatorios o con fines informativos, se multiplican y sus efectos a través de la red cobran dimensiones desconocidas, cuyo alcance futuro desconocemos.

[38] Vease http://picasaweb.google.es/y http://wwe.flickr.com/.

Pero el ordenamiento jurídico no tiene establecidos mecanismos jurídicos suficientes y efectivos para poder solventar todos los riesgos que, la introducción de datos personales en la Red conllevan para la privacidad por cuanto que, desde el punto de vista tecnológico los sistemas actuales no permiten un control efectivo y verificación de los datos, como tampoco de aspectos tan relevantes como resulta ser el consentimiento, cuestión ésta que se hace especialmente delicada y difícil tratándose de menores de edad. Pero es que entendemos que, a pesar de las dificultades existentes, por parte de los prestadores de servicios de las distintas redes sociales que operan en Internet, se han de poner todos los medios disponibles para el establecimiento y efectivo control de sistemas de garantía y protección, sobre todo cuando se trata de menores, a pesar de los avances efectuados.

No obstante, de lo expuesto en este trabajo podemos colegir algunas consideraciones finales:

Primera.– Se requiere no sólo una normativa nacional e internacional, que sea capaz de adaptarse a la situación real que genera el fenómeno de las redes sociales sobre los datos personales en todos sus aspectos relevantes, sino contar con la colaboración de los propios proveedores de servicios, que deberán contribuir a la seguridad de la privacidad, a través de sistemas de autorregulación, fijando herramientas y protocolos más potentes para el control y bloqueo, en su caso, cuando se trate de menores, debiendo de existir una verificación real y efectiva sobre los consentimientos exigidos, no sólo para el alta, sino también para su posterior operatividad en la red y volcado y tratamiento de datos personales.

Segunda.– Respecto de las imágenes, fotografías y videos colgados en las web de las redes sociales, se deberán implementar herramientas que mejoren la gestión de las etiquetas de la información, anteriormente a la posibilidad de su tratamiento, creando espacios en un perfil personal para indicar la presencia de un nombre de usuario en imágenes o videos, con etiquetas que queden a la espera del consentimiento especifico e inequívoco del usuario, máxime en el caso de menores de edad, que deberá otorgarse por sus padres o tutores. El establecimiento de plazos para las etiquetas que no hubieren recibido el consentimiento expreso en cuestión, y su borrado cuando no llegaran a obtenerlo.

Tercera.– Las autoridades de control de los diversos países del entorno de la UE, así como la AEPD en el caso español, deberán propiciar no sólo los correspondientes Códigos de Conducta, sino fomentar la coordinación de las políticas de protección de datos en-

tre ellas, como ya se contiene en la Propuesta de Reglamento de control de datos personales de 25 de enero de 2012, fijando no sólo sanciones efectivas a los prestadores de servicios de Red, que incumplan sus obligaciones de control y vigilancia, máxime en el supuesto de menores de edad, sino incluso incluyendo otras que pudieren llegar a la suspensión temporal o definitiva de los servicios ofrecidos.

Cuarta.– Se deberá fomentar por la AEPD y otras instancias competentes, la realización de iniciativas tendentes, entre otras, a la elaboración de documentos normalizados con un lenguaje asequible, además de herramientas y otros recursos que se pongan a disposición de los de los menores, así como de sus padres o tutores con objeto de concienciar e informar sobre el riesgo que la utilización de las redes sociales conlleva sobre la privacidad, y sobre las dificultades de control de los datos, una vez estos entran en la Red. Usar todos los medios que la tecnología pone a su alcance sí, pero puesto que ésta es su medio natural y social, han de aprenden a protegerse, de la ahí la importancia de la educación y concienciación, sin perjuicio de la tipificación adecuada de las conductas ilícitas, y la debida cooperación para su evitación entre las distintas instancias administrativas y judiciales.

VII. BIBLIOGRAFÍA

ABOSO, G. E. y ZAPATA, M. F.; *Cibercriminalidad y Derecho Penal.* Madrid 2006.

ALCÓN YUSTAS, Mª. F.; *Los menores en el proceso judicial.* Madrid 2011.

BENÍTEZ ORTUZAR, I. F.; «*Informática y delito. Aspectos penales relacionados con las nuevas tecnologías*», en: Reforma del Código Penal. Respuestas para una sociedad del siglo XXI, obra coordinada por L. Morillas. Madrid 2009.

BONILLA SÁNCHEZ, J. J.; *Personas y derechos de la personalidad. Colección jurídica general. Monografías.* Madrid 2010.

CASTELLS MANUEL, M.;

— *La galaxia de Internet*. Barcelona 2001.

— *La Sociedad Red (The Rise of Network Society). La era de la información, Vol. I.* Barcelona 1996.

CASTIÑEÍRA PALOU, M. T.; *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, en:* Lecciones de Derecho penal parte especial, obra dirigida por J.M. Silva. Madrid 2009.

DE LAMA AYMÁ, A.; *La Protección de los derechos de la personalidad del menor de edad.* Valencia 2006.

FERNÁDEZ SANTIADO, A. y CASTRO FUERTES, M.; *Comentarios al artículo 197 del Código Penal, en: Código Penal. Doctrina jurisprudencial.* Madrid 2009.

FERNÁDEZ TERUELO, J. G.; *Cibercrimen. Los delitos cometidos a través de Internet*. Madrid 2007.

GARCÍA GONZÁLEZ, J.; *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet*. Valencia 2010.

GARRIGA DOMÍNGUEZ, A.; *Tratamiento de datos personales y derechos fundamentales.* Madrid 2009.

GONZÁLEZ FUSTER, G.; «*Privacy 2.0?*». Rue du droit des Tecnologies de Information. Núm. 3. Septiembre 2008.

GUERRERO PICÓ, M. C.; *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*. Madrid 2006.

HERNÁNDEZ FERNÁNDEZ, L.; *El honor, la intimidad y la imagen como derechos fundamentales*. Madrid 2009.

MARTÍNEZ MARTÍNEZ, R. y LOMBARTE RALLO, A. (Coord.); *Derecho y redes sociales.* Navarra 2010.

MARTOS DÍAZ, N.; «Redes sociales y privacidad», *Revista digital datos personales Opinión de Expertos*.Org, de 31 de enero de 2010, Núm. 43. AEPD. Madrid 2010.

MONTALVO JAASKELAINEN, F.; *Los menores en el proceso judicial*. Madrid 2011.

PALOMINO MARTÍN, J. M.; *Derecho Penal y nuevas tecnologías.* Madrid 2006.

PIÑAR MAÑAS, J. L.; *Redes sociales y Privacidad del menor.* Madrid 2011.

REBOLLO DELGADO, L.;

— *Derechos fundamentales y protección de datos*. Madrid 2004.

— *El Derecho fundamental a la intimidad.* Madrid 2005.

— *Limites a la libertad de comunicación pública.* Madrid 2008.

— *Temas 16 y 18 «la Videovigilancia y la imagen como dato»*. Master de Protección de datos de UNED. Madrid 2009-2010.

— *Comentario Jurídico a la Sentencia del Tribunal de Justicia de la Unión Europea de 6 de noviembre de 2003. Caso Bodil Lindqvist*. Revista de Protección de datos, nº 9. Mayo 2004.

RODRÍGUEZ LAINZ, J. L.; «Dirección IP, IMSI e intervención judicial en comunicaciones electrónicas», *Diario la Ley de 2 de enero de 2009-(D-382)*.

TRONCOSO REIGADA, A.; *La protección de datos personales*. *En busca del Equilibrio*. Valencia 2010.

URIARTE VALIENTE, L. M.; «Delincuencia organizada a través de Internet», *La Ley Penal nº 46,* Febrero de 2008.

VELA SÁNCHEZ-MERLO, «La privacidad de los datos en las redes sociales», *Revista Española de Protección de datos* núm. 5. Madrid 2008.

VILASEU SOLANA, M. (en la obra coordinada por RALLO LOMBARTE, A. y MARTÍNEZ MARTÍNEZ, R.); *Derecho y Redes Sociales*. Navarra 2010.

VV.AA;

— DICTAMEN 5/2009 aprobado por el Grupo del Artículo 29. http://ec.europa.eu//justice_home/fsj/privacy

— «*Children on virtual World what parents should know*». *INFORME ENISA* Septiembre 2008.

— «*Security Issues and Recommendations for Online Social Networks*» Octubre 2007. www.enisa.europa.eu

— «*Social networking goes global*» COMSCORE WORLD METRIX, *INFORME* Agosto 2008.

— «Captación y difusión no consentidas de la imagen de las personas públicas en momentos de su vida privada. Comentarios a la STEDH de 24 de junio de 2004», *Repertorio Aranzadi del TC,* num.13. Pamplona 2004.

— «Resolución aprobada sobre Protección de la Privacidad en las Redes Sociales» *por la 30ª Conferencia Internacional de Privacidad* celebrada en Estrasburgo en Octubre de 2008. *www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_ en.pdf*.