LAS REDES SOCIALES Y LA PROTECCIÓN DE DATOS HOY

Carlos BARRIUSO RUIZ[*]

SUMARIO: I. *Consideraciones generales.* II. *La autodeterminación informativa como base de las políticas sobre datos personales en las redes sociales.* III. *Perfiles de datos de los usuarios de las redes sociales y debilitamiento de las garantías y principios básicos de la protección de datos.* IV. *Responsabilidad y riesgos de los menores de edad en las redes sociales.* V. *Fuentes consultadas.*

I. Consideraciones generales

El germen teórico-sociológico de las redes sociales fue propuesto inicialmente por Frigyes Karinthy (1929) con la teoría de los "seis grados de separación", que fundamenta el hecho de que cualquier persona puede conectarse e interaccionar con cualquier otra persona del planeta con sólo seis enlaces (conexiones). El concepto reafirmado por Duncan J. Watts (2004), está basado en la idea de que el número de conocidos crece exponencialmente con el número de enlaces en la cadena, y sólo un pequeño número de enlaces son necesarios para que el conjunto de conocidos se convierta en toda la población humana.

Es decir que cualquiera en la Tierra puede estar conectado a cualquier otra persona del Planeta a través de una cadena de conocidos que no tiene más de cinco intermediarios, conectando a ambas personas en tan solo seis clicks.

Por su parte el fundamento del "software social" (SoSo) que potencia estas "redes sociales" converge con herramientas informáticas *on-line* de "comunicación" "comunidad" "cooperación" y últimamente también de "*Web* semántica", que permite formar comunidades colaborativas, interconectadas y afines de ámbito general o específico, con una arquitectura orientada a la *Web* como modelo para el desarrollo de programas y servicios.

Cada una de las distintas redes sociales que conforman la *Web* 2.0 segmenta grupos de población con un interés o afinidad común que los caracteriza. Así se teje y se amplían estas redes con personas que comparten ideas, necesidades, aficiones, intereses, objetivos o gustos afines y específicos. Esta interacción "entre iguales" se nutre por un lado de los datos aportados para registrarse y por otro de los perfiles elaborados por los usuarios con sus datos personales y los de su entorno y por la colaboración (no competencia) con contenidos abiertos, en la creación y puesta en marcha de servicios propios de las redes sociales.

En ellas, cada eslabón debe actualizar sus propios datos, y el sistema genera las citas, invitaciones, alertas sociales, etc. y mantiene la agenda. Se conocen personas de cualquier parte del mundo y te conocen; se colabora y coopera; se crea y se

---

[*] Dr. en Derecho, profesor universitario de informática jurídica y abogado del ICAM (Derecho informático).

comparte contenido, información, experiencias, páginas personales, enlaces de interés; se interacciona con otros usuarios, con grupos de amigos y con familiares sin importar que residan en otros países; se publican contenidos propios y se valoran los de otros, se mezclan; se establece una comunicación desinhibida en ambos sentidos intercambiando fotos, vídeos, música, libros, zonas de marcha, chateo, etc.; se crean relaciones personales, se hacen listas de reproducción; se participa en juegos *on-line*, que en el caso del "*blended networking*" combina lo virtual y lo real.

Pero también se hacen negocios (*networking*), se crean relaciones profesionales; se gestionan organizaciones; se interacciona socialmente en distintos ambientes; se aprende; se intercambian ideas sobre una temática concreta; se fomenta conocimiento colectivo; se participa democráticamente y se crean entornos colaborativos de gestión basados en la *Web* 2.0.

La red social como dinamizador de las comunicaciones en el mundo, potencia las marcas y promociona los productos o servicios asociados.

El usuario de estas redes sociales es a la vez consumidor y productor (Prosumer). Pero debe saber que su identidad digital y sus relaciones sociales en línea repercuten en la vida real, que a su vez retroalimenta su identidad digital. Hay grupos de interés o de poder que atesoran los contenidos de las redes sociales, entre ellos, datos personales, como información muy valiosa. No es altruismo lo que permite que estos servicios funcionen gratuitamente, quitando los beneficios por publicidad; a cambio pueden obtener información de la "inteligencia colectiva" del "neuromundo". Información que siendo monitorizada, controlada, analizada y segmentada puede evaluar ratios de todo tipo. Esta información de los "medios sociales" sometida a algoritmos de análisis, selección y extracción de contenidos, con seguimiento de palabras clave de forma selectiva permite obtener perfiles de alto significado, con las tendencias por edades, profesiones, aficiones, etc. Lo que obliga a mantener un control efectivo sobre el cumplimiento de la normativa de protección de datos en las redes sociales.

En ellas el marketing directo ve la panacea del análisis y control de los mercados. La posibilidad de integración de la marca o producto en la red social afín; la posibilidad de segmentación y microsegmentación en la definición de targets como: localización, sexo, edad, gustos, ideología, eventos, viajes, estudios, familia, coche, nivel de vida, trabajo, preferencias, etc. que formando perfiles, patrones, o tendencias, son potencial e inversamente proporcionales a los niveles de privacidad e intimidad que consideramos normales. Incluso ahora con la incipiente segmentación semántica se agrava. Ello conforma un universo de datos donde cuantos más datos estén disponibles para el análisis y mas poderosas sean las herramientas de análisis, más significativa será la información que se obtenga y más riesgos habrán de vulnerar la intimidad y las prescripciones sobre protección de datos personales.

Es cierto que un análisis inteligente y respetuoso de estos "medios sociales" (redes sociales, *blogs*, *post*, fuentes de noticias, *microblogs*, etc.) permite evaluar el impacto y nivel de aceptación o de critica de campañas o lanzamiento de productos e incentivos. Donde conceptos como la reputación o la popularidad de la marca publicitada son objetivos concretos en la estrategia de comunicación de las redes sociales. Para conocer lo que se dice sobre una organización, marca, o competidor en torno a su prestigio, se emplean diversas herramientas que en esta línea aportan

beneficios empresariales, como, entre otras, el "Social Media Metrics", "Socialmention" o "SiteMeter" o "Twitalyzer".

También el mundo laboral encuentra una valiosa herramienta de análisis en las redes sociales. Es conocido que en éstas se busca información sobre futuros candidatos a puestos de trabajo antes de contratarlos. Así como que posteriormente se monitorean sus actividades a través de las redes sociales y sus redes de contactos. Aunque también cuando se elaboran los perfiles de puestos de trabajo se incluye y se valora la red social de cado uno de los candidatos y el número de contactos que posea. Aunque a veces incida negativamente en la privacidad, la protección de datos e incluso en la propia relación laboral.

El caso de la británica Kimberley Swann fue noticia mundial, por haber sido despedida al haber hecho comentarios en su página de "*Facebook*" de que su trabajo era aburrido.

Hernán Torres, gerente general de Dridco Colombia que es la propietaria de ZonaJobs, sostiene que las posibilidades de información aumentan y permiten consultar sin pagar ni pedir permiso. Aunque no se puede generalizar, se han conocido casos de algunos jefes que usan perfiles camuflados o apodos para acceder a la información que sus empleados vuelcan en las redes sociales, sin que estos se percaten.

Lo que de cara a nuestro propósito actual nos pone en alerta ante la falta de protección de los datos personales, o la protección de la intimidad de los trabajadores que establece el R.D. Ley 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, al indicar que los registros se harán respetando al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible. Salvando el control lícito del empresario que deberá ser puesto en conocimiento del trabajador.

Máxime cuando se contempla ya una evolución marcada hacia las redes sociales semánticas o "redes sociales de conocimiento" como "Gnoss" donde el aprendizaje será mas rápido y la extracción de conocimiento mas eficiente, serán los conceptos los que unirán la red, y donde los requerimientos y necesidades específicas de cada usuario serán resueltas por el propio sistema, en base a perfiles e identidades digitales obtenidos por complicados algoritmos. Es decir, se tratarán todo tipo de datos personales y el sistema tenderá a perpetuarlos y a clasificar a sus integrantes con patrones y procedimientos de inferencia establecidos que harán disminuir el control personal del usuario sobre ellos. Los usuarios, unidos por una relación semántica, representarán las redes específicas de las que no tendrán en ocasiones constancia de su existencia ni que se hayan efectuado con su consentimiento.

Pero antes que esto, hoy nos preocupa que el 77% de los menores españoles que utilizan redes sociales cuelguen un perfil personal accesible a todos los internautas. Teniendo en cuenta que el número de usuarios de redes sociales creció en un 34 por ciento a nivel mundial. Y que el 74% de los usuarios activos de Internet en España, visitó algún medio social. Así como que el 58% de los usuarios de Internet

usa redes sociales. Con la previsión de que antes de que termine la primera década de este siglo, todos los internautas estaremos involucrados en una red social de cualquier tipo. Siendo los usuarios de *Facebook* en Mayo de 2010 mas de 10 millones de usuarios y los usuarios de la misma en idioma castellano más de 62,3 millones.

Por todo ello las redes sociales deben extremar las medidas de protección de la privacidad. Así, en su infraestructura se debería implantar el uso de tecnologías PET con sistemas para favorecer los derechos de protección de datos e intimidad de los usuarios como: La disociación (o anonimato) de forma automática de los datos; el uso de encriptación de los datos; el uso de antivirus y filtros de *spam, cookies, phising*, gestión de identidad; análisis de las políticas de privacidad de los SRS (sitios de redes sociales) mediante la Plataforma de Preferencias de Privacidad, etc. Así como extremar las medidas de seguridad en su sistema informático y ser auditadas y controladas convenientemente, de oficio, para evitar los riesgos actuales, en orden a la efectiva protección de los datos personales que tratan.

También se debería establecer una colaboración con los usuarios en la definición de "políticas" y "gobierno" que evite distorsiones, ya que los usuarios participan en la generación y propagación de sus contenidos y condicionan el uso de sus datos mediante el principio de autodeterminación informativa que, por tanto, en ambos casos, legitima para ello.

Colateral a esto existe, no obstante, indignación en las redes sociales por la ley que permita bloquear y cerrar *webs* que atenten contra la propiedad intelectual, que no debería dejarse fuera de un control judicial estricto.

Es evidente que el titular del dato y la información que ofrecen las redes es del usuario, y aunque se discuta si los propietarios de las redes sociales son responsables o corresponsables del contenido que suben sus usuarios, el poder de disposición debe pertenecer al usuario en cualquier caso.

Normativamente se debería obligar a las redes sociales a establecer una configuración de privacidad que salvo modificación por el usuario restrinja el acceso al perfil de los usuarios y que no permita su recuperación fuera del entorno de la propia red para la cual fueron entregados. Aunque las propias redes se hacen eco del clamor pidiendo a sus usuarios que procedan a revisar y actualizar la configuración de su privacidad, es claro que por defecto la política de privacidad de estas redes sociales debería ser muy restrictiva con las cesiones y usos no permitidos fuera del alcance propio de la red e informar debidamente a los usuarios.

En este sentido, el Dictamen de marzo del 2010, del Supervisor Europeo de Protección de Datos, recomendó a la Comisión Europea a adoptar urgentemente un proyecto legislativo que regule las redes sociales. Por su parte el Grupo de Trabajo del Artículo 29 en su sesion del 12-05-2010 que reunio a las 27 autoridades europeas de protección de datos califico de "inaceptable" la configuración de privacidad adoptada por *Facebook* y exigió la autorización del usuario.

Algunos países como Alemania y Suiza, se anticipan y reclaman a las redes más control. Es el caso del gobierno de Angela Merkel que aprobó en consejo del 25-8-2010 la primera ley de protección de datos para impedir que se usen los datos

guardados en las redes sociales por los patronos empleadores, prevaleciendo el interés del usuario que debe ser protegido. Aunque será extremadamente difícil su descubrimiento y aolicacion efectiva la restricción es buena y no afectara a las redes profesionales como LinkedIn, donde se da el perfil laboral conscientemente.

En España aparte de las iniciativas de la AEPD encaminadas a que se respete la protección de datos en las redes sociales, es de señalar la Memoria 2010 de la Fiscalía General del Estado (Fiscal de Sala Delegado en materia de Delitos Informáticos) que llama la atención sobre los delitos contra la intimidad , contra la libertad y la usurpación de identidad. Indicando la gravedad de los " ataques a la integridad moral cometidos mediante la grabación de imágenes ofensivas (caídas, golpes, palizas) a menores o personas con discapacidad, para posteriormente difundirlas por Internet a través de portales especializados de amplia difusión (*Youtube, MySpace, Orkut, Facebook* y similares). Dichos comportamientos son muy frecuentes en la jurisdicción de menores, pudiendo ser calificados de delitos contra la integridad moral del artículo 173.1 CP en concurso con los correspondientes actos delictivos cometidos (lesiones, injurias...)." Donde también cobran importancia preocupante los fenómenos de coacciones y amenazas, asociados a la revelación de secretos personales, afectando a diversos bienes jurídicos personales (intimidad, libertad, honor, integridad moral).

La falta de esta regulación, no obstante, no debe provocar el abandono de estas redes. Creemos que el no aparecer o no tener contactos o seguidores en estas redes sociales, así como autoexcluirse de cualquier actividad o servicio *on-line* por miedo a perder la protección de nuestros datos y de nuestra privacidad, o padecer los restantes riesgos inherentes a ellas, es traumático para nuestra vida en el mundo real y virtual, ya que produce efectos negativos en muchos aspectos socio-laborales, culturales y profesionales. Ausentarse de la red, impedirá estar en la sociedad del conocimiento, impedirá el avance en nuevas tecnologías y la interacción beneficiosa que es la que tenemos que defender.

Así el desarrollo de las políticas y prácticas para la integración de las TICs, los servicios, usuarios, organizaciones, administraciones y sociedad en general, es decir la evolución de la sociedad de la información y la democracia, habrán fracasado y con ella el progreso social político y económico que representa.

Por tanto, la pertenencia a estas redes no es cuestionable por motivos de falta de seguridad; prueba de ello es que todas estas redes sociales están en constante progreso y tienen ya un poder de movilización social antes desconocido, que trasciende ideas de nación, religión, raza, o políticas clásicas, para centrarse en las relaciones de los individuos, como nuevo aglutinante socio-grupal con una fuerza desconocida hasta hoy.

Hay que tener en cuenta que si fuera un Estado *Facebook* (ha alcanzado ya los 250 millones de usuarios) ocuparía el cuarto lugar del ranking mundial, sólo superado por los cerca de 1.300 millones de habitantes de China, los 1.000 millones de India y los más de 280 millones de Estados Unidos.

La comunicación ha evolucionado y está evolucionando de forma progresiva gracias a una tecnología e interfaz ágil, flexible y amigable que agrupa los sistemas de

información y comunicación, como: la Red Universal Digital (RUD); los protocolos de red , la *World Wide Web* (WWW); las *Rich Internet Applications* (RIA); los *Content Management Systems* (CMS), los *Really Simple Syndication* RSS, el *eXtended Markup Language* (XML) y la *Asynchronous Javascript And XML* (AJAX); los *Social Networking* (SoNet); el *Software* social (SoSo), etc. , y por primera vez en la historia esta comunicación es bidireccional de uno a uno o de muchos a muchos con posibilidad de retorno.

Esto permite que la información se comente, se actualice, se matice, se valore, se transmita a la red, a filtros sociales colectivos, y en definitiva que se cree "inteligencia colectiva" a través de las redes sociales y que esté accesible con un solo golpe de *click*.

Los "Mass media" unidireccionales de uno a muchos y sin posibilidad de retorno o con retorno muy limitado encuentran su competencia o quizá su "Aplicación Killer" en los "social media" bidireccionales y capilarizados que establecen una comunicación participativa y representativa en esta "aldea global" , lo cual es de una importancia capital de cara a la propia democracia, que aumenta la participación de forma horizontal y convierte las redes sociales en redes activas cooperativas. En todo caso, como reafirma Gillmor (2004), los recursos de noticias no tradicionales permiten crear un contexto valioso alternativo a los intereses comerciales de los grandes medios, pues éstos se han convertido en "instituciones arrogantes con un conservadurismo poco crítico".

Para Castells (2001) esto implica que el método ha de cambiar, y conscientes de ello, muchos políticos se han planteado utilizar la Red frente al modo tradicional de hacer política.

Un ejemplo reciente lo tenemos en la campaña presidencial de Barack Obama basada en las redes sociales de Internet, utilizando *Facebook* profusamente, luego Myspace, más tarde *Twitter* y al final los blogs.

Otro ejemplo mas reciente es la propia familia real británica que dispone de una página en *Twitter* para permitir, a quien esté interesado, seguir las actividades oficiales de sus miembros.

Pero no todos los políticos que están en *Facebook*, *Twitter*, You Tube, Blogger, etc. aparecen de manera oficial y por su propia voluntad, sino que lo pueden hacer terceros, lo cual es un exponente más del retorno de estas aplicaciones.

Internet cambia el concepto de comunicación tradicional poco interactiva, sólo apta para enviar un mensaje a la población sin esperar respuesta. Existen encuestas (Baldassare, 2000) que indican que este modelo tradicional no convence a la mayoría que considera que sus problemas no interesan a los políticos.

La afinidad de intereses que caracteriza las comunidades virtuales y la sociabilidad que produce también es constatada por Castell y otros autores Katz, Rice (2001) para quienes Internet aumenta las relaciones sociales fuera de la red. En el mismo sentido Di Maggio (2001) que ven el efecto positivo de Internet para la interacción social y para el contacto con nuevas fuentes de información.

Frente a quienes opinan que propicia el aislamiento, se está demostrando como un dinamizador real de relaciones interpersonales, tal es el caso de los *Beers&Blogs*, (B&B) encuentro de comunidades virtuales en el mundo real (F2F).

Incluso muchas veces las redes sociales se están convirtiendo en el último bastión informativo que les queda a la población cuando la censura, el bloqueo informativo o algún desastre impiden que lleguen las demás comunicaciones. Por eso los "*tweets*" empiezan a ser temidos y se censuran en aquellos Estados que tratan de controlar la Red, interviniendo la comunicación o introduciendo filtros para bloquear páginas. Filtros que empiezan a ser demasiado frecuentes. Hoy se está vendiendo a más de 150 países tecnología para filtrar y controlar las comunicaciones, según *The Wall Street* Journal y la BBC.; el argumento oficial es que así se frena la pornografía infantil.

Respecto al régimen interior de estas redes sociales, como revulsivo a la colaboración que se da en ellas entre usuarios y titulares, su estructura de gestión sigue férreamente controlada por su titular o sus dueños, sin importar, la mayoría de las veces, la opinión de sus usuarios, lo cual no siendo ilícito, daña el espíritu colaboracionista de estas redes y genera, a veces, arbitrariedades en la forma de imponer sus criterios particulares con una objetividad discutible para el resto de los usuarios, que, al fin y al cabo, reiteramos son los que las proveen de contenidos. Cuestión ésta a tener en cuenta a la hora de enjuiciar ciertos hechos en la red, en lo que atañe a los datos personales y a otros contenidos que suben los usuarios, y de los cuales pretenden los titulares de algunas redes sociales, ostentar la propiedad absoluta sobre los mismos. Esta arbitrariedad de poder y el ejercicio no democrático del mismo es lo que está provocando el rechazo de su propio colectivo y, en su caso, la rebelión.

Un ejemplo de este tipo de rebelión lo ilustra López Ponce (2009) mediante la fábula que escribió George Orwell en su novela satírica "Rebelión en la Granja" con el reciente caso del "Ban Day" de la red social "meneame.net", que ha ocasionado una rebelión de cientos de usuarios contra los administradores de esta red social, por su forma de ejercer el poder. En desacuerdo con su sistema de votación, que promueve las noticias más votadas a su página principal (corregido posteriormente).

Curiosamente este libro, "Rebelión en la granja", junto con "Nineteen Eighty-four" de George Orwell ha sido retirado recientemente de los Kindle de los clientes de Amazon (según ella, por carecer de derechos), que están muy disgustados al ver manipulada su biblioteca personal de forma remota por Amazon, aunque se les haya devuelto el dinero. Lo que independientemente de su validez legal, ha puesto de manifiesto la fragilidad de la privacidad de los lectores de Kindle que presuntamente pueden ser manipulados a distancia, retirándoles obras compradas sin su consentimiento.

Para David Pogue, en *The New York* Times, la acción de Amazon es tan grave e inaudita como si empleados de una librería entraran de noche en nuestra casa, se llevaran dos libros de las estanterías y nos dejaran un cheque en la cocina. En distintos foros de Internet, varios compradores de las citadas obras en Amazon muestran su disgusto por la medida y advierten del peligro de que el Gran Hermano pueda husmear y administrar los libros que tienes en casa. Los libros o cualquier otro contenido digital, por razones comerciales o políticas.

Otro ejemplo fue protagonizado por *Facebook* con la modificación de su política, términos y condiciones de uso que, en principio, permitía cerrar su cuenta al usuario, y con ello, cancelar todos los derechos sobre el contenido original que se hubiera subido, y que posteriormente fue modificada unilateralmente por *Facebook*, de tal forma, que obtenía con la nueva redacción de los términos y condiciones una licencia mundial irrevocable, perpetua, no exclusiva, transferible, totalmente pagada (con derecho a sublicenciar), que permitía a *Facebook* a utilizar, copiar, publicar, transmitir, almacenar, conservar o mostrar públicamente, transmitir, escanear, cambiar, modificar, editar, traducir, extraer, adaptar, crear obras derivadas y distribuir (a través de múltiples niveles), cualquier contenido que el usuario publique en el servicio de *Facebook* .

Semejante disparate contra la privacidad ocasionó la rebelión de miles de usuarios y la protesta y acciones legales de organizaciones de defensa de la privacidad y protección de datos, entre ellas la *Electronic Privacy Information Center* (EPIC) que exigió que la red social regresara a sus anteriores condiciones.

Ante lo cual *Facebook* retrocedió y volvió a las condiciones de uso anteriores El propio Mark Elliot Zuckerberg, fundador de *Facebook*, lo indicaba en su blog de la siguiente forma:

> *A couple of weeks ago, we revised our terms of use hoping to clarify some parts for our users. Over the past couple of days, we received a lot of questions and comments about the changes and what they mean for people and their information. Based on this feedback, we have decided to return to our previous terms of use while we resolve the issues that people have raised."*

Ante tanta arbitrariedad sería conveniente contemplar, estatutariamente, una cierta participación de los usuarios en la administración y definición de políticas de uso y de privacidad a través de algún método reglado, como encuestas vinculantes, foros, medidas democráticas, etc. para evitar situaciones de abuso y la falta de consentimiento y legitimidad en el uso de ciertas políticas respecto a contenidos que son de los usuarios.

Por otra parte, respecto a la protección de datos existen problemas técnicos y organizativos en estas redes sociales, que necesariamente habría que subsanar, como las posibles copias que pueden circular sin control o la reproducción de datos por otros usuarios o ante las propias debilidades y fallas de seguridad del propio sistema o ante robos de información o usos ilícitos de ésta.

Con respecto a los fallos técnicos o robos de información, alarmados por sus continuas repeticiones, comentamos a modo de ejemplo los siguientes:

El presunto pirata informático francés Hacker Croll ha sustraído información confidencial del sitio de *microblogging "Twitter"*, con datos sobre selección de personal, actas de reuniones, contraseñas, previsiones financieras,... mucha información sensible para *Twitter* cuya seguridad ha sido burlada por tercera vez este año, según la agencia *Associated Press.*

En Alemania, los datos del Registro Civil de Alemania pudieron ser consultados

libremente en Internet debido a un fallo de seguridad

En España, ataques masivos de "*phishing*" en redes sociales han sido usados para obtener datos personales de los usuarios / víctimas, con robos de identidad, de su perfil en la red social y los datos privados de los contactos. Esta información puede ser utilizada maliciosamente de distintas maneras. Pero además, con la información personal del perfil robado y sus contactos, se puede aumentar su virulencia mediante "ingeniería social" con ataques de 'spam', '*phishing*' o 'malware' con los datos reales obtenidos de los contactos, generando confianza en la posible nueva víctima gracias al perfil robado, que hace posible enviar nuevos ataques de *phishing* de la red social y continuar la cadena de propagación.

En Inglaterra, la Agencia de Protección de Datos del Reino Unido hizo público un informe en 2007 en el que aseguraba que 4,5 millones de jóvenes británicos tenían su futuro profesional comprometido por culpa del rastro que habían dejado en las redes sociales de Internet.

Sin mencionar el escándalo producido por la pérdida de dos discos duros con datos (nombres, direcciones, fechas de nacimiento, registros de la seguridad social y en algunos casos detalles de transacciones bancarias) de 25 millones de ingleses al ser enviados por correo normal desde el Fisco a la Oficina Nacional de Auditoría en 2007.

Por otra parte, en Nueva York, su fiscal general anunció el 10-07-2009, que demandará a la red social "Tagged.com" por "robar millones de identidades de personas, realizar prácticas engañosas de mercadotecnia por correo electrónico e invadir la privacidad usando una virulenta forma de 'spam' y engaño a los usuarios.

Sin mencionar este mismo verano el robo de los datos de 130 millones de tarjetas de crédito.

En definitiva, lo que queremos hacer constar es la fragilidad y peligro para la protección de datos en redes sociales, por la negligencia del responsable de seguridad y la falta de seguridad de la tecnología o del propio sistema informático. Lo cual se minimizaría, por ejemplo y en último extremo, con el uso del anonimato como forma de preservar los datos.

Sin que ello deba interrumpir el avance de las redes sociales y las Tecnologías de la Información, lo que obliga a preguntarnos si las autoridades de protección de datos, en nuestro caso la Agencia Española de Protección de Datos, que con tanta pulcritud y eficacia vigila la normativa sobre protección de datos, y con tanto esmero mantiene una *Web* modélica en forma y contenido, debe intervenir de oficio en las "Redes Sociales" para controlar ciertas políticas de protección de datos, pero sobre todo, para inspeccionar y auditar sus sistemas de información y aquellas de sus prácticas presuntamente abusivas. Los códigos de conducta de amplio uso en el sistema jurídico anglosajón, entendemos, no son del todo eficaces para el nuestro, que por el contrario, exige un control democrático más profundo de este proceso de socialización que vivimos con las redes sociales, aunque sólo sea inspirado en el derecho de autodeterminación informativa, base de la protección de datos personales y en la función social que debería abarcar a todas las Redes Sociales. Lo que nos lleva a

pensar, sino debería instituirse legalmente alguna forma de democratización de la gestión de estas redes sociales (por ejemplo, como las asociaciones), que controlen a su vez las políticas de protección de datos y condiciones de uso. Moderando así el exclusivo control actual del titular de las redes o de sus eruditos y manteniendo el prístino valor de las redes sociales, como son la colaboración por igual entre empresarios y productores/consumidores y la socialización del medio. En suma, la interacción social y la participación democrática potenciada, como fundamento esencial de la sociedad de la información.

Tal era el sentir de Castells (2001), cuando afirmaba que la comunicación de los Mass media tradicionales, soporta una estructura jerarquizada que no se diferenciaba del modelo burocrático y centralizado en que funcionaba la sociedad entorno del Estado y la coordinación política clásica. Es decir, que debido a la crisis de las organizaciones tradicionales estructuradas, decía Castells, la coordinación social ya no pudo estar entregada exclusivamente a un ordenamiento jerárquico (Lechner 1997), ya que las redes, modelo en las que se basa la construcción de espacios virtuales, operarían de manera satisfactoria sólo donde exista una pluralidad representativa de los intereses y las opiniones sociales.

Entendemos que las actuales tecnologías y procesos que permiten la existencia de estas redes sociales deben operar siempre con el consentimiento de sus participantes, obtenido con todas las garantías y con un control efectivo de cumplimiento de la normativa de protección de datos, que impida que los datos que se suben para participar y formar parte de estas redes sociales, exceda del ámbito de confianza y de autodeterminación para el cual se subieron incumpliendo la finalidad con la que se ofrecieron. Deben permitir ejercitar los derechos ARCO, con especial importancia el derecho de cancelación de los datos cuando no sean necesarios para la finalidad declarada, conservando sólo los datos para los propósitos legítimos adecuados a las finalidades para las que se recogieron o se entregaron y por el tiempo adecuado, fuera del cual serán cancelados, disociados o anonimizados. Evitando la confección de perfiles, –ideológicos, raciales, sexuales, económicos o de cualquier otra índole- etc. a partir de los datos aportados.

II. La autodeterminación informativa como base de las políticas sobre datos personales en la redes sociales

El antecedente internacional por excelencia donde se perfila el derecho a la "autodeterminación informativa" por primera vez, como un derecho fundamental que garantiza la facultad del individuo de decidir básicamente por sí sólo sobre la difusión y utilización de sus datos personales, es en la Sentencia del Tribunal Constitucional Alemán de 15 de Diciembre 1983, que declaró inconstitucionales algunos artículos de la Ley del Censo de Población de 1982 de la República Federal Alemana, en base al derecho a la dignidad humana y al libre desarrollo de la personalidad.

En España, la jurisprudencia del Tribunal Constitucional definió y configuró este nuevo derecho fundamental de la "libertad informática" en la STC 254/1993, que en su Fundamento Jurídico séptimo (in fine) recoge la garantía de la intimidad que adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona, la llamada «libertad informática» como derecho a controlar el uso de los datos (habeas data). Recogido del mismo modo en la STC 292/2000 en su

Fundamento Jurídico sexto al indicar que el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. Donde el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos.

El concepto clásico de intimidad surgido del famoso artículo de los Juristas Warren-Brandeis denominado "The Right to Privacy" considerado por el juez Cooley como el derecho a ser dejado solo, a ser dejado en paz, como "The right to be alone" se transforma hoy en el derecho a la autodeterminación informativa.

Así, las redes sociales tienen correlativa y necesariamente, pues, que cumplir unos deberes jurídicos que permitan hacer efectivo a sus usuarios el poder de control y disposición sobre sus datos personales de cualquier tipo, sea o no íntimo. Es decir, el derecho del usuario de las redes sociales (como titular del dato) a la "autodeterminación informativa" impone a estas mismas redes que tienen, mantienen, utilizan y tratan, en papel o soporte informático, o en forma automatizada o manual, sus datos de carácter personal, someterse a la normativa de "protección de datos" que supone que el interesado, cuyos datos son objeto de tratamiento, pueda decidir, quién, cuándo y cómo se van a tratar sus datos personales. De lo contrario si estas garantías se tratan de modificar por vía contractual, se debería declarar su nulidad por ser contrarias a esta normativa.

Así pues la "autodeterminación informativa" constituye la base de la libertad y dignidad de los usuarios. Convirtiéndose en el principio rector del consentimiento, que permitirá a cada usuario de estas redes sociales, decidir voluntariamente quien detentará la información que le concierne personalmente, sea íntima o no, con el objeto último de proteger su propia privacidad, identidad, dignidad y libertad. Preservando los aspectos de la vida que no se desea que se conozcan. Lo que implica garantías y facultades que aseguren que esos datos personales que manejan los responsables de las redes sociales sean exactos, completos y actuales, y se hayan obtenido de modo leal y lícito, con la preceptiva información, ya que el contenido del derecho fundamental a la protección de datos, incluye la obligación a que se requiera el previo consentimiento para la recogida y uso de los datos que identifiquen o permitan la identificación de personas físicas, así como el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar los mismos.

La Protección de Datos de carácter personal supone el nacimiento de un denominado derecho de tercera generación que ampara a las personas físicas contra la posible utilización, por terceros, no consentida ni permitida por la ley, de sus datos personales susceptibles de tratamiento. Este derecho fundamental enmarcado en el derecho de la personalidad, libertad y dignidad humana como características fundamentales ha sido recogido en todas las legislaciones sobre protección de datos de los países de la Unión Europea y de nuestro entorno

En este sentido, para interpretar cuándo ha de considerarse que nos encontramos ante un dato de carácter personal, la Agencia de Protección de Datos ha venido siguiendo el criterio, sustentado por las distintas Recomendaciones emitidas por el Comité de Ministros del Consejo de Europa, en las que se indica que la persona deberá

considerarse identificable cuando su identificación no requiere plazos o actividades desproporcionados.

Entendemos que habrá de considerarse pues que la identificación del titular de una cuenta de una red social no exige esfuerzos o plazos desproporcionados, y que los datos de cualquier naturaleza concernientes a ellos que contiene la red social es un tratamiento de datos de carácter personal en cuanto que es identificable su titular. Por tanto la autodeterminación informativa, debe ser base del principio rector de las políticas de los sites de redes sociales y legitíma que los usuarios participen en sus políticas, sin entrar en otras argumentaciones como: la propiedad intelectual de los contenidos de estas redes, los servicios de la sociedad de la información, etc.

Es evidente que si las redes sociales dan el poder al usuario para generar contenidos y compartir información es justo que les den participación y poder para decidir las políticas por las que se gobernará el sitio y que se convierta en la norma de regulación de las relaciones entre los usuarios y los proveedores de servicio de medios sociales, avalada con una legislación que lo desarrolle.

Las autoridades de control, en su función preventiva, deberán declarar nulos e ilícitos, las condiciones o cláusulas que permitan desviaciones de la finalidad con la que fueron recabados los datos. Así como el almacenamiento, la utilización y la transmisión ilimitada o tráfico ilícito de los datos concernientes a los usuarios de estas redes, o cualquier otro acto que suponga la pérdida del poder de control sobre el uso y destino de los datos personales de sus usuarios, es decir, para su dignidad y derechos. Correlativamente deberán vigilar, así mismo, el cumplimiento del resto de deberes jurídicos por los responsables de las redes sociales que permitan hacer efectivo a sus usuarios el poder de control y disposición sobre sus datos personales.

Los derechos de los usuarios deberían ser tenidos en cuenta siempre al definirse y ejecutarse cualquier política de las redes sociales. Frente a lo cual mostramos preocupación por algunos hechos a los que estamos asistiendo en algunos SRS como censura, manipulación, control férreo y subjetivo, pactos contra ley, etc.

III. Perfiles de datos de los usuarios de las redes sociales y debilitamiento de la normativa de protección de datos

La importancia de las redes sociales de cualquier tipo es directamente proporcional a la cantidad, en millones, de perfiles de usuarios de estas redes. Para incrementar estos perfiles con nuevos "participantes/usuarios" se emplea fundamentalmente un proceso viral, en el que los propios participantes o el sistema, en nombre de ellos, manda invitaciones a los cercanos a su propia red social para que se adhieran al sitio con la descripción de su perfil.

Más cuando describimos nuestro perfil de usuario en alguna red social, damos a conocer datos personales, en proporción directa, también, al tamaño de nuestra red social. Este es un efecto perverso para las propias políticas de prevención y protección de datos personales, ya que condiciona nuestra mayor presencia en la red social a la mayor cantidad de datos aportados. Cuanto más completo esté nuestro perfil en una red social, más sentido tiene nuestra pertenencia en ella porque aumenta nuestra interelación con otros usuarios, pero más en riesgo colocamos nuestros datos

personales, pues aunque podemos establecer distintos perfiles (público, privado, íntimo), casi siempre optamos por el perfil público, y esta exposición pública personal desarrollada para construir y mantener nuestra identidad digital en la Red, añade valor a su titular, pero plantea graves problemas sobre el control de la propia identidad, y de los datos que la forman.

Máxime cuando la infraestructura del espacio virtual en el que relacionamos, construimos y gestionamos nuestra identidad digital online, tiende a una convergencia e interoperatibilidad de las distintas redes sociales que permitirá concentrar todos los datos en un solo perfil, lo que ampliará su influencia, incluso ante la propia identidad real.

El mayor problema radica en que la identidad digital que genera estos datos de la actividad y presencia en las redes sociales, dan la falsa impresión al usuario de que permanecen en el círculo de su control y confianza, cuando por el contrario, tienen una difusión y alcance exponencial descontrolado, donde, por un lado, la cancelación de los datos "subidos" en el SRS no es efectiva porque, o bien no se lleva a efecto, o bien permanecen en otros enlaces y se reproducen aunque el usuario cierre su cuenta. Así como en otros casos se desvía de su carácter inicial la finalidad real de algunos de estos datos. Lo cual genera las protestas de los usuarios por la no cancelación efectiva y/o por permitir que alguna aplicación los utilice para otras finalidades.

Además la política de privacidad de sus afiliados no incluye información relativa a opciones de usuario a efectos de gestión de cookies, donde se especifique claramente que otros terceros podrán incluir y leer cookies en el navegador de usuario; o el mismo contrato de adhesión donde se les conmina a aplicar y cumplir una política de privacidad adecuada, desconociendo los efectos transnacionales de Internet.

Y por último, y no por ello menos grave, el problema de la minoría de edad del usuario, en donde se pone el acento en la solución del problema prohibiendo a los menores la entrada o controlándoles los contenidos en los SRS, como si el problema se solucionara prohibiendo la entrada y los contenidos a las víctimas, en lugar de educarlas o enseñarlas a cumplir los requisitos necesarios y a afrontar los peligros inherentes a la seguridad de la información. En lugar de dirigir de forma efectiva y eficiente la vigilancia de lo que se hace realmente con los datos de las redes sociales; con los perfiles de los usuarios; con las cookies que introducen y con los datos de los usuarios que no se cancelan ni destruyen, etc. ; y de lo que se hace para acabar con las practicas dudosas o el malware, etc.

En este sentido Piñar Mañas, JL (2009) asevera que la solución para proteger la identidad de los menores no consiste en aplicar medidas restrictivas, lo que sería recrear "el síndrome de la fruta prohibida".

El problema no es baladí ya que el 77% de los menores españoles que utilizan redes sociales cuelgan un perfil personal accesible a todos los internautas, según revela el Libro Blanco de los Contenidos Digitales elaborado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), que merece sea tratado en epígrafe aparte.

Todo lo cual, entendemos, confirma la necesidad de dotar de una normativa

efectiva y coherente la protección de datos en las redes sociales.

La Comisión Europea, consciente de este problema, aboga por un marco regulador para las bitácoras a través de un DNI para los "bloggers" . Así mismo elabora un código de conducta para regular las redes sociales de Internet, cuya iniciativa surgió tras una recomendación de la Agencia europea de Seguridad de las Redes y de la Información (Enisa), que desde su sede en Atenas ha alertado sobre los potenciales riesgos de esos clubes sociales virtuales , recomendando la revisión de su marco regulador. Aunque disentimos de la efectividad de los "códigos de conducta o memorándum de entendimiento" no habitual en nuestro ordenamiento jurídico y de la identificación electrónica "DNI específico", que impide el seudónimo o anonimato como forma de preservar la privacidad.

As la Comisión de Libertades Informáticas, aunque refiriéndose a prácticas en los aeropuertos (videovigilancia a pasajeros y escaneres) censura la poca decisión de la Comisión Europea, que en vez de propiciar una armonización para garantizar los Derechos Fundamentales de los ciudadanos y ciudadanas que vivimos en Europa, lo que está propiciando es una obsesión para que cada Estado de la Unión, recopile el máximo de información de cada uno de nosotros.

Estamos totalmente de acuerdo en que la adopción de instrumentos para la protección de los intereses nacionales y, en particular, para la seguridad nacional y la investigación de delitos graves es prioritaria frente a cualquier derecho. Siendo constitutivo de un interés general superior, que debe corresponder al imperativo de claridad normativa inherente al Estado de Derecho. El establecimiento de obligaciones y medidas de control y vigilancia está justificado en aras de proteger la seguridad pública, el problema es que se están debilitando, a nuestro juicio, los principios básicos de la protección de datos sin el suficiente respeto de los derechos relativos a la privacidad, intimidad.

Por un lado, los Estados, las empresas y Organizaciones diversas se están dotando de amplias medidas de control, videovigilancia, monitorización informática, geolocalización, interceptación de todo tipo de comunicaciones electrónicas (vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles, etc.), retención y procesamiento de datos personales; filtrado de contenidos, aplicaciones y servicios, etc. de forma cada vez más creciente.

Por otro, ante la generalizada sensación de inseguridad se percibe un cierto debilitamiento de las políticas básicas de protección de datos y, si bien las medidas de seguridad contemplan situaciones especiales y ciertas prevenciones, no puede invadirse con ellas la privacidad de los usuarios de redes sociales o de otros servicios de Internet, ni violarse la reserva de ley orgánica establecida en el artículo 81.1 de la Constitución, ante el derecho fundamental al secreto de las comunicaciones y a la protección de datos (artículo 18.3 , 18.4 y 55.2) de la Constitución.

Siendo así que, en todo caso, son las Leyes Orgánicas las únicas que regulan las garantías necesarias para legitimar la injerencia de los poderes públicos en el derecho al secreto de las comunicaciones y a la protección de datos.

En este sentido, por ejemplo, la Ley 32/2003 en materia de interceptación de

comunicaciones, así como Ley 25/2007, de 18 de octubre, entendemos vulneran la reserva de ley orgánica. Aun cuando se haya modificado el artículo 33 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en su redacción dada por la Ley 25/2007, de 18 de octubre que reproduce los "nuevos" apartados sexto y séptimo del artículo 33 de la Ley 32/2003, y sin que ello dote de aptitud jurídica al Reglamento para regular esta materia. Incuestionable, en todo caso, en los apartados 6º y 7º del referido Art. 33, en los que se impone a los sujetos obligados facilitar al agente facultado una serie de información, que puede no estar incluida en la orden de interceptación. Y sin que además sea suficiente la remisión de esta última al artículo 579 de la Ley de Enjuiciamiento Criminal y a la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial previo del Centro Nacional de Inteligencia.

Así como los intentos de criminalización o la interrupción del servicio de acceso a Internet, sin control judicial de los consumidores, no es una buena solución para combatir la piratería informática en las redes sociales, la monitorización de los usuarios en estas mismas redes en aras de la seguridad, creemos, tampoco es una buena solución.

El aumento de la supervisión por parte de las autoridades y el debilitamiento legislativo se hace patente también con la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la directiva 2002/58/ce, (DOUE 13.4.2006); que implica un régimen de conservación de determinados datos con fines de prevención, investigación, detección y enjuiciamiento de delitos, que obliga a los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones a garantizar que los datos de tráfico, localización e identificación del abonado estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, con determinadas condiciones y períodos de conservación.

La transposición de esta Directiva Europea, mediante la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, supone también en la ley una cierta regresión del derecho a la intimidad. La Ley, que tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales. Establece como excepción al régimen general de la LOPD, que el responsable del tratamiento de los datos no comunique la cesión de datos efectuada de conformidad con esta Ley, y pueda denegar la cancelación de los datos que soliciten los usuarios basándose en estas previsiones.

Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

Por su parte, la STS de fecha 9 de mayo de 2008 es significativa, declarando que las direcciones IP en redes P2P no están protegidos por el derecho a la intimidad. Y en consecuencia, declara válida la prueba de los rastreos efectuados sin autorización judicial previa, mediante los cuales se obtuvo el listado de IPS inculpatorio. Considerando, además, que cuando se utilizan estas redes muchos datos pasan a ser públicos en Internet.

Sin duda, la sentencia, a nuestro entender, desconoce el carácter de dato personal de las direcciones IP y de que los datos de estas redes, si identifican o hacen identificable al usuario, constituyen datos de carácter personal.

Así lo entendió la sentencia del Tribunal de Justicia de la Unión Europea (TUE), de 29 de enero de 2008 en el Caso Promusicae – Telefónica que rechazó los argumentos de la demandante por los cuales ésta pretendía lograr que se le revelase los datos de los clientes que se descargasen obras musicales a través de las redes P2P (Kazaa), por vulneración de determinados derechos de autor. En ella la Gran Sala resolviendo la petición de decisión prejudicial sobre la interpretación de diversas directivas afectadas, en el marco de un litigio entre la asociación sin ánimo de lucro Productores de Música de España (Promusicae) y Telefónica de España, S.A.U. En relación con la negativa de ésta a comunicar a Promusicae, que actúa por cuenta de los titulares de derechos de propiedad intelectual agrupados en ella, datos personales relativos al uso de Internet a través de conexiones suministradas por Telefónica. Declaró que los Estados miembros no están obligados a imponer, en una situación como la del asunto principal, el deber de comunicar datos personales con objeto de garantizar la protección efectiva de los derechos de autor en el marco de un procedimiento civil.

En el mismo sentido, el Grupo de trabajo del artículo 29 considera las direcciones IP como datos personales en su Dictamen 4/2007, declarando además que en aquellos casos en los que el tratamiento de direcciones IP se lleva a cabo, con objeto de identificar a los usuarios de un ordenador (por ejemplo, el realizado por los titulares de los derechos de autor para demandar a los usuarios por violación de los derechos de propiedad intelectual), el responsable del tratamiento prevé que los «medios que pueden ser razonablemente utilizados» para identificar a las personas pueden obtenerse, por ejemplo, a través de los tribunales competentes (de otro modo la recopilación de información no tiene ningún sentido), y por lo tanto, la información debe considerarse como datos personales.

Las perspectivas tampoco son halagüeñas analizando las propuestas legislativas del denominado paquete Telecom (Telecoms Package) para armonizar las normas sobre telecomunicaciones e Internet. Que en lo referente a la protección de los datos personales o de los consumidores, incrementa las amenazas a la protección de datos y la privacidad, a través de la retención y procesamiento de datos personales por "razones de seguridad", además de permitir el filtrado y la negación de acceso en línea a material protegido. Sin garantizar a los usuarios la existencia de prácticas no discriminatorias, ni restricciones injustas del servicio, ni controles legales sobre las actividades de los proveedores de servicios que impidan las prácticas injustas y restrictivas.

Ya que de prosperar las propuestas legislativas, los ISP tendrán potestad para

discriminar el tráfico. Se diluirá la protección como dato personal de las direcciones IP hasta desaparecer y las propias redes sociales sufrirán bloqueos. La neutralidad de la red se perderá, etc.

Frente a ello entendemos que las infraestructuras de las redes sociales y las operadoras que exploten redes públicas de comunicaciones electrónicas, deben adoptar las medidas técnicas necesarias para garantizar el secreto de las comunicaciones y la protección de datos. Ya que serán también el soporte sobre el que se desarrollen los productos, servicios y aplicaciones de la sociedad de la información, y el funcionamiento libre y democrático de aquellas, sin restricciones, condicionará el futuro de éstas.

IV. Responsabilidad y riesgos de los menores de edad en las redes sociales

La minoría de edad de los usuarios de estas redes sociales, entraña riesgos especiales que pueden dar lugar a la imposición de diversas sanciones y a la responsabilidad correspondiente por los daños o perjuicios causados. Además pueden ser nulas las posibles condiciones o políticas aceptadas por ellos sin el consentimiento y autorización paternal.

Aunque el artículo 315 del Código Civil define la mayoría de edad a los 18 años, no define la minoría de edad. En principio hay que diferenciar los usuarios mayores de 14 años de los restantes menores de edad. Los mayores de 14 años, por sus condiciones de madurez pueden consentir, por sí mismos, el tratamiento automatizado de sus datos de carácter personal. En cambio, los menores de 14 necesitan el permiso paterno.

En este sentido, la Agencia Española de Protección de Datos ha manifestado en repetidas ocasiones que los menores de 14 años necesitan el permiso de los padres para registrarse en redes sociales y que no lo pueden hacer por sí solos. Incluso, indicamos nosotros, que aunque conste el consentimiento del menor o de sus representantes legales, cualquier utilización de su imagen o su nombre en los medios de comunicación, que implique menoscabo de su honra o reputación, o sea contrario a sus intereses se considerará intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, que puede, en este sentido, entendemos nosotros, ser extensivo a las redes sociales, como integrantes que son de los medios de comunicación (Mass sociales).

En los Estados Unidos, la Children's Online Privacy Protection Act (1998) establece una serie de salvaguardas para la privacidad de los menores en Internet. De las que destacamos que no se puede recabar por Internet ninguna información o dato de carácter personal de menores de 13 años sin el permiso verificable de sus padres o representantes legales. Los cuales tienen el derecho a conocer qué información sobre sus hijos se les ha solicitado y su finalidad, así como el derecho a decidir sobre su cesión a terceros o sobre su cancelación.

Las distintas responsabilidades están pues en relación directa con el número de años del menor:

Para exigir la responsabilidad penal se requiere un grado de madurez suficiente del menor, y muchos menores, a menudo, no tienen sensación de culpabilidad o no aprecian las consecuencias de su decisión y sus eventuales repercusiones sobre su vida futura.

El Código Penal, aunque se puede aplicar excepcionalmente a menores de edad, comprendidos entre dieciséis y dieciocho años, no serán responsables criminalmente los menores de dieciocho años con arreglo a este Código. No obstante, cuando un menor de dieciocho años y mayor de catorce años cometa un hecho delictivo podrá ser responsable por la comisión de hechos tipificados, como delitos o faltas en el Código Penal o las leyes penales especiales y podrá dar lugar a ser sancionado con internamiento en régimen cerrado, abierto, semiabierto, terapéutico; tratamiento ambulatorio; asistencia a un centro de día; permanencia de fin de semana o libertad vigilada; prohibición de ausentarse del lugar de residencia; prohibición de acudir a determinados lugares, establecimientos o espectáculos; prohibición de aproximarse o comunicarse con la víctima o con aquellos de sus familiares u otras personas que determine el Juez, etc.

En cuanto a la responsabilidad civil por los daños y perjuicios causados, incluidos los morales, se ejercitará por el Ministerio Fiscal, salvo que el perjudicado renuncie a ella, o la ejercite por si mismo o se la reserve para ejercitarla ante el orden jurisdiccional civil.

Responsabilidad que alcanzará, solidariamente, en el caso de menores de dieciocho años a sus padres, tutores, acogedores y guardadores legales o de hecho. En el entendimiento que si éstos no hubieren favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada por el Juez según los casos.

En el caso de menores de catorce años no se le exigirá responsabilidad, sino que se le aplicará lo dispuesto en las normas sobre protección de menores previstas en el Código Civil y demás disposiciones vigentes. En este caso, el Ministerio Fiscal deberá remitir a la entidad pública de protección de menores testimonio de los particulares que considere precisos respecto al menor, a fin de valorar su situación, y dicha entidad habrá de promover las medidas de protección adecuadas a las circunstancias de aquel conforme a lo dispuesto en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.

Sin olvidar que el artículo 162.1º del Código Civil exceptúa de la representación legal del titular de la patria potestad a "los actos referidos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo".

Pero como indicábamos al principio de este epígrafe, muchos menores, a menudo, no tienen sensación de culpabilidad, aunque cada vez son más conscientes de la falta de privacidad. Nosotros entendemos que todavía no son conscientes del

destino y uso de sus datos, ni de quien controlará el acceso a la información que revelan ni de las implicaciones que ello puede conllevar.

Los datos que se envían a las redes sociales por los menores escapan de su control, una vez que estos datos salen de su círculo de confianza para el que fueron entregados, perdiendo su intimidad y privacidad y el carácter predeterminado de privados. Hecho que se agrava por la falta de advertencia de su potencial lesividad al menor de estos hechos y de sus consecuencias futuras. Y por el exceso de confianza de estos usuarios con las redes sociales y sus contenidos, que en ocasiones pasan a ser proactivos y altamente colaborativos, integrando la red social en su propio entorno personal. Lo que inhibe las defensas o prevenciones, ante el riesgo real de pérdida de control. Y hace necesario formarle para un uso responsable de las redes y controlar la tecnología y las aplicaciones implicadas en estas redes sociales.

Por tanto, si mantener la privacidad en general es difícil, en el caso especial de los menores en las redes sociales preocupa que los datos se compartan en Internet sin las debidas garantías, y ante la certeza de riesgos importantes como:

La falta de control de los datos de cualquier tipo. Ante la facilidad de los menores para la captación de imágenes, videos, audio, y datos con la tecnología actual y la mayor facilidad para transmitirlos y difundirlos en las redes sociales. Hace que este material propio, plagiado, ajeno, de personas identificadas o identificables o en situaciones de identificabilidad inequívoca, usado en muchos casos sin consentimiento de su titular, incida en situaciones de riesgo para los menores si no se hace con el debido control:

Por un lado las imágenes son datos personales y para su utilización, lo mismo que el resto de datos, es necesario el consentimiento del titular, que en el caso de los menores de 14 años deberá estar autorizado por sus padre o tutores, lo que en caso contrario, podría constituir revelación de secretos o violaciones de la privacidad e intimidad.

Por otro, si son imágenes de contenido sexual pueden tener transcendencia delictiva si se trata de menores de edad con conductas que puedan estar relacionadas con la pornografía infantil; acoso sexual (Art. 184 CP); exhibicionismo obsceno y provocación sexual (Art. 185 y 186CP); corrupción de menores (Art. 187 CP); o pueden tipificar el "sexting" con imágenes robadas o entregadas privadamente que pueden ser sumamente nocivas cuando pasan al dominio público, vulnerando la intimidad y privacidad de la víctima que queda desprotegida a merced de cualquier agresión o acoso, como el ciberbullying, que constituye uno de los principales peligros para los menores en Internet con resultados emocionalmente devastadores, cuyo aumento de potencialidad lesiva en las redes sociales podría constituir un delito contra la integridad moral 173-1 CP y el grooming con una finalidad mas especifica que puede derivar en un posterior abuso sexual. En algunos casos implican otros tipos delictivos como Amenazas (Artículos 169 y 171 Código Penal). Coacciones (Artículo 172 del Código Penal). Calumnias (Artículo 205 CP). Injurias (Artículo 208 y 209 CP.) Delitos contra la libertad e indemnidad sexuales (artículos 181 a 183). etc.

Por su parte, las redes sociales amplificarán, potenciarán y dirigirán el daño justo a nuestro entorno social con acciones repetitivas emocional y psicológicamente

lesivas para la víctima, con lo que la presión psicológica se podrá hacer verdaderamente insoportable.

Riesgos potenciales reales que pueden encontrar en sus páginas los menores de edad y de los cuales pueden ser responsables, en determinadas ocasiones, los titulares de las redes sociales por no actuar con la diligencia y prevención necesaria, ni de acuerdo a las prescripciones legales. Así como de los órganos legislativos comunitarios y nacionales ante su pasividad en dotar de instrumentos legislativos adecuados a estas redes sociales.

La responsabilidad de las redes sociales puede estar en la comisión de hechos o políticas abusivas, alegales o ilegales o negligentes, no solo hay que buscarla en la conducta de buena fe o despreocupada de los usuarios, en especial si son menores. Así: la falta de verificación de la edad a los efectos jurídicos del consentimiento y validez de los actos realizados por menores en las redes sociales, es una "obligación" de los titulares de estas redes sociales, en materia de contratos, protección de datos, servicios de la sociedad de la información, etc. En consecuencia, la falta de exigencia del consentimiento expreso y por escrito de los padres o tutores del menor en sus políticas es ilícita.

Así como la falta de garantía de que las opciones de privacidad estén destacadas y sean accesibles fácilmente en todo momento, y la falta de garantía de que funcione correcta y eficazmente en todo momento informando a los usuarios quién puede ver lo que cuelgan en línea y qué peligros existen de manipulación. La falta de garantía de que todos los perfiles y listas de contactos de los usuarios menores de edad estén predeterminados como «privados».

La no cancelación de perfiles y cookies; la cesión de datos; los usos distintos a la finalidad para la que fueron recogidos; el registro de datos de los usuarios que exceda de las finalidades del proveedor del servicio de la red social; la solicitud de datos excesivos; la falta de consentimiento informado; la indexación de datos y perfiles personales; la indexación de listas de contactos y de imágenes en buscadores que permitan su localización; la falta de control (filtros) para evitar el spam o comunicaciones no consentidas; el malware, etc. Como obligaciones en materia que afecta a la normativa sobe protección de datos. Así como el phising y *spoofing*, los acosos, daños, y comportamientos fraudulentos etc. en materia penal.

Pero referido a la protección de datos, insistimos, hay que dirigir de forma efectiva y eficiente la vigilancia de lo que realmente se hace con los datos y sancionar las practicas dañosas, actuando de oficio los órganos responsables si es necesario.

Pensamos que las situaciones que pueden constituir riesgos pueden tener su origen, entre otras, en el estado actual de las TIC y la falta de seguridad. Amenazas técnicas y pérdida de información. Sin el establecimiento por la Administración de medidas legislativas de control específico para estas redes.

En este sentido las conclusiones del análisis de la percepción de los padres sobre la situación de seguridad general en el uso de las TIC por niños y adolescentes del "Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes" indican que el mayor porcentaje (60%) de los padres y madres demandan que debería ser la

Administración la encargada de hacer de Internet un sitio más seguro para los menores. Además las tasas de incidencia directa (al propio menor) de amenazas técnicas son las más altas de los riesgos analizados en el estudio.

El establecimiento en el equipo de Antivirus, Antispam, Antiphising y firewall y backup; Eliminación de archivos temporales, cookies e historial de navegación; Seguridad en el establecimiento de Contraseña y Encriptación de datos, mejora en el lado del Cliente la seguridad, pero implica demasiadas obligaciones no la soluciona completamente.

Todo lo cual nos confirma la necesidad de dotar de una regulación efectiva y coherente de protección de datos a estas redes sociales (SRS). Constatando el sentir generalizado de dotar a estas redes de la seguridad necesaria que minimice los actuales riesgos, en especial referidos a los menores.

Todo esto pudiera dar la impresión que el sector público no ha tomado iniciativas al respecto, nada más lejos de la realidad; lo que ocurre es que no se acaba de plasmar normativamente las prevenciones necesarias que regularicen estas redes sociales. En este sentido, con ámbito internacional, la 30 Conferencia Internacional de Autoridades de Protección de Datos y privacidad celebrada en Estrasburgo, en octubre de 2008, propuso elaborar una normativa común de ámbito mundial para las redes sociales, que garantice una protección mínima y básica, sobre todo para los menores, acordando la celebración en Madrid, en noviembre del año 2009, de la 31 Conferencia Internacional de Protección de Datos, que elabore un primer borrador de esta regulación con miras a su aprobación a nivel internacional.

Entre otras muchas iniciativas dirigidas a preservar a los menores de los riesgos de las redes sociales, enumeraremos a continuación algunas:

Por un lado el Parlamento Europeo y del Consejo, establece programas comunitarios plurianuales sobre la protección de los niños en el uso de Internet y de otras tecnologías de la comunicación (Safer Internet). El nuevo programa que la UE adopta tiene como objetivo hacer de Internet un lugar más seguro para los niños.

También la Comisión de la Sociedad de la Información y Medios de Comunicación, órgano ejecutivo de la Unión Europea, alcanzó un acuerdo voluntario en Luxemburgo, el 10 de febrero de 2009, con ocasión de la celebración del Día Internacional, por una Internet más Segura con algunas redes sociales en Internet (Arto, Bebo, Dailymotion, *Facebook*, Giovani.it, Google/YouTube, Hyves, Microsoft Europe, Myspace, Nasza-klaza.pl, Netlog, One.lt, Skyrock,StudiVZ, Sulake/Habbo Hotel, YahooEurope, y Zap.lu.) para mejorar la seguridad de los menores de edad que utilizan redes sociales. Los objetivos del acuerdo van dirigidos en general a garantizar la privacidad de la información de los menores y proporcionar un botón para «denuncia de abusos» fácil de utilizar. Que dificulte el acceso a las personas con malas intenciones o comportamientos inadecuados.

Por otro lado, para combatir estos riesgos son notorias las acciones de las Autoridades de Protección de Datos y privacidad, así la Agencia Española de Protección de Datos, está informando, en todos los órdenes sobre peligros y prevenciones, llegando a acuerdos generales y acciones concretas para conseguir el

máximo grado de protección a los usuarios y en especial a los menores.

Destacamos, entre ellas, el acuerdo con la red social de Internet Tuenti para prohibir el acceso a los menores de 14 años, así como implantar sistemas que verifiquen la edad de los usuarios, que permitan denunciar fácilmente abusos, que controlen la presencia de menores, y que depuren las cuentas cuyos titulares no superen los 14 años.

La preocupación de las autoridades por la seguridad de los jóvenes en la Red ha llevado también a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información a elaborar un decálogo audiovisual para asesorar a los más jóvenes en el uso de las redes sociales, que se puede consultar en *www.chaval.es.*

A nivel autonómico la campaña "Menores en la Red" ha tratado de informar a los padres de los peligros y también de las herramientas a su alcance, sobre las cuales tampoco se tiene demasiada información.

La autorregulación de la industria, entendemos, (responsables de redes sociales han comunicado su "preocupación por la protección de los menores") si se llevara efectivamente a la práctica y se regularan sanciones para el caso de que no se lleve a efecto o se realizara de forma incompleta, contribuiría también a la prevención.

Pero son medidas de difícil control, que no incluyen la penalización en caso de incumplimiento. Estas medidas o declaración de intenciones realmente hay que articularlas normativamente para que sean operativas.

Regulación que reiteramos debería incluir, respecto a las "politicas" de estos "sites" la opinión y colaboración de los propios usuarios de forma democratica, lo que sería deseable se convirtiera en derecho positivo lo antes posible.

Por su parte compartimos la opinión de educar y enseñar a los usuarios de los peligros y medidas protectoras en contra de la exclusión y prohibición o controles que traten de prohibir la conexión, o para conocer las páginas visitadas, con quién se chatea y cuánto tiempo se emplea en la red, ya que comporta una cierta exclusión de las redes sociales que atenta contra la esencia fundamental de Internet y las redes sociales cual son la interconexión y globalización, tratar de cercenarlo limita la sociedad de la información y del conocimiento. Preferimos un menor informado que un menor excluido.

Por ello, las redes sociales aunque estén en un entorno virtual, sus peligros se asemejan en sus consecuencias a cualquier entorno real, y los daños causados son absolutamente reales.

Por tanto, una forma efectiva de protección es educar, advertir e informar sobre las cautelas y precauciones que hay que adoptar frente a los riesgos existentes. Riesgos que tienen que hacerse explícitos, y en el caso de menores aumentar la preparación y extremar las precauciones ante otros usuarios extraños o sospechosos, o ante la cesión o entrega de datos personales. Pero adoptar medidas de exclusión de la red, insistimos, destruye la propia naturaleza de la Sociedad de la información. Por tanto es indispensable para el avance de Sociedad de la Información, tener un acceso

universal, ubicuo, equitativo y asequible a la infraestructura y servicios existentes, entre ellos las redes sociales.

V. Fuentes consultadas

CASTELLS, Manuel: "La Galaxia Internet, reflexiones sobre internet, empresa y sociedad" 2001; Ed. Areté Barcelona, 317 pp.

Frigyes Karinthy "Chains" 1929;Teoria reafirmada actualmente por el sociologo Duncan J. Watts en "Six Degrees: The Science of a Connected Age" Ed. Norton, 2004.

Libro Blanco de los Contenidos Digitales elaborado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), en: www.comscore.com a 18 de marzo de 2008.

Marshall McLuhan en el sentido de comunicación transfronteriza que hace del mundo una sola comunidad.

Power to the people social media. Wave 3 de Universal McCann dede marzo de 2008

Fuetes electrónicas

Cumbre Mundial sobre la Sociedad de la Información (CMSI) *http://www.itu.int/wsis/geneva/index-es.html* , consultado Julio 2009

Wikipedia: *http://es.wikipedia.org/wiki/Seis_grados_de_separaci%C3%B3n*
http://es.wikipedia.org/wiki/Web_2.0 y *http://en.wikipedia.org/wiki/Prosumer*

"*Facebook* remark teenager is fired" BBC NEWS CHANEL_ 27 February 2009 en: *http://news.bbc.co.uk/2/hi/uk_news/england/essex/7914415.stm;* Consultado Julio 2009

www.ZonaJobs.com.co

García Ferro, Sandra; e-volución-TI; " Redes sociales especializadas empiezan a ganar terreno" 20-1-2009, en *http://www.cronica.com.mx/nota.php?id_nota=409960*

Comunicado de la Comision Europea de la Sociedad de la Información y Medios de Comunicación de 10 de febrero de 2009 (IP/09/232; in the Safer internet day 2009; Bruselas)

The Cocktail Analysis iab Spain Research, (CAWI 14-3 a 8-4 2009

http://tcanalysis.com/.

http://www.sitemeter .com ; -http://twitalyzer .com/twitalyzer/index.asp

http://www.elimparcial.es/mundo/el-uso-de-internet-en-la-campana-de-obama-fue-decisivo-para-su-victoria-43450.html

http://Twitter.com/BritishMonarchy; -http://privacy-data.es/

http:// www.arboldenoticias.com/ 25/06/2008

EcoDiario.es "Si *Facebook* fuera Estado ocuparía el cuarto lugar entre los más poblados" 16/07/2009

http://www.elpais.com/articulo/tecnologia/Amazon/retira/obras/Orwell/Kindle/clientes/elpepucul/20090720elpeputec_1/Tes

http://www.cincodias.com/articulo/empresas/hacker-deja-cuentas-Twitter-desnudo/20090717cdscdiemp_18/cdsemp/

http://www.madrid.org/cs/Satellite?c=CM_Noticia_FA&cid=1142473453247&idRevistaElegida=1142455919293&language=es&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales

"Ataques masivos de "*phishing*" en redes sociales para obtener datos personales"

http://www.elpais.com/articulo/sociedad/Twitter/basta/revolucion/elpepusoc/20090709elpepisoc_1/Tes -BLANCO Silvia09/07/2009

Pelaezedwin: http*://www.monografias.com/trabajos14/rebelion-granja/rebelion-granja.shtml*

LOPEZ PONCE, José: "Meneame.net, la *Web* 2.0 y la Rebelión en la Granja" 3-5- 2009. En: http://www.rizomatica.net/meneamenet-la-*web*-20-y-la-rebelion-en-la-granja/

Update on Terms en *http://blog.facebook.com/blog.php?post=54746167130*

JIMÉNEZ, Marimar "Un hacker deja las cuentas de *Twitter* al desnudo" CincoDias.com 20-07-2009.

"Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres" Instituto Nacional de Tecnologías de la Comunicación (INTECO) bajo una licencia Reconocimiento-No comercial- Edición: Marzo 2009, en: *www.inteco.es.*

Grupo de estudio sobre redes sociales " la Comisión media en un acuerdo entre las principales empresas de la *web* . IP/09/232; Safer internet day 2009; Bruselas, 10 de febrero de 2009"

Medidas de privacidad Red social Tuenti presentada a la AEPD el 06/07/2009 entre las que figura el filtro de perfiles de usuarios menores de 14 años. Exigiendo fotocopia del DNI en caso de sospecha de que el usuario no supere los 14 años y en caso de que no aporten la documentación necesaria, seran dados de baja de la red.

Documento: WSIS-05/TUNIS/DOC/7-S de 28 de Junio de 2006 en *http://www.itu.int/wsis/index-p2-es.html*

Agencia Española de Protección de Datos, Informe jurídico 425/2006 ; Informe jurídico 327/2003; Informe jurídico de la AEPD 0114/2008; Memoria del año 2000

Legislación y Jurisprudencia:

Directiva sobre privacidad y comunicaciones electrónicas, Art. 6(6a)

Constitución Española artículos 18.3 y 18.4 y 55.2 ; -Convención de Derechos del Niño de 20 de noviembre de 1989; -Carta Europea de Derechos del Niño de la R. Parlamento Europeo A3-0172/92 de 8 -7-1992; -Articulo 61-3 de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores; - Articulo 4.3 y Artículo 5 aptdo 1 de La Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor; Articulo 19 del Codigo Penal; Articulo 1 de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

Código Civil y de la Ley de Enjuiciamiento Civil; Ley Orgánica 10/1995, de 23 de noviembre del Codigo Penal ; La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE). Real Decreto 1720/2007.

STC 254/1993, de 20 de julio. Ante la petición de información a la administracion de sus ficheros automatizados solicitada por un particular, sobre sus datos personales.

STC 292/2000, de 30 de noviembre y mas recientemente en la misma linea la SAN, Seccion 1 de 13 Abril de 2005, que señalaba que como uno de los pilares basicos el principio de consentimiento o autodeterminación; -Sentencia de la Sala de lo Penal del Tribunal Supremo de fecha 9 de mayo de 2008 .