Intimidad, privacidad y honor en Internet

POR **VÍCTOR SALGADO SEGUIN**

Se abordan algunos de los derechos personales que se ven más amenazados por la evolución de las nuevas tecnologías, como el derecho a la intimidad, a la privacidad y al honor, en el contexto específico de las redes sociales. Se señalan las principales diferencias entre los modelos norteamericano y europeo, así como la conjugación entre estos derechos y el derecho a la libertad de información de los medios de comunicación.

Todo cambia, nada permanece.
Heráclito de Éfeso (Siglo V a.C.)

No hay duda de que Internet ha supuesto una verdadera revolución en nuestras vidas. El modo en que trabajamos, nos comunicamos y disfrutamos de nuestro tiempo de ocio tiene un antes y un después desde la aparición de la Red de redes. Pero lo cierto es que la propia Red está cambiando y evolucionando a una gran velocidad ante nosotros.

Los riesgos de la Web 2.0

Poco tiene que ver la Internet de hoy con la que nos empezó a llegar a nuestros hogares y empresas allá por la mitad de la década de 1990. Entonces, unos pocos expertos 'privilegiados' eran los creadores de contenidos[1], mediante el manejo de oscuros y complicados lenguajes de programación como el propio HTML; mientras, la gran mayoría de internautas nos limitábamos a 'consumir' dichos contenidos, con una muy limitada o nula participación en los mismos.

Hoy en día, sin embargo, estamos inmersos en el fenómeno de la Web 2.0, donde todos somos creadores de contenidos para la Red gracias a la enorme simplificación de las herramientas de publicación y edición *on line*. Fenómenos como el de los *blogs*, los foros de opinión y las webs de imágenes y vídeos publicados por los usuarios, o las propias redes sociales, son muy recientes (YouTube, por ejemplo, data sólo de febrero de 2005) y han supuesto una nueva

revolución tanto dentro de la propia Red como -y muy especialmente- fuera de ella. Y lo cierto es que esto parece ser solamente la punta del iceberg: los nuevos servicios, como el de las redes sociales o el *cloud computing*, son parte de la tercera revolución que ya nos está empezando a llegar.

Toda esta revolución, cada vez más acelerada, tiene un denominador común: el riesgo para nuestros derechos personales va en aumento y éstos cada vez se ven más y más comprometidos: derechos como nuestra intimidad, nuestra privacidad o nuestro honor están mucho más amenazados en esta nueva realidad.

Nos hemos acostumbrado, además, a que todos los servicios esenciales de la Red que usamos más habitualmente sean completamente gratuitos: las búsquedas que realizamos, nuestro correo electrónico, el perfil de nuestra red social, etc. Esto no es cierto, como veremos; en realidad estamos pagando con otra moneda que no conoce divisa: nuestros propios datos.

Este peligroso modelo de negocio hace que, hoy más que nunca, debamos proteger nuestra intimidad y nuestra privacidad en la Red.

Por otro lado, y toda vez que cualquier persona puede crear contenidos en la Red y además hacerlo de un modo de aparente anonimato, ha causado que en ocasiones se viertan opiniones o informaciones de terceras personas que afectan seriamente a su dignidad personal y a su prestigio social, ambos elementos esenciales de su derecho al honor, como veremos.

El derecho a la intimidad de las personas

Uno de los derechos que se han visto más amenazados por el fenómeno de la nuevas tecnologías e Internet es, sin duda, el derecho a la intimidad de las personas y, más recientemente, el nuevo derecho a la privacidad. Pero ¿qué entendemos por intimidad? ¿Y por privacidad? ¿Cómo protegemos estos derechos en el ámbito de la Red?

Comencemos por el derecho más clásico: la intimidad. El artículo 12 de la *Declaración Universal de Derechos del Hombre* de 1948[2] reza lo siguiente: «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».

En la misma línea, el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[3] dispuso:
«1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho salvo cuando esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de

terceros».

Finalmente, nuestra Constitución de 1978 lo reconoce como un derecho fundamental en su artículo 18:
«1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolucio?n judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

A efectos prácticos, podemos definir la intimidad[4] como una esfera de protección que rodea la vida más privada del individuo frente a injerencias ajenas o conocimiento de terceros, salvo excepciones muy concretas contenidas en la Ley. Dicha esfera protege tanto elementos físicos e instrumentales (como la propia vivienda, la correspondencia o las comunicaciones privadas), como elementos sustanciales que suponen determinados datos sensibles sobre el individuo (su ideología, religión, creencias, vida sexual o salud).

La intimidad es, pues, un derecho fundamental clásico en nuestro acerbo jurídico y ha sido objeto de un amplio desarrollo tanto legislativo[5] como jurisprudencial en nuestro país.

El derecho a la privacidad

Distinto es el caso de la llamada 'privacidad'. Pero ¿de dónde sale este término y en qué se diferencia de la intimidad?

Pues lo cierto es que la propia palabra 'privacidad' no existió en nuestra lengua hasta muy recientemente; el propio *Diccionario de la Real Academia Española* no la incluyó hasta el año 2001 (RAE, 2001).

Su origen está en el término del inglés *privacy*, que sí existe y ha sido reconocido al individuo en el derecho anglosajón.

En concreto, en los Estados Unidos de América el *right to privacy* o derecho a la privacidad fue desarrollado por primera vez en un conocido artículo jurídico de 1890 (Brandeis & Warren), en el cual se definió como t*he right to be let alone*, literalmente 'el derecho a que me dejen estar solo' o, más libremente, 'el derecho a que me dejen en paz'. Pero ¿quién? Pues el Estado y los demás poderes públicos, principalmente, los cuales no podían injerir en el ámbito y la vida privada del individuo, una vez más, sin su consentimiento o sin una autorización judicial fundamentada. Con base en el citado artículo y siguiendo el peculiar sistema de creación de derecho anglosajón, basado tanto en el precedente judicial como en la propia ley, se fue reconociendo el citado derecho en el sistema norteamericano, incorporando principios como la inviolabilidad del domicilio, la correspondencia o, más recientemente, las telecomunicaciones.
Es decir, el *privacy* se traduciría en nuestro Derecho como la 'intimidad'. Entonces, ¿para qué

castellanizar dicho término, si ya tiene traducción? Muy sencillo: porque se necesita una nueva palabra para definir algo muy distinto. Ese 'algo' distinto viene contenido en el apartado 4 del artículo 18 de nuestra Constitución que recordamos a continuación: «4. La ley limitara? el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

Este sencillo pero clarividente párrafo, incluido por nuestro constituyente ni más ni menos que en 1978, sentó las bases de lo que el Tribunal Constitucional ha definido como un derecho fundamental autónomo: el derecho a la protección de datos de carácter personal[6],también denominado 'derecho a la privacidad'.

La privacidad sería así una nueva esfera, mucho más amplia que la de la propia intimidad, que contendría ni más ni menos que todos los datos vinculados a un individuo, sean éstos sensibles o no, los cuales deben ser controlados y protegidos en su tenencia y tratamiento por parte de terceros.

Este derecho a la privacidad es mucho más reciente que el de la intimidad y su nacimiento viene causado directamente por la gran capacidad de las Tecnologías de la Información y la Comunicación (TIC) para tratar gran cantidad de datos de un individuo y ponerlos en relación con otras fuentes a gran distancia y obtener un perfil muy detallado del mismo: sus gustos, sus hábitos, sus aficiones, incluso su ideología o sus creencias religiosas. Todo ello sería ciencia ficción hace 50 años o requeriría unos ingentes recursos de investigación y documentación; recursos que sólo se empleaban en casos y personas muy limitadas y relevantes, pero que hoy en día se podrían extender, a muy bajo coste, a la práctica totalidad de la humanidad.

Este es el motivo de que este derecho se haya intentado proteger también a nivel internacional. Desde el Convenio 108 del Consejo de Europa de 1981[7], pasando por la Directiva Europea 95/46/CE de 1995[8] y la Carta Europea de Derechos Fundamentales[9], cuyo artículo 8 se redacta como sigue: «Protección de datos de carácter personal:
1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».
En España, dicho derecho a la privacidad se protege con gran rotundidad, además de por la propia Constitución, por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)[10].

Asimismo, una loable iniciativa durante la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Madrid y auspiciada por la AEPD[11], permitió la adopción de un texto estandarizado[12], que pretende servir de base para futuras normas en la materia por parte de países sin tradición al respecto.

Sin embargo, esta 'estandarización internacional' se encuentra con una dificultad trascendental: la fuerte colisión entre dos modelos normativos contrapuestos: el modelo europeo y el modelo americano. Dicho choque evidencia la concepción tan distinta que europeos y americanos tenemos sobre la 'privacidad'.

Para un estadounidense, el derecho a la privacidad no es un derecho fundamental reconocido por su Constitución, a diferencia de, por ejemplo, la libertad de expresión recogida en su famosa 'Primera Enmienda'[13]. Dicho derecho, por tanto y tal y como hemos visto, fue creado y perfilado por la propia jurisprudencia americana[14] suponiendo, en la práctica, una protección muy parecida a nuestro derecho a la intimidad (es decir, inviolabilidad del domicilio, secreto de las comunicaciones y protección de la vida privada).

Por el contrario, visto lo analizado, para un europeo la privacidad es algo muy distinto. Dado que nuestra legislación reconoce y protege ya todos estos aspectos mediante el derecho a la intimidad, la privacidad ha surgido como una esfera de protección más amplia. Dicha esfera abarca todos los datos que cualquier entidad tenga sobre un ciudadano, y no solamente los estrictamente privados. En Europa, por tanto, el derecho a la privacidad no es otra cosa que el derecho que protege a las personas físicas en relación al tratamiento de sus datos por parte de terceros o, dicho de otro modo, el derecho a la protección de datos de carácter personal.

También, a diferencia de EEUU y como hemos visto, en Europa el derecho a la privacidad se protege como un derecho fundamental, recogido tanto en el artículo 18.4 de nuestra Constitución como en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, además de ser desarrollado por la LOPD y por la Directiva Europea 95/46/CE.

Estas diferencias son muy notables y, habida cuenta de que EEUU ha sido la cuna de Internet y es donde se ubican las principales empresas proveedoras de sus servicios a nivel mundial, como Google, Facebook, Microsoft o Apple (cuyos modelos de negocio se copian también en Europa), se están creando importantes problemas jurídicos con una gran trascendencia práctica, como luego veremos.

La falacia de la gratuidad

Lo cierto es que tanto el derecho a la intimidad como el de la privacidad se encuentran hoy en día más amenazados que nunca. El motivo, además del aumento significativo de la capacidad de tratamiento y digitalización de la información personal, son los nuevos hábitos de riesgo adoptados por los propios usuarios de la Red.

Y es que los individuos nos estamos habituando peligrosamente a no pagar nada por los servicios que disfrutamos en Internet: el correo electrónico, nuestro perfil en redes sociales, nuestra agenda, nuestras fotos y vídeos, etc. Todo ello lo podemos disfrutar sin efectuar ningún desembolso económico; pero ¿son realmente gratuitos?

Hay quien diría que las empresas que nos ofrecen dichos servicios realmente se están financiando con la publicidad genérica. Esto, sin duda, es cierto en parte: si doy algo gratis,

tengo más visitas; si tengo más visitas, ingreso más por publicidad visionada. Pero ¿ese ingreso es suficiente? A la luz de los precios que se manejan por publicidad mostrada en la Red[15], muy inferiores a los de la publicidad impresa en medios tradicionales, resulta difícil imaginarlo.

Pues bien; las cuentas cuadran cuando nos percatamos de que realmente no son servicios gratis. Es cierto que no pagamos con dinero, pero en cambio sí pagamos con otro bien tanto o incluso más preciado[16]: nuestros datos. Nuestro perfil, nuestros gustos, nuestros hábitos de consumo, etc. Todo ello es información que, consciente o inconscientemente, estamos volcando y/o está siendo recabada sobre nosotros en Internet, ya sea con fines comerciales (publicidad selectiva), económicos, políticos o de seguridad.

Este modelo de negocio deriva principalmente del sistema imperante de los Estados Unidos. En este país, debido a su comentada diferente concepción del derecho a la privacidad, la información de los ciudadanos pertenece a los que la poseen y tratan. Por tanto, las corporaciones pueden comerciar libremente con ella como un activo o producto empresarial más. De hecho, al no existir propiamente una Ley Federal de Protección de Datos en los EEUU, la normativa de protección se deja casi exclusivamente en manos de la autorregulación por parte de las propias empresas que los tratan. Así, son muy comunes en Internet las llamadas Políticas de Privacidad, donde los proveedores del servicio informan a los usuarios sobre las normas internas que han decidido adoptar para proteger los datos personales. Pero al no tratarse de normas jurídicas, las consecuencias ante un eventual incumplimiento por su parte son prácticamente nulas[17].

Por ejemplo, en el caso de Facebook, que se estima alcanzará los 1.000 millones de ingresos en 2010[18], podemos encontrar el siguiente texto en sus Condiciones generales[19] y su Política de privacidad[20]: «Nos concedes una licencia no exclusiva, transferible, con posibilidad de ser sub-otorgada, sin *royalties*, aplicable mundialmente, para utilizar cualquier contenido de PI (incluyendo fotografías y vídeos) que publiques en Facebook o en conexión con Facebook (en adelante, 'licencia de PI'). […] Algunas categorías de información como tu nombre, la foto de tu perfil, tu lista de amigos y de páginas de las que eres fan, tu sexo, región geográfica y las redes a las que perteneces, se consideran totalmente públicas y disponibles para todos, incluyendo las aplicaciones avanzadas de Facebook, por lo que no puedes configurar su privacidad».

Por su parte, Google incorpora el siguiente texto en su Política de privacidad[21]: «Información que usted nos proporciona: al solicitar una cuenta de Google u otros servicios o promociones de Google que requieren un proceso de registro, el solicitante deberá facilitarnos datos personales (nombre, dirección de correo electrónico y contraseña de la cuenta, por ejemplo). Para determinados servicios, como nuestros programas publicitarios, solicitamos también información sobre la tarjeta de crédito u otra información bancaria, que guardamos en formato encriptado en nuestros servidores seguros. Es posible que combinemos los datos que nos proporciona el solicitante a través de su cuenta con la información procedente de otros servicios de Google o de terceros a fin de proporcionarle una experiencia óptima y de mejorar la calidad de nuestros servicios. Para determinados servicios, le ofreceremos la oportunidad de

decidir si desea o no que realicemos dicha combinación de datos.

Cookies: cuando usted visita Google, enviamos una o varias *cookie*s (un pequeño archivo que contiene una cadena de caracteres) a su equipo mediante las que se identificará de manera exclusiva su navegador. Utilizamos *cookies* para mejorar la calidad de nuestro servicio gracias a que almacenamos las preferencias del usuario y a que supervisamos las tendencias de comportamiento, por ejemplo, el tipo de búsquedas que realiza».

En Europa, por el contrario y gracias nuestra mencionada normativa jurídica con poder coactivo, los datos personales siguen siendo propiedad de los ciudadanos y, salvo muy contadas excepciones, no se podrán ceder o tratar sin la autorización de los mismos.

Los riesgos de las redes sociales

Especialmente preocupante para la privacidad e intimidad es el reciente fenómeno de las redes sociales[22] que, lejos de constituir una moda pasajera, han llegado para quedarse y forman ya una nueva realidad social a la que el Derecho debe dar respuesta. Como características fundamentales del nuevo riesgo añadido que suponen las redes sociales para los citados derechos del individuo, podemos enumerar las siguientes:
– Prácticamente la totalidad de los datos y contenidos que se ubican en las redes sociales son volcados en las mismas por los propios interesados.
– Dichos datos y contenidos, desde su propia introducción en la Red, son cedidos y compartidos con terceros, tanto relacionados directamente con el 'introductor' como indirectamente o incluso sin relación.
– Dichos terceros, a su vez, pueden apropiarse de los datos y contenidos y volver a comunicarlos a otras personas o entidades a su vez, haciendo prácticamente imposible su control o retirada ulterior.
– Muchos usuarios de estas redes sociales son menores de edad (incluso menores de 14 años).
– Las empresas, cada vez más, dirigen sus campañas de promoción y publicidad a las redes sociales, tratando muchos de los datos de los interesados para confeccionar perfiles de gustos y compras potenciales.
– Por su parte, a dichas redes acceden igualmente todo tipo de entidades para obtener información de los interesados a muy distintos efectos: procesos de selección, control de productividad y bajas de empleados, perfiles de personalidad, evaluación de solvencia y crédito, evaluación de concesión de subvenciones, seguros, etc.
– Los datos y contenidos de las redes sociales se transfieren a países distintos de donde residen los propios interesados y su acceso y comunicación ulterior se realizan a nivel global.
– Debido a la enorme capacidad de computación necesaria para almacenar y procesar los datos y contenidos de los millones y millones de usuarios diarios de estas redes sociales, se utilizan los llamados sistemas de *cloud computing*[23] o 'computación en nube', que exigen que dichos datos se traten en, literalmente, miles de ordenadores a la vez, repartidos por todo el mundo, siendo muy difícil, por no decir imposible, determinar dónde se almacena físicamente la información en un momento concreto.

Estos riesgos añadidos se agravan con la circunstancia, ya comentada, de que la mayor parte de las redes sociales son propiedad de empresas ubicadas en los Estados Unidos de América, con todo lo que ello implica en cuanto a la normativa y a las medidas de protección en materia de privacidad.

Sin embargo, y con independencia de la legislación aplicable a los proveedores de servicios, lo cierto es que ya se están empezando a exigir obligaciones a los propios usuarios que vuelcan y comparten contenidos y datos de terceros.

Esta eventual aplicación de la LOPD a los propios usuarios de la redes sociales vendría determinada por el número de 'amigos' [24] con que se cuente en las mismas. Así, según el reciente Informe Jurídico 0615-2008 de la Agencia Española de Protección de Datos (AEPD)[25], tener un número demasiado alto de amigos podría exceder el ámbito de las 'relaciones privadas' del usuario y, por tanto, cualquier compartición de datos de terceros entenderse como una posible comunicación pública ilícita.

En efecto, el artículo 2.2.a) de la LOPD excluye de la aplicación de la Ley a aquellos ficheros que se usen 'exclusivamente' en el ámbito privado. Dicho artículo dispone lo siguiente: «El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:
a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas».

Pero ¿qué se entiende por 'actividad personal o doméstica'?

Como bien refiere el citado Informe de la AEPD, este concepto fue aclarado por la Sentencia de 15 de junio de 2006 de la Audiencia Nacional [26] del siguiente modo: «Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos».

Para su traducción en el ámbito de las redes sociales, se remite el citado Informe de la AEPD al Dictamen 5/2009 relativo a las redes sociales en línea, adoptado el 12 de junio de 2009 por el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE[27], órgano consultivo independiente de la UE sobre protección de los datos y la vida privada. Dicho Dictamen señala que: «Generalmente, el acceso a los datos de un usuario (datos del perfil, mensajes, historias…) se limita a los contactos elegidos. Sin embargo, en algunos casos, los usuarios pueden adquirir un gran número de contactos terceros y no conocer a algunos de ellos. Un gran número de contactos puede indicar que no se aplica la excepción doméstica y el usuario podría entonces ser considerado como un responsable del tratamiento de datos».

Por tanto, argumenta la AEPD que no se beneficiarán de este concepto privilegiado de 'ámbito personal' aquellos casos en que «la publicación se efectúe en una página de libre acceso para cualquier persona o cuando el alto número de personas invitadas a contactar con dicha página resulte indicativo de que dicha actividad se extiende más allá de lo que es propio de dicho

ámbito».

Esto significará en la práctica que, por ejemplo, a la hora de publicar datos o imágenes de otras personas (fotos de cenas, amigos, hijos, hijos de amigos, etc.) se deberá obtener el consentimiento previo e inequívoco de dichas personas o de sus representantes legales, según concluye la AEPD, «tanto para la obtención de la imagen como para su publicación en la página web, en tanto que esta última constituye una cesión o comunicación de datos de carácter personal, tal y como viene definida por el artículo *3j)* de la LOPD, esto es, como 'Toda revelación de datos realizada a una persona distinta del interesado'».

Esto, sin duda, supone la primera piedra de una eventual estrategia jurídica de aplicar nuestra normativa europea en el ámbito de las redes sociales, aunque éstas se ubiquen en el extranjero (obviamente, en este caso, para usuarios que se ubiquen en Europa).

Los derechos del interesado

Pero ¿qué puede hacer un individuo cuando se encuentra con datos publicados en la Red sin su consentimiento y/o conocimiento?

Esto, lejos de ser algo anecdótico, se ha convertido en la norma en Internet. Como muestra de ello, sin duda, una de las experiencias más impactantes es buscar nuestro nombre en Google, especialmente si entrecomillamos nuestro nombre completo en el campo de búsqueda. Realmente, la Red tiene mucha más información sobre nosotros de la que siquiera somos conscientes: un expediente académico, una publicación ya olvidada, nuestra ficha de antiguos alumnos, nuestro perfil en redes sociales, esa multa que no fuimos nunca a recoger a correos y un largo etcétera.

Mucha de esta información (por no decir la mayoría) la hemos suministrado nosotros mismos: aquel formulario de alta en el servicio de correo gratuito o en el foro de mi cantante favorito, mi perfil de Facebook o MySpace, mi cuenta de Flickr, mi usuario con vídeos favoritos de YouTube, nuestro perfil profesional para búsqueda de empleo o contactos, etc. A ello se suma que no siempre el titular de la web nos ha informado adecuadamente ni ha obtenido válidamente nuestra autorización para publicar nuestros datos en la Red.

Ante esto, la Ley pone en manos del individuo unas armas muy poderosas para defenderse: los llamados 'derechos del interesado'. Dichos derechos están reconocidos por los artículos 15 y siguientes de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y son principalmente los siguientes: el derecho de acceso, el derecho de rectificación y el derecho de cancelación u oposición.

Dichos derechos pueden ser ejercidos en cualquier momento y gratuitamente por el propio titular de los datos o su representante legal frente a cualquier entidad que posea o trate dichos datos, estando obligado el responsable del tratamiento a actuar en consecuencia en el plazo taxativo de entre 10 días y un mes[28] desde la solicitud, so pena de incurrir en importantes sanciones económicas. En concreto:

– El derecho de acceso nos sirve para que nos informen de todos los datos que tienen sobre nosotros, así como del origen de dichos datos (de dónde los han obtenido) y a quién se los han comunicado.
– El derecho de rectificación nos faculta para instar la corrección de cualquier dato erróneo o incompleto sobre nosotros o nuestros representados.
– El derecho de cancelación u oposición supone que podemos obligar a la completa retirada o bloqueo de nuestros datos de un fichero concreto o de la Red, salvo excepción legal aplicable.

Estos derechos pueden ser ejercidos ante el propio titular o responsable de la web, a través de los medios y datos de contacto indicados por él mismo en su clausulado informativo, según viene obligado por la Ley[29] (en ocasiones, incluso, se puede realizar simplemente por teléfono o *e-mail*) y, en todo caso, sin coste alguno para el solicitante.

Para garantizar y orientar en el correcto ejercicio de estos derechos, la Agencia Española de Protección de Datos confeccionó en su día una serie de modelos y formularios para utilizar como guía en las solicitudes de estos y otros derechos del interesado que puso a libre disposición del público en su página web[30].

Con el correcto y asiduo ejercicio de estos derechos podremos controlar y limitar mucha de la información que sobre nosotros se publica constantemente en la Red.
Sin duda, y como hemos visto, una de las experiencias más impactantes en Internet es la de buscar nuestro nombre en Google. Los resultados de dicha búsqueda nunca dejan de sorprendernos, ya que revela mucha información sobre nosotros y, desgraciadamente, no toda positiva.

La protección ante la vulneración del derecho a la propia imagen y al honor

Acabamos de ver cómo podemos actuar para eliminar dichos datos en base a la normativa de protección de datos (LOPD). Sin embargo, en muchos casos es conveniente hacer ‘algo más’. Hablamos de supuestos en los que se agredan otros derechos, como son el de la propia imagen o el honor.

La palabra ‘honor’ parece un poco trasnochada; sin embargo, es algo plenamente vigente en nuestra sociedad (y más desde que existen las nuevas tecnologías). El derecho al honor es un derecho fundamental, reconocido en el artículo 18.1 de nuestra Constitución, que protege tanto la dignidad como la reputación de una persona en la sociedad[31].

Con el auge de Internet, éste es uno de los derechos más atacados hoy en día. Frecuentemente se publican comentarios o informaciones sobre personas a las que insultan o acusan de hechos que en muchas ocasiones resultan inciertos y que menoscaban su imagen pública. Esto además se facilita con la posibilidad de un ‘aparente anonimato’ en la Red[32] del que muchas veces difunde dichos comentarios. Ello se acrecienta, además, con la enorme capacidad de los buscadores (especialmente de Google) para referenciar e indexar toda esta información y mostrárnosla por orden de relevancia.

De este modo y en muchos casos, al buscar el nombre de una persona en Google lejos de aparecer los datos de su curriculum vitae y de sus logros, nos aparecen críticas, insultos e informaciones dudosas sobre la misma. Esto daña enormemente su reputación tanto a nivel privado como profesional.

Ante esto, la legislación nos protege tanto por vía civil, a través de 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, como por vía penal, a través de los delitos de injurias y calumnias.

En concreto, el artículo 7 de la citada Ley Orgánica dispone lo siguiente: «Tendrán la consideración de intromisiones ilegítimas […]

Tres. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo[…]. Siete. La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación».

Por su parte, y ya en el ámbito de Internet, el artículo 8.1 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) afirma que:
«1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes […] podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes: […] c. El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social[…]».

Gracias a la antedicha normativa, es posible dirigirse tanto contra el que vertió dichos comentarios e informaciones difamatorias como ante el titular de la página web o foro que alberga los mismos. Con la ventaja de que, como efecto inmediato, podemos solicitar a este último la retirada de dichos contenidos de Internet.

Por su parte, y a pesar del 'aparente anonimato' que protege al autor de estos ataques en foros y demás, lo cierto es que todos dejamos un rastro en la Red (el número IP) que puede ser seguido en la persecución de delitos de este tipo[33].

Derecho a la libertad de información de los medios de comunicación

Sin embargo, debemos de aclarar que el derecho al honor no es absoluto y debe respetar igualmente otros derechos fundamentales, como la libertad de la información que protege a los medios de comunicación.

En estos casos, siempre que la información sea 'veraz' y no afecte a la intimidad del individuo,

los citados medios (prensa, radio o televisión) están amparados por la legislación vigente para publicar una noticia referida a aquél, aunque pueda afectar a su reputación. Los únicos límites a estos efectos son la veracidad de la información transmitida y su pertenencia al ámbito público (objeto noticiable).

Con referencia a ello y en el ámbito de Internet, el citado artículo 8.1 de la LSSI dispone lo siguiente en sus últimos dos párrafos: «En la adopción y cumplimiento de las medidas de restricción [...] se respetarán, en todo caso, las garantías, normas y procedimientos [...] para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados.

En todos los casos en los que la Constitución y las Leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo, en tanto garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información».

Por tanto, sólo un juez podría ordenar la retirada de un contenido referido a un medio de comunicación en la Red.

Conclusiones

De acuerdo con todo lo comentado en el presente artículo, podemos concluir que tanto los clásicos derechos fundamentales a la intimidad y al honor como el más reciente a la privacidad personal están sufriendo una fuerte injerencia motivada por el actual desarrollo y auge de los nuevos servicios de Internet.

Aunque nuestra legislación está dotada con los mimbres necesarios para responder a este reto y seguir protegiendo estos derechos en el nuevo escenario, se hace necesaria una rápida reacción tanto de la doctrina como de la jurisprudencia.

El principal reto es entender, plena y profundamente, la nueva realidad que se nos presenta (en continuo y vertiginoso cambio) y, en segundo término, adoptar las medidas necesarias para que nuestros derechos fundamentales no se vean mermados.

Sin duda, entre dichas medidas se encuentran concretos cambios legislativos, pero en especial se debe reforzar el esfuerzo internacional para adoptar normas y estándares comunes que nos lleven a una verdadera protección universal de dichos derechos.

Aunque con puntos esenciales comunes, la comentada actual divergencia entre el modelo norteamericano y el europeo (por no hablar del de otras partes del mundo) en el propio concepto y protección de nuestros derechos supone un riesgo añadido para la salvaguarda los mismos en una sociedad digital globalizada. Una mayor armonización y colaboración se hace imprescindible en este ámbito entre los estados.

Sin duda, ya se están dando pasos en este sentido, aunque queda mucho camino por recorrer.

Notas

1 A los efectos de este artículo, entenderemos por 'contenidos' cualquier dato, texto, imagen, sonido, vídeo o cualquier otra obra o unidad de información disponible en formato digital y accesible a través de Internet.

2 Declaración aprobada y proclamada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948.

3 Adoptado por el Consejo de Europa en Roma el 4 de noviembre de 1950, el texto del Convenio fue modificado en varias ocasiones; la última, por el Protocolo No. 11 (STE No. 155), a partir de la fecha de su entrada en vigor, el 1 de noviembre de 1998.

4 Según la Sentencia del Tribunal Constitucional, Sala 2ª, No. 73/1982, «la intimidad es un ámbito o reducto en el que se veda que otros penetren» (BOE de 29 de diciembre de 1982).

5 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 (BOE de 14 de mayo de 1982).

6 Mediante sendas Sentencias del Tribunal Constitucional Nos. 291/2000 y 292/2000, ambas de 30 de noviembre de 2000.

7 Convenio 108 del Consejo de Europa, sobre protección de datos personales frente a su tratamiento automatizado, de 28 de enero de 1981.

8 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE L 281, de 23 de noviembre de 1995).

9 Carta de los Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000 (DOCE C 364, de 18 de diciembre de 2000).

10 Conocida por sus fuertes sanciones económicas en caso de incumplimiento, la LOPD no fue la primera en la materia en España: la precedió la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), la cual estuvo vigente hasta el 14 de enero de 2000.

11 Agencia Española de Protección de Datos. Véase *http://www.agpd.es*

12 Estándares Internacionales sobre Protección de Datos y Privacidad (también denominado 'la Resolución de Madrid').

13 La primera enmienda a la Constitución de los EEUU recoge además las libertades de culto, prensa, petición y reunión y data del 15 de diciembre de 1791.

14 Véase *http://en.wikipedia.org/wiki/Privacy_laws_of_the_United_States*

15 Véase *http://sergimateo.com/publicidad-cpm-de-los-principales-medios-online/*

16 Véase *http://www.kriptopolis.org/si-pueden-no-googleen*

17 A excepción de intervenciones concretas y puntuales de la *Federal Trade Comission* (FTC) en materia de protección de consumidores y usuarios ante abusos sustanciales por parte de las empresas. Véase *http://www.ftc.gov/*

18 Véase *http://www.ojointernet.com/noticias/facebook-alcanzara-los-1000m-en-ingresos/*

19 Véase *http://www.facebook.com/terms.php?locale=ES*

20 Traducción libre del texto original en inglés. Véase *http://www.facebook.com/policy.php.*

21 Véase *http://www.google.es/privacypolicy.html*

22 Este término genérico se ha popularizado para definir aquellos servicios de Internet cuyo objetivo básico es poner en contacto personas y gestionar sus interacciones, organización, agrupaciones de intereses e intercambio de información entre ellas. Las más conocidas son Facebook, LinkedIn, Twitter y en nuestro país, Tuenti.

23 Véase *http://es.wikipedia.org/wiki/Computación_en_nube*

24 O, en definitiva, el número de contactos que persona tenga en una red social de Internet.

25 Véase *http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdfs/2008-0615_Inaplicaci-oo-n-LOPD-a-actividad-de-particulares-que-comparten-fotos-de-sus-hijos-a-trav-ee-s-de-Internet.pdf*

26 Véase *http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/audiencia_nacional/common/pdfs/sentencia_AN_15062006.pdf*

27 Véase *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_es.pdf*

28 10 días para la atención de solicitudes de rectificación o cancelación y un mes ante solicitudes de acceso (art. 16 de la LOPD y art. 29 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD).

29 Art. 5 de la LOPD.

30 Véase *https://www.agpd.es/portalweb/canalciudadano/denunciasciudadano/derecho_cancelacion_den/index-ides-idphp.php*

31 A este respecto, véase, entre otras, la Sentencia del Tribunal Constitucional No. 185/1989, Sala 2ª, de 13 de noviembre de 1989 (BOE No. 290, de 4 de diciembre de 1989).

32 Nada más lejos de la realidad, dado que todo usuario de Internet está identificado por un número IP (*Internet Protocol*) único, que queda grabado en la Red y que, eventualmente y por práctica forense, puede llegar a ser vinculado con un sujeto concreto.

33 Mediante prueba forense y consulta pertinente a la operadora de la red administradora del número IP concreto, indicando fecha y hora concreta de su uso.

Bibliografía

Real Academia Española (RAE) (2001). *Diccionario de la lengua española*. Madrid: Espasa Calpe.

Brandeis, L. &Warren, S. (1890, 15 de diciembre). The Right to Privacy. *Harvard Law Review*, IV(5),