@RED Y ÉTICA. REFLEXIONES PARA UN USO ÉTICO-CÍVICO DE LAS REDES SOCIALES

JOAN LLUÍS PÉREZ FRANCESCH

Responsable principal del Grupo de investigación sobre libertad, seguridad y transformaciones del Estado del Departamento de Ciencia Política y Derecho Público de la Universidad Autónoma de Barcelona

Muchas de las preocupaciones que podemos tener al intentar orientar la gestión de las redes sociales tienen un *contenido jurídico*, puesto que se trata de aspectos tan importantes como la identidad de las personas, el uso del espacio y la ponderación entre derechos (privacidad, libertad de expresión) o limitaciones de acuerdo con normas y regulaciones. Pero, más allá de las regulaciones jurídicas, hay que desarrollar un código de buenas prácticas en el uso de las redes sociales, a modo de comportamiento cívico. Estas buenas prácticas no deben limitarse a no vulnerar la ley (protección de datos, derechos al honor, a la intimidad y a la propia imagen, etc.) sino que suponen asumir el civismo, el respeto a los demás, la pertenencia a una comunidad virtual, una buena educación. La responsabilidad social de la persona se expresa también en las redes sociales y en la red.

Many difficultties that we can have on attempting to orientate the management of social networks have some juridical contents, since it deals with aspects as important as personal identity, the use of the space and the balance among rights (privacy, freedom of speech) or even limitations in accordance with rules and regulations. But, beyond the juridical regulations, it's necessary to develop a code of good practices in the use of social networks, such as civic behavior. These good practices do not have to limit themselves to not breaking the law (protection of data, right to honor, to privacy and to self image, etc) but rather assuming the public spirit, with respect to others, to belonging to a virtual community, or to a good education. Social responsibility is also expressed in social networks and in Internet.

1. LA NECESIDAD DE UNAS BUENAS PRÁCTICAS O CRITERIOS ORIENTADORES PARA UN BUEN USO DE LAS REDES SOCIALES

Quizás algunas de las recomendaciones que podemos dar no tienen nada del otro mundo y forman parte de una idea de auto-responsabilidad propia de una actitud ante la vida, que no tiene que diferenciar el mundo virtual del real. Se trataría tan sólo de adaptar a las TIC aspectos positivos, sin pensar que estamos ante un ámbito más peligroso que otro, como puede ser la calle. Las actitudes de auto-responsabilidad y de conciencia de nuestras acciones son indispensables para una sociedad madura, en la cual se vinculan de forma constructiva la ética individual como usuario y la comunidad de usuarios de la red. Se trataría, así, de poner en conexión a la persona y la comunidad en que se inserta, una comunidad que se hace con él y gracias a él.

Quiero hablar del concepto de «red social», concepto sociológico antiguo que hace referencia al hecho de intrincar a las personas en un entramado que les da sentido y que las comunica. No se había inventado Internet y ya se hablaba de redes sociales. Ahora bien, las redes sociales virtuales nos han vuelto a poner de relieve la importancia de la comunidad, con unos vínculos interpersonales más sólidos que los meramente societarios, con todos los aspectos positivos y negativos que eso pueda significar.

También quiero destacar la importancia del «saber estar» en el mundo, en el caso que analizamos, virtual, dentro de un rol, un papel, en el marco de una lógica de las relaciones interpersonales, incluso de la amistad y de los lazos de afectividad. Ese «saber estar» comporta lanzar mensajes, ser espectador, incluso promocionar o expandir ideas ajenas, lo cual como es obvio ni en las redes sociales ni en el mundo real puede hacerse de cualquier forma. Supone moverse con criterio en un espacio público donde se desarrolla una parte importante de la vida social de la persona.

Como en todo, se puede hacer un abuso o un mal uso de las redes sociales, sin responsabilidad, con frivolidad o incluso con mala fe. Eso pasa, por ejemplo, cuando se produce una suplantación de la personalidad, se crean perfiles falsos, se promocionan páginas delictivas de signo diverso, desde pornografía infantil a estafas… La confianza en las relaciones humanas es determinante y en nuestro objeto de reflexión todavía más.

Por lo tanto, es necesario saber qué estamos haciendo, permanecer atentos, no fiarse, de la misma forma que tampoco es recomendable hacerlo en la calle. ¿Si en el mundo «real» no nos relacionamos con desconocidos, por qué lo vamos a hacer en el «virtual» y, en especial, en las redes sociales? Los malhechores saben que la facilidad del contacto virtual puede aprovecharse para sus intereses. Y el deseo de compartir o la necesidad de salir de la soledad pueden tener consecuencias catastróficas dentro de las redes sociales si no se realiza con prudencia y, como he dicho, con responsabilidad, sobre todo en lo que se refiere a niños y adolescentes. *Hay que tener cuidado con todo lo que se hace, porque el anonimato no existe en Internet*. Las cosas no son como parecen. Así, pues, es preciso recomendar que no se suban a Internet —y menos aún dentro de la comunidad virtual de una red social— informaciones sensibles o privadas sobre uno mismo, como datos personalísimos, aspectos íntimos, ni fiarse ingenuamente de lo que se ve en una pantalla, porque puede ser una auténtica trampa. Hace falta un cuidado especial con todo lo que hacemos, incluso todavía más que en la calle.

Muchas de las preocupaciones que podemos tener al intentar orientar la gestión de las redes sociales tienen un *contenido jurídico*, puesto que se trata de aspectos tan importantes como la identidad de las personas y sus consecuencias, el uso del espacio y por lo tanto la ponderación entre derechos (privacidad, libertad de expresión) o limitaciones de acuerdo con normas y regulaciones. Los atentados a la privacidad o al honor, por ejemplo, son muy similares en el mundo real y las técnicas de estilo *hacker* que se meten en los ordenadores de los demás comportan inmisiones inaceptables de la privacidad y de datos personales y patrimoniales, entre otros.

Hoy nos hace falta desarrollar un *código de buenas prácticas en el uso de las redes sociales*, más allá de las regulaciones jurídicas, y de la aplicación de los términos y condiciones de uso que marcan las empresas que gestionan estas redes sociales, a modo de comportamiento cívico. Puesto que nos movemos en un *contexto comunitario, voluntario y responsable*, habría que tener claro qué se puede hacer y qué no es recomendable, por razones jurídicas, pero también deontológicas, éticas y cívicas. En definitiva, por salud democrática. Muchas plataformas han adoptado unos criterios para incorporarse a ellas y hacer un uso mínimamente cívico, con unos principios de funcionamiento, especialmente preocupados por su propia reputación, más que por la de sus usuarios. Existen conductas que tienen una sanción jurídica, como el acoso o la violación de los derechos de los menores. Pero lo que yo denomino uso cívico va más allá. En realidad se trataría de *no molestar* a los demás como principio general y de aprovechar los aspectos positivos de las redes sociales en términos de creación de comunidad, de responsabilidad comunitaria, de respeto, de buena educación. *El civismo tendría que ser el conjunto de buenas prácticas aceptadas por la comunidad de usuarios*.

Ese civismo debería incluir la prohibición de la «mala administración», intentando evitar así que quien vulnere los derechos de las personas sean los poderes públicos, auténtico despropósito democrático, mediante espionajes, prohibiciones de derechos por razones políticas, u otras conductas excesivas, en términos jurídicos. Esta «mala administración» también se da cuando no hay respuestas a las demandas ciudadanas y los poderes públicos actúan sin sentido de servicio público y de respeto a las personas usuarias.

También es importante aludir a las implicaciones profesionales del buen uso de las redes sociales, tanto en el sentido de las consecuencias profesionales que puede tener el mal uso, como las potencialidades que presentan para promocionar productos, publicar anuncios, etc., siempre con respeto a los derechos de los clientes. El consentimiento previo de las personas referenciadas, de fotos o datos personales, es imprescindible en cualquier caso como un buen elemento para gestionar correctamente los perfiles.

Por otra parte, desde la perspectiva de la seguridad, las personas tienen que asumir un papel muy activo en la gestión de su seguridad en las redes, ya que los cuerpos de seguridad no pueden realizar el monitoraje de los millones de actividades que se producen diariamente con el fin de prevenir posibles ilícitos penales, administrativos o civiles, y menos aún intentar que se cumplan las buenas prácticas. En consecuencia, la *única forma de conseguir una utilización segura de las redes sociales y de los recursos que ofrece Internet es potenciar la educación de los ciudadanos y eso se debe llevar a cabo mediante programas de concienciación de los riesgos y de las amenazas existentes, con el fin de establecer medidas de autoprotección y para prevenir cualquier suceso no deseado*.

En la actualidad se constata un aumento de la percepción de los riesgos que comportan las redes sociales o de ciertas actividades en Internet (p. ej. el comercio electrónico); pero nos encontramos todavía con una gran falta de información. Eso es especialmente grave en relación a los menores, ya que muchas veces existe esa *rendija generacional* entre padres e hijos, que hace que éstos últimos no tengan la

imprescindible supervisión en la navegación. Por otra parte, la idea genérica que la seguridad es responsabilidad principalmente de los cuerpos de policía es absolutamente errónea y, por lo tanto, muchos ciudadanos adoptan una actitud pasiva o poco reactiva a la hora de tomar las medidas de protección necesarias, en éste y otros campos. En definitiva, la ciudadanía tiene que adoptar un *rol activo* en su autoprotección en el mundo virtual, debe comprender que por las características del medio no puede delegar sin más las tareas preventivas a los cuerpos de seguridad, como tampoco tiene sentido hacerlo en el mundo físico. Finalmente, cabe recordar que es imprescindible que las compañías proveedoras de los servicios de Internet y en concreto las que gestionan las redes sociales se impliquen al máximo con el fin de hacer posible un uso cívico y evidentemente respetuoso con la legalidad y los derechos de las personas.

Tabla 1. Cinco objetivos para mejorar el uso de las redes sociales e Internet en general
(Grupo de trabajo sobre Seguridad del Plan Nacional de Valores, Generalitat de Cataluña, junio 2013)

Objetivo 1	Potenciar una navegación segura y responsable de los ciudadanos en la red (autoprotección de los usuarios).
Objetivo 2	Implicar a las compañías privadas proveedoras de servicios en Internet para conseguir un mundo virtual seguro y evitar así el incivismo informático.
Objetivo 3	Fomentar la educación de los menores en el uso seguro de las redes y concienciar a los padres de los riesgos y amenazas que supone la navegación.
Objetivo 4	Corregir la rendija generacional en el seno de la familia.
Objetivo 5	Proteger los derechos fundamentales de los ciudadanos en el uso de las nuevas tecnologías, evitando ilícitos penales o civiles.

2. CONTENIDOS ILÍCITOS Y NOCIVOS

La Dirección General de Atención a la Infancia y la Adolescencia (DGAIA), del Departamento de Bienestar Social y Familia de la Generalitat de Cataluña, junto con el CESICAT,[1] firmaron en 2012 un convenio de colaboración que tiene por objeto la producción de materiales, la publicación y promoción de contenidos y material audiovisual en los medios de comunicación o la realización de estudios

1. El Centro de Seguridad de la Información de Cataluña (CESICAT) es el organismo ejecutor del Plan nacional de impulso de la seguridad TIC aprobado por el Gobierno de la Generalitat de Cataluña el 17 de marzo de 2009. Es una fundación pública creada por la Generalitat. Para más información, visitar su web: https://www.cesicat.cat/.

sobre la seguridad en el uso de las nuevas tecnologías por parte de niños y adolescentes.[2]

Fruto de esta colaboración, en abril de 2013 se publicó la Circular sobre redes e Internet,[3] en la que como directriz se establece una diferenciación entre los contenidos ilegales y los contenidos nocivos que afectan directamente a la infancia y la juventud pero también a la sociedad en general.

Son ejemplo de *contenidos ilícitos*, entre otros:[4]

— pornografía infantil,
— propagación de material que incite al odio, racismo, antisemitismo u otro tipo de discriminación en función del sexo, religión, origen, orientación sexual,
— propagación de materiales y discursos con violencia o sangre extrema (*gore*),
— incitación al suicidio,
— apología de la anorexia y la bulimia,
— juego en línea ilegal.

Respecto a *contenidos nocivos*, es decir, la información perjudicial para la integridad personal, cabe destacar que no están tipificados como delito y por lo tanto su difusión está permitida. Estos contenidos son diversos, como de tipo pornográfico o violento. Los riesgos están asociados a las conductas tanto de los niños y adolescentes como de otras personas que se comunican con ellos por correo electrónico, las redes sociales y otras plataformas (foros, chats, juegos en red…). Los más comunes son:

— la difusión de datos de identidad personal: nombre, número de teléfono, dirección, correo electrónico… muy importante limitarlo en el uso de redes sociales;
— el contacto continuado con desconocidos y la posterior invitación a intercambiar información delicada o sensible, o a encontrarse físicamente en algún lugar;
— la escalada de mensajes desagradables con vejaciones, amenazas e injurias;
— el abuso escolar y el ciberacoso escolar (*cyberbullying*);

2. Fuentes: «*Benestar Social i Família i el CESICAT organitzen un cicle de jornades sobre seguretat i riscos a Internet i en l'ús de xarxes socials*» [en línea] <http://premsa.gencat.cat/pres_fsvp/AppJava/notapremsavw/detall.do?id=202287&idioma=0>. También «Riscos a Internet i en les xarxes socials» [en línea] <http://www10.gencat.cat/gencat/AppJava/cat/actualitat2/2013/30612riscosaInternetienlesxarxessocials.jsp> (Consulta: 12 junio 2013).

3. Se puede consultar el documento completo en línea en: <http://premsa.gencat.cat/pres_fsvp/docs/2013/06/04/12/45/cdb8cd6d-4594-40b0-9fe0-8f9f00bde20f.pdf> (Consulta: 12 junio 2013).

4. Otros muy graves son el *grooming*, acoso de carácter sexual de un menor; las acciones del *grooming* tienen el objetivo de establecer una relación y un control emocional sobre un niño/a para después abusar de él sexualmente. A diferencia del ciberacoso, este tipo de acoso tiene un objetivo explícitamente sexual. También el *phishing,* como forma de engañar a los usuarios para que revelen información personal o financiera mediante un mensaje de correo electrónico o sitio web fraudulento.

— el tiempo incontrolado en el uso de juegos o dispositivos, que puede comportar problemas de adicción al móvil o caer en el *gambling* (juego con apuestas).

Hay que decir que es necesario denunciar todos los contenidos y acciones de carácter ilícito en las redes sociales y poner los hechos en conocimiento de la policía mediante la denuncia correspondiente. Sin embargo, una vez más reiteramos la importancia de la educación, de la responsabilidad en el uso de las redes, de la prevención y, si se trata de niños o adolescentes, del control parental presencial —acompañando a los menores en la navegación— o mediante el uso de filtros.[5] Los padres, madres o tutores son responsables de las actuaciones de sus hijos y ésta es una responsabilidad que no pueden rehuir en el ejercicio de la patria potestad.

En la misma circular, la DGAIA y el CESICAT también proponen unos consejos en el uso de Internet para niños y adolescentes, y también para padres, madres y educadores/oras.

En el apartado de niños y adolescentes concretan los consejos distinguiendo por franjas de edad: niños de ocho a diez años, niños de once a trece años y niños de catorce a quince años.

Ahora bien, un consejo dirigido a todas las franjas de edad es que en la red se encuentran muchísimas cosas buenas, pero también existe alguna mala. Se avisa que si en una web el niño encuentra alguna palabra o foto que le hace sentir mal, salga de la página y no deje que le moleste. También se recomienda que lo explique a los padres o maestros y, si son adolescentes, a algún amigo o amiga.

También se recomienda a todas las edades no enviar fotografías, ni dar el nombre, la dirección o el teléfono; ser cuidadosos con las listas de contactos y las contraseñas; avisar a los padres sobre las nuevas relaciones que inician en la red, y marcharse de los chats que hagan sentir al niño o adolescente incómodo o molesto.

Asimismo se recuerda que *el acceso autorizado* a la mayoría de redes sociales es a los *catorce años*. Es importante no adelantarse ya que los adolescentes pueden encontrarse con problemas por el solo hecho de no controlar suficientemente quién puede ver la información que publican. Por eso se les recomienda que dejen asesorarse por un adulto en la configuración del perfil cuando accedan por primera vez.

Precisamente, a partir de esa edad se dan consejos más específicos sobre comprar o hacer algo por Internet que pueda costar dinero, sobre dar números de tarjeta de crédito o datos bancarios; también se avisa sobre ciertos programas que se puedan descargar de la red, ya que pueden comportar algún virus o programas espías. También se alerta sobre lo que es información fiable o dudosa.

Finalmente se aconseja al joven que, si se quiere ahorrar posibles problemas y ser un buen ciudadano en línea, actúe correctamente y evite hacer algo que

5. La web del Safer Internet Programme, www.sipbench.eu, se actualiza trimestralmente y compara la efectividad y la robustez de los filtros a diferentes edades, dispositivos y sistemas operativos.

pueda perjudicar a otra gente ya que puede cometer algún delito como por ejemplo amenazar, difamar, atacar el derecho a la intimidad enviando fotografías de compañeros…

En el apartado dirigido a padres, madres y educadores/oras, se explica que la mejor manera de prevenir situaciones de riesgo y ayudar a los hijos o al alumnado a navegar con seguridad es:

— hacerlos conscientes de los beneficios y riesgos de Internet,
— educarlos para que sepan navegar de forma responsable,
— darles estrategias que les ayuden a autoprotegerse mientras navegan.

También es destacable que se recomiende a los adultos que hablen abiertamente con los niños y adolescentes sobre el uso de Internet, que se interesen por lo que niños y adolescentes hacen en el ordenador y mantener una buena comunicación con hijos o alumnos. Asimismo es importante que se acostumbren a presentarnos a las amistades que mantienen por la red.

La mejor estrategia es trabajar con ellos de forma que puedan aprender de lo que ha pasado, adquirir unos hábitos de seguridad y saber como protegerse por si mismos. Crear una atmósfera de confianza respecto al uso de la red nos ayudará a prevenir situaciones de riesgo.

Otro método para prevenir los riesgos es procurar navegar junto a los niños y hacer de Internet una actividad lúdica y familiar. Al compartir dicha actividad se puede comentar con ellos, por ejemplo, la diferencia entre publicidad y contenido educativo o de entretenimiento y mostrarles ejemplos de cada cosa.

En la circular también se aconseja a los adultos que se informen sobre las herramientas de control (como los filtros que limitan el acceso a contenidos nocivos) o que impongan reglas básicas de seguridad en el hogar: colocar el ordenador en una sala común a la vista de todos, fijar los sitios web visitables, horarios de conexión, enseñarles a navegar con seguridad (a tener cuidado con los datos personales y las contraseñas, avisar sobre casos que les resulten desagradables, tratar de conocer a los ciberamigos, compras…).

Un punto importante es también que se aconseje sobre los primeros pasos en el uso del móvil y las redes sociales.

Por último, se exponen alternativas ante un posible problema o si existen indicios de riesgo para los hijos o el alumnado, y así poder reaccionar a tiempo.[6]

6. Ante indicios de riesgo para los hijos o el alumnado, primero se puede hablar con ellos, pero también notificarlo a la dirección electrónica internetsegura@gencat.cat o llamar al 112. En caso de encontrar pornografía infantil, material presuntamente ilegal o cualquier otro que se considere que puede herir la sensibilidad de niños o adolescentes, se puede contactar con la policía para denunciarlo. También se puede denunciar a través del CESICAT a la dirección info@cesicat.cat o al teléfono 977 010 893.

Tabla 2. Consejos en las redes sociales. CESICAT[7]

Las redes sociales te permiten conocer a gente y tener amigos por todo el mundo. Puedes compartir información al mismo tiempo con todos tus compañeros y puedes conocer otras culturas y costumbres. El uso de las redes sociales se ha extendido de forma muy rápida, pero también es un medio que utilizan los delincuentes (sobre todo acosadores sexuales) para captar a sus víctimas. Por eso es necesario estar alerta:
• **No aceptes «amistades» de desconocidos.** En Internet es muy fácil decir mentiras y simular que eres otra persona.
• **Publicar información en las redes sociales es muy fácil y rápido, pero una vez publicada no sabes cómo van a emplearla.** Antes de colgar una noticia o publicar una fotografía piénsatelo bien. No facilites o publiques datos, información, fotografías o videos de otras personas sin que te hayan dado su permiso.
• **Inventa contraseñas largas y complejas.** Utiliza un alias (*nick*) que sólo conozcan tus amigos.
• **Si alguien te molesta o te acosa en algún chat o grupo,** sal del grupo y avisa a tus padres o tutores. Sé respetuoso tú también con todas las personas del grupo.
• **No compartas datos** como el teléfono, la dirección o tu nombre y apellidos. No envíes nunca tus fotos ni facilites tus datos personales a ningún desconocido.
• **En Internet no todo el mundo es amigo.** No quedes con las personas que conozcas mediante la red. Y si quedas con alguien, avisa a tus padres o algún amigo para que te acompañen y queda en un lugar público.
• **No aceptes archivos de personas que conozcas en el chat**, porque podrían llevar algún virus. Incluso las canciones o las fotos que te envían pueden ser peligrosas.

3. UN DISCURSO POSITIVO PARA LAS REDES SOCIALES

De todo lo que estamos comentando deriva la necesidad de hacer un uso ético y responsable de las redes sociales, aparte de atender a las consecuencias legales de los propios actos.[8] No podemos olvidar el gran rol que juegan en la construc-

7. Noticias en la web del CESICAT: «Bienestar y Família y CESICAT organizan un ciclo de jornadas sobre seguridad y riesgos en Internet y en el uso de redes sociales» [en línea] <https://www.cesicat.cat/ca/article/bsf-cesicat-seguretat-xarxes-socials> (Consulta: 4 junio 2013). También consultar la página web por la navegación segura por la Red del mismo CESICAT: <http://www.Internetsegura.cat/>.

8. Sobre el derecho a la protección de datos personales: Ley orgánica 5/1999, de 13 de diciembre, de protección de datos de carácter personal y STC 292/2000, de 30 de noviembre, sobre esta Ley; Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones; Ley 34/2002, de 11 de julio, de servicios de la información y del comercio electrónico, modificada por la Ley 32/2993, de 3 de noviembre; Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (modificada por la Ley 32/2003, de 3 de noviembre, general

ción de una sociedad democrática, con más transparencia y capacidad de debate de los asuntos colectivos.[9] Las redes sociales tienen que promocionar el conocimiento del derecho que también las regula y afecta a usuarios y administradores. De hecho, se discute si los *community managers* de grupos o bloques son responsables de los contenidos de los miembros o seguidores activos. Hoy todo el mundo puede ser considerado periodista, en sentido impropio,[10] como creador de una opinión pública libre, a partir del debate racional de la información puesta en la red; por esa razón hay que velar por la veracidad y por el respeto de los derechos al honor, a la intimidad, a la propia imagen, sin olvidar la protección de datos personales. Un tuit en el Twitter se ve sometido a estos condicionantes por cuanto nos convertimos en partícipes del ágora de la red social. La capacidad de incidir en la *construcción del espacio público deliberativo* y de afectar así a la reputación de los demás (y de uno mismo) hace que la presencia en la red social no pueda utilizarse impunemente para injuriar, difamar o lesionar derechos de los demás. Derecho y ética van de la mano.

Ahora bien, hay que diferenciar entre *hechos y opiniones*. Los primeros tienen que ser verídicos y las segundas, respetuosas con los derechos de las personas. Aparte está la calidad de los mensajes y la vulgaridad de lo que se dice aunque sea verdad. En esta línea, plantearse qué habría que hacer cuando un usuario cuelga, por ejemplo, un tuit erróneo en el Twitter o que contiene una información falsa. ¿La mejor solución es borrarlo, rectificar la información o colgar otro? Dejamos la pregunta abierta, pero la respuesta tiene un fuerte contenido educativo, ético y cívico.

Han aumentado las fotos que se cuelgan y se comparten en las redes sociales. Hay que respetar los derechos de autor y, por qué no, evitar la compartición sin que se formalice la autorización. En otro caso, el usuario se convierte en un personaje «solo ante el peligro» y tendrá que asumir las consecuencias. La identidad y la reputación digital se configuran hoy en gran parte mediante lo que ponemos de nosotros mismos y lo que los demás ponen de nosotros en las redes sociales. Por ello hay que ser cuidadosos y diligentes con lo que decimos, las fotos o vídeos que

de telecomunicaciones, por Ley 59/2003, de 19 de diciembre, de firma electrónica, por Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, y por la Ley 56/2007, de medidas de impulso a la sociedad de la información); STC 94/1998, de 4 de mayo (datos de afiliación sindical, como datos sensibles).

Por otra parte, hay que tener en cuenta los límites y la ponderación entre los derechos fundamentales del art. 20 y 18 CE. La jurisprudencia del Tribunal Constitucional sobre la limitación de derechos fundamentales, como la STC 57/1994, establece que todo acto o resolución que limite derechos fundamentales debe garantizar que las medidas restrictivas sean adecuadas, es decir eficaces para obtener lo deseado, necesarias, que no haya una medida igualmente eficaz pero en cambio menos limitadora de derechos fundamentales, y proporcionada, que el sacrificio final del derecho no sea mayor en relación al objetivo alcanzado. En general es primordial atender al principio *favor libertatis* como criterio interpretativo. Por útlimo, citar la relación que se establece entre la libertad de expresión, el secreto profesional y la seguridad nacional (como ponen de manifiesto el caso Roldán o el caso WikiLeaks).

9. Véase, en este sentido, Castells (2012). Entre otros aspectos hay que reseñar el uso ya imprescindible de las redes sociales por parte de políticos, personajes famosos, profesionales, empresarios, etc. El presidente Obama realizó una intensa campaña en Facebook durante las elecciones de 2008. También cabe recordar la lucha para un uso libre y no sometido a censura en varias partes del mundo, y la capacidad cada vez mayor de convocatoria para encuentros en general y para manifestaciones, huelgas, etc. en especial.

10. Cada usuario se convierte en un creador de opinión pública, sin proponérselo.

colgamos, etc. De hecho, la privacidad, en sentido clásico, era concebida como un santuario que protegía a la persona, cosa todavía muy importante. Pero hoy es algo diferente, porque consentimos fácilmente en mostrar todo tipo de aspectos de nuestra vida, también los más privados e incluso íntimos. Debemos ser conscientes de que frecuentemente el límite que ponemos es muy bajo, tanto en las redes sociales como en Internet en general. Diego Guerrero Fuertes (2010, 2011) ha puesto de manifiesto que la navegación puede ser algo seguro y placentero, siempre y cuando se haga con cuidado y responsabilidad.[11] Facilitar datos financieros, aceptar *cookies* sin pensar, navegar por lugares inseguros, responder a la geolocalización, no atender a la vulnerabilidad del hardware, cortafuegos y antivirus con el fin de evitar caballos de Troya, contactar con extraños, en especial en el caso de menores... tiene sus peligros y no nos ayuda a hacer de la vida digital un mundo seguro y habitable.

Las redes sociales son un importante producto de nuestra sociedad de masas y, por lo tanto, un ámbito adecuado para ejercer determinados liderazgos (comerciales, políticos, ideológicos, etc.). Son también un peligroso campo de experimentación donde la persona *masa* puede adentrarse y ser manipulada, pidiéndole información de todo tipo, y ser objeto de fechorías o actuaciones denigrantes. Las relaciones personales en la red no pasan sólo en sentido horizontal —entre miembros— sino con relación a los creadores o propietarios del servicio, los cuales aprueban unas condiciones de uso que suponen un auténtico *contrato de adhesión*. Este contrato es importante dado que, entre otras cosas, se determina la propiedad compartida de las fotos, la información y el propio perfil de cada usuario, en términos de privacidad (aunque se ofrecen varios niveles). Sin embargo, el fomento del trabajo cooperativo en la construcción de grupos es un dato altamente relevante y formativo, que no podemos obviar. Los administradores de la red normalmente advierten de los controles de privacidad que procuran y articulan mecanismos con el fin de denunciar comportamientos o contenidos ilícitos o peligrosos. Un aspecto a destacar es el «derecho al olvido», actualmente muy en voga puesto que los datos corren rápidamente por la red y acabamos perdiendo su control, incluso aunque nos demos de baja.

Si tomamos como ejemplo Facebook, cabe recordar que tiene una *declaración de derechos y responsabilidades*, basada en la libertad para compartir y conectarse, en la propiedad y el control de la información de las personas que se adhieren, la igualdad de trato entre todos los miembros, la gratuidad, la transparencia y la universalidad. Además, hay que saber que los datos pueden ser cedidos a terceros (como mínimo en los EE.UU.), a pesar del consentimiento expreso exigible por la protección de la propiedad intelectual; que los menores reciben una protección especial (en España no se acepta a menores de catorce años); que hay que dar una

11. «Diez consejos para despistar al 'Gran Hermano' de Internet». *La Vanguardia.com*, 16 junio 2013 [en línea] <http://www.lavanguardia.com/Internet/20130616/54375645613/diez-consejos-evitar-ser-controlados-Internet.html>.

información auténtica del nombre (a pesar de los seudónimos)[12] y de la fotografía, aspectos que *no se consideran datos privados*. Además, Facebook *almacena* información de todo lo que ponemos en la red, incluso obteniéndola de terceros, aunque el usuario puede modular su grado de privacidad. Cuando se cancela una cuenta se elimina el perfil, pero no la «huella» que hemos dejado en la interconexión con los «amigos». Creo que de esto también deberíamos ser más conscientes. Facebook fundamenta el negocio en el marketing según nuestro perfil.

En el caso de Twitter, por citar otra gran red social, es importante leer las condiciones de uso y la política de privacidad. Los tuiteos comportan solicitud de publicidad del mensaje en la red y por lo tanto licencia para gestionarla. El límite de edad de acceso es de trece años en todos los países. En función de los perfiles de los usuarios se ofrece información comercial.

En todo caso, es preciso recordar que los propietarios de las redes sociales son *empresas privadas*, guiados por los principios del mercado y que, como tantos sectores de Internet, es difícil de controlar, vista la no territorialidad de las actuaciones. Aun así, las condiciones de uso fijan siempre las cláusulas contractuales de sumisión jurisdiccional a los tribunales competentes, normalmente de la nacionalidad de la sociedad gestora. El problema, sin embargo, es cómo solucionar los conflictos sin recurrir a los tribunales. Y a menudo también superar una cierta desconfianza sobre el uso real de los datos personales que tienen, por la vía de la cesión de archivos.

Hay que tener siempre en cuenta los parámetros de la Organización para la Cooperación y el Desarrollo Económicos (OCDE):[13] concienciación, responsabilidad, respuesta de los participantes para hacer frente a los retos de la seguridad, ética —respecto a los intereses de terceros—, respeto a los principios democráticos, evaluación del riesgo, adopción de protocolos de seguridad, o reevaluación de la seguridad de los sistemas empleados.

Ahora bien, en términos de *civismo*, no podemos caer en la parte negativa, ya que las redes sociales permiten una nueva forma de comunicarse y de relacionarse muy interesante, y hoy en día ya ineludible, en especial de cara a la juventud. No hay duda que provocan una integración de las personas en una comunidad (aunque sea para compartir fotos, por ejemplo) y, además, de forma muy sencilla y asequible a cualquiera. El hecho de la gratuidad todavía hace más rápida y simple la incorporación a la red, lo que no debería hacernos suponer que tenemos un control absoluto de los contenidos, sino más bien al contrario, porque la información que proporcionamos es precisamente la materia prima del «negocio» de las redes sociales. Y también tendríamos que ser conscientes de que en principio cualquier persona, incluso la más anónima, nos podría observar.

12. Normalmente se exige en las condiciones de uso una identificación real, pero se pueden utilizar seudónimos para ser menos localizable, o para compartir sólo con los amigos que te conozcan la información que se sube a la red. Uno puede poner lo que quiera, pero en sentido estricto eso no estaría recogido por las normas generales de uso de la red, porque facilitaría la creación de perfiles falsos.

13. Recomendaciones de la OCDE en el documento «Directrices para la seguridad de sistemas y redes de información: hacia una cultura de seguridad» adoptadas por el Consejo de la OCDE en la sesión número 1.037, de 25 de julio de 2002.

De la idea anterior derivaría un principio general *de auto-responsabilidad* no tan sólo en el uso de la red sino en el propio hardware que se utiliza. La seguridad es una preocupación general que contextualiza actividades de intercambio de información e incluso de comercio. El acceso a páginas cifradas, o desde un puerto seguro, cuidar la protección de datos personales, el respeto a los derechos de las personas (no tan sólo los de la personalidad sino los conectados a ella como la propiedad industrial e intelectual) tiene que ser la máxima divisa de una buena actuación en las redes sociales.

Claro está que hay que luchar para evitar que se vulnere el derecho al honor de los demás y, por lo tanto, que no se calumnie (acusación de haber cometido un delito) ni injurie (lesionar la reputación y el honor de otros). Es fácil atentar contra el honor de las personas en las redes sociales, si tenemos en cuenta que el propio instrumento nos facilita una actitud proactiva y una predisposición para decir cosas. Deberíamos ser conscientes de que a veces ¿es mejor callar? La identificación de los usuarios, obligados legalmente a darse de alta con datos reales, nos tendría que hacer reflexionar sobre la *capacidad potencialmente lesionadora de lo que podemos decir de los demás*. También el derecho a la intimidad puede ser fácilmente vulnerable, si ponemos informaciones sobre personas que después pueden ser reenviadas a terceros, y de forma especial deberíamos ser respetuosos con la imagen de los demás, como puede pasar si colgamos fotos con amigos en el Facebook o Twitter. Eso aun puede ser más grave si aparecen menores. Llegado el caso debemos buscar el consentimiento de sus representantes legales. Todos estos derechos son objeto de protección por la vía penal o por la vía civil. También hay que evitar y perseguir todo tipo de amenazas y coacciones a terceros, que, como es obvio, constituyen delitos. Ahora bien, las redes sociales ofrecen la posibilidad de denunciar conductas abusivas, ilegales y contrarias a las condiciones de uso. La libertad de expresión tiene que ser modulada y ponderada con el ejercicio de los derechos que estamos comentando, de acuerdo con el art. 20 CE.[14]

Igualmente hay que proteger la propiedad intelectual, los derechos de autor, porque no podemos aceptar que el mundo de Internet y menos lo que funciona en ámbitos «cerrados» como las redes sociales sean «libres», como la selva. Las plataformas ponen al alcance de los usuarios mecanismos de denuncia. Aun así, la capacidad para «copiar» contenidos, imágenes o vídeos es altísima y difícilmente controlable en su totalidad, y todavía menos cuando se hacen trucajes o modificaciones sin permiso de los autores. Es fácil ser «creativo» y tomar ideas de otros para reenviarlas reelaboradas. Lo mismo pasa con el respeto a la propiedad industrial, de marcas o logos. En todos los casos, si la vía preventiva no funciona, habrá que atender a la responsabilidad penal o civil de las personas que produzcan acciones lesivas.

Otro punto de colisión con el ordenamiento jurídico y que comporta una conducta de un desvalor importante en términos también de civismo en el uso de las

14. «Difundir por redes sociales información privada puede ser delito» [en línea]. *La Vanguardia.com*, 30 de noviembre de 2012. <http://www.lavanguardia.com/Internet/20121130/54355958465/difundir-redes-sociales-informacion-privada-delito.html>.

redes sociales es la vulneración de la privacidad y de los datos personales, como vamos insistiendo en estas líneas, en casos donde *no se respeta el necesario consentimiento previo de los afectados* o, más grave aun, recopilar datos de forma engañosa, conductas consideradas como graves y muy graves por la Ley orgánica 5/1999 de protección de datos de carácter personal. También tenemos el robo de datos personales, la suplantación de la identidad digital y en general conductas ilícitas que suponen una gran molestia y perjuicio a terceras personas. Por otra parte, los *hackers* utilizan conocimientos técnicos para robar contraseñas, crear perfiles falsos, secuestrar la cuenta de usuario en definitiva, todo con el fin de hacer fechorías. Incluso la consulta de un enlace en un tuit, al mostrarse de forma tan breve y diferente del original, puede provocar un engaño.

Las redes sociales permiten cada vez más lo que se ha denominado la *extimidad.*[15] Hoy parece que no existe ni pizca de pudor en explicar cualquier aspecto de la vida privada, como una especie de *reality show*, con el peligro de un exceso de confianza para con los «amigos», que quizás no siempre lo son. La vida se desarrolla, así, en una especie de «casa de cristal» donde es fácil rastrear y conocer mediante nuestras huellas muchos aspectos de la vida más íntima (vida amorosa, ocio personal y tal vez excesos que pueden cometerse, incluso acciones delictivas en potencia, como colgar fotos o vídeos comprometidos).[16] El concepto de «vida privada» se ha transformado en parte, cuando menos, por las propias conductas de los usuarios en las redes sociales, tanto en relación con ellos mismos como ante terceras personas.[17]

Últimamente ha habido casos que han hecho saltar las alarmas por una actuación «viral».[18] El caso del robo y la difusión de teléfonos de la agenda del periodista Pipi Estrada. El hecho de retuitear unos datos privados puede ser un delito de revelación de secretos del art. 197 CP en condición de cooperador necesario o cómplice. Y las víctimas han sido no sólo el periodista sino las personas afectadas por la revelación de su número de teléfono. Otro caso conocido ha sido el de la presentadora de televisión Paula Vázquez,[19] al difundir por Twitter su teléfono y después, al no poder parar las llamadas, distribuir los teléfonos de los «acosadores», en una especie de espiral sin fin. Por otra parte, en el Reino Unido miles de

15. Véase, M. Garmendia: «Internet impulsa el exhibicionismo». *La Vanguardia.com*, 23 de junio de 2013, p. 34. Éste es un concepto creado por el psicoanalista Lacan y que hoy se ha puesto de relieve por P. Sibina, en *La intimidad como espectáculo*, FCE, México, 2008.

16. El caso de Olvido Hormigos es el más claro. Se trataba de la difusión sin consentimiento de un vídeo íntimo. La persona afectada ganó notoriedad. Consultar *El Huffington Post* [en línea] de 6 de septiembre de 2012: <http://www.huffingtonpost.es/2012/09/06/video-concejal-psoe-alcaldia_n_1860262.html>, o del 11 de octubre de 2012: <http://www.huffingtonpost.es/2012/10/11/olvido-hormigos-dice-que-_n_1957742.html>.

17. M. Wieviorka, «Secreto, seguridad y vida privada», *La Vanguardia*, 21 junio de 2013, p. 21.

18. «Difundir por redes sociales información privada puede ser delito» [en línea]. *La Vanguardia.com*, 30 de noviembre de 2012. <http://www.lavanguardia.com/Internet/20121130/54355958465/difundir-redes-sociales-informacion-privada-delito.html>.

19. «Paula Vázquez desencadena una crisis en su perfil de Twitter tras publicar su número de teléfono» [en línea]. *La Vanguardia.com*, 22 de octubre de 2012. <http://www.lavanguardia.com/Internet/20121022/54353796828/twitter-crisis-paula-vazquez.html>.

tuiteros han sido acusados de difamadores por retuitear mensajes[20] que acusaban de abuso de menores a un político retirado. En todo caso, en términos jurídicos, se ha empezado a reconocer que una red social es un medio adecuado para rectificar una información falsa, por orden judicial,[21] y Facebook se considera un medio de prueba válido en juicios.[22]

Pero como venimos diciendo, no todo son peligros y actos ilícitos, que hay que integrar en la cultura del ciberespacio. Existen redes sociales, como la plataforma Linkedin, especializadas en las relaciones profesionales y empresariales. Se puede propiciar un trabajo cooperativo, promocionar las propias actividades a modo de marketing en línea, entrar en contacto con nuevos empleados potenciales, generar datos reputacionales en definitiva. Como elemento destacable, en el sector empresarial, me parece interesante la capacidad para poner en común la responsabilidad social corporativa.

La censura es uno de los grandes peligros del mundo de las redes sociales. La censura es incompatible con la sociedad democrática que las redes sociales tienen que poder desarrollar, de cara a construir una democracia más deliberativa. Algunos gobiernos han censurado redes —por no decir gran cantidad de páginas web— como China, por ejemplo. Pero hay que tener en cuenta también la improcedencia de la presencia organizada de grupos (neonazis, jihadistas, mafias, etc.) que pretenden captar adeptos e incluso hacer apología de actividades criminales terroristas.

Las redes sociales se han erigido como escenario del ejercicio de los derechos sociales, como es el derecho a la educación, el derecho al trabajo (teletrabajo), y son una vía sostenible del mantenimiento de los estándares de derechos, cuando falla la presencialidad por su coste elevado. El trabajo cooperativo, en grupos, es una gran aportación de las redes sociales al mundo de la cultura, que no hay que olvidar. El futuro, cada vez más, se desarrollará mediante plataformas, campus virtuales, redes sociales y por lo tanto escenarios virtuales, dónde se tendrá muy en cuenta el espíritu emprendedor, la motivación y la construcción de una ciudadanía activa (basada en competencias y habilidades transversales). En el otro lado de la balanza, se han dado casos en que, para dar un trabajo, el empresario consulta antes el perfil de Facebook de una persona, y se ha rescindido el contrato de trabajadores que consultan redes sociales en la empresa.

Las redes sociales tienen que garantizar al máximo no tan sólo la seguridad sino el pleno desarrollo de los derechos de las personas y ayudar a aumentar la confianza en las TIC. Es necesario hacer pedagogía en positivo, sin miedos, y reconocer que como en todas las áreas de la vida se puede hacer un mal uso y que

20. «Miles de tuiteros acusados de difamación por rebotar rumores en la red» [en línea]. *El País*, 22 de noviembre de 2012. <http://sociedad.elpais.com/sociedad/2012/11/22/actualidad/1353599720_847000.html>.

21. «El derecho de rectificación se extiende a las redes sociales» [en línea]. Expansión.com, 18 de junio de 2013. <http://www.expansion.com/2012/11/23/juridico/1353693916.html>. El juzgado de primera instancia de Pamplona obliga a publicar la decisión en Twitter, en ejercicio del derecho de rectificación.

22. «El derecho a la intimidad se redefine en Internet» [en línea]. *Expansión.com*, 12 de abril de 2012. <http://www.expansion.com/2009/04/12/juridico/1239560180.html>.

entonces cabría aplicar con contundencia la ley. Pero hoy debemos reconocer que las redes sociales son un buen instrumento de ayuda a las personas y así lo ha entendido la policía, los bomberos, protección civil, los servicios sociales de los ayuntamientos… que las utilizan. También es un gran bazar de información: el seguimiento de las redes te permite estar informado de la actualidad, en un proceso de retroalimentación entre actores públicos y privados de gran trascendencia social. Por otra parte, permite un reencuentro con personas y una socialización masiva si así se desea, incluso localizando a personas en tiempo real según las últimas aplicaciones. El uso en los ámbitos educativo, comercial, político, etc. conforma uno de los fenómenos sociológicos más trascendentales de nuestros días.

En el marco del *discurso positivo y constructivo,*[23] siempre acompañado de la reflexión jurídica, destacan las buenas prácticas, porque hay que dar un paso adelante en la argumentación y no dejarnos llevar por el discurso del miedo y los peligros. Está claro que hay muchos peligros. Pero para progresar hay que fijar medidas efectivas para luchar contra los malhechores de todo tipo. También hay que mejorar el control sobre unas empresas privadas que si bien desarrollan una función social, su principal objetivo es económico o mercantil.[24] Y especialmente el gran problema es el carácter globalizado de unas actuaciones que habría que ordenar también desde una política global —se intenta a nivel europeo, con la nueva propuesta de reglamento de protección de datos de la Unión Europea,[25] pero los Estados todavía no aceptan unos estándares de conducta únicos; y a veces ellos mismos son los primeros interesados en esta diversidad.

En el contexto de la argumentación positiva, hay que recomendar a los usuarios que se lean las *condiciones de uso* de las redes y, en especial, la política de privacidad, y que una vez en su interior hagan un uso seguro y responsable, sin exponerse a actuaciones abusivas ni lesivas de los derechos de terceros. El problema es la interpretación de casos concretos, como podemos ver en las *Directrices de la comunidad YouTube*,[26] aunque adoptar las buenas prácticas ayuda mucho. A grandes rasgos, destaco algunas de las directrices que establece el equipo de YouTube:

— respeto a todo el mundo y uso adecuado;
— nivel de confianza;

23. Touriño, A. «Escribir en Internet: Guía jurídica para los nuevos medios y las redes sociales». ***Actualidad.*** Abogacía Española, 2 de octubre de 2012 [en línea] <http://www.abogacia.es/2012/10/02/escribir-en-Internet-guia-juridica-para-los-nuevos-medios-y-las-redes-sociales/>.

24. «El peligro del SaaS para la libertad de expresión». *La Pastilla Encarnada*, 30 de septiembre de 2012 [en línea] <http://lapastillaroja.net/2012/09/peligro-saas-para-libertad-expresion/>.

25. Véase por ejemplo: «España apoya el Reglamento europeo de protección de datos ante el rechazo de algunos Estados miembros» [en línea]. *DiarioJurídico.com*, 7 de junio de 2013. <http://www.diariojuridico.com/actualidad/noticias/espana-apoya-el-reglamento-europeo-de-proteccion-de-datos-ante-el-rechazo-de-algunos-estados-miembros.html>. Y también: «¿Qué novedades y requerimientos establece el nuevo Reglamento Europeo de Protección de Datos»? [en línea]. *Expansión.com*, 20 de junio de 2013, <http://www.expansion.com/2013/06/20/empresas/tmt/1371710142.html>. Se prevé una regulación uniforme de ámbito europeo del derecho de la privacidad.

26. Pueden consultarse las *Directrices de la comunidad YouTube*, completas, en <http://www.youtube.com/t/community_guidelines?gl=ES&hl=es>.

— revisión de los vídeos marcados como inadecuados;
— las infracciones de las condiciones de uso pueden provocar una notificación de advertencia o la cancelación de la cuenta;
— no cruzar la línea de las reglas del sentido común: YT no está pensado para mostrar pornografía ni contenido sexualmente explícito, ni para mostrar cosas crueles como maltrato de animales, consumo de drogas o fabricación de bombas; no se permite la violencia gráfica o gratuita; no es un lugar de conmociones; hay que respetar los derechos de autor; no se admite la incitación al odio; tolerancia cero con los comportamientos depredadores, acosos, amenazas, hostilidades, invasión de la privacidad o revelación de datos personales de otros miembros; no hacer acciones que confundan y comporten correo basura;
— se recuerda al usuario que YT es su comunidad y que cada uno de ellos hace que este lugar sea el que es.

Figura 1. Imagen de la página web de *Directrices de la comunidad YouTube*

4. REFLEXIÓN FINAL

En este trabajo he querido destacar que las redes sociales están ya para quedarse y, por lo tanto, necesitamos unas reglas claras de buen uso. Este buen uso no debe limitarse a no vulnerar la ley (protección de datos, privacidad, derechos al honor, a la intimidad y a la propia imagen, etc.) sino que tiene que ir más allá. Las buenas prácticas suponen asumir el civismo como concepto que implica el respeto a los demás, la pertenencia a una comunidad virtual y una buena educación. La responsabilidad social de la persona se expresa también en las redes sociales y en Internet, en el mundo entendido como una totalidad.

Ante el discurso del miedo, los peligros y las incertidumbres, necesitamos seguridades, visiones constructivas de las acciones humanas. La calidad del uso de las redes sociales es una muestra de la calidad humana y, por extensión, de la ca-

lidad del país. Un país educado, con personas que saben lo que se hacen es un país admirable y al que aspiramos. No renunciemos a poner el listón lo más alto posible. Ésa tendría que ser nuestra esperanza.

REFERENCIAS

CASTELLS, M. *Redes de indignación y esperanza.* Madrid: Alianza, 2012.
GUERRERO FUERTES, Diego. *Fraude en la red*. Madrid: Ra-Ma, 2010.
— *Facebook. Guía rápida*. Madrid: Star Book, 2011.