INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online

Edición: Febrero 2009

ÍNDICE

RESUMEN EJECUTIVO

I Situación: definición de las redes sociales

- Las redes sociales online son servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado.

- El modelo de crecimiento de estas plataformas se basa fundamentalmente en un *proceso viral*, en el que un número inicial de participantes, mediante el envío de invitaciones a través de correos a sus conocidos, ofrece la posibilidad de unirse al sitio web.

- Estos nuevos servicios se configuran como poderosos canales de comunicación e interacción, que permiten a los usuarios actuar como grupos segmentados: ocio, comunicación, profesionalización, etc.

- Uno de los principales objetivos de la red social se alcanza en el momento en el que sus miembros utilizan el medio online para convocar actos y acciones que tengan efectos en el mundo offline.

- A nivel mundial, las últimas estadísticas (3ª Oleada del Estudio *Power to the people social media, Wave 3* de Universal McCann de marzo 2008) cifran el número de usuarios de redes sociales en 272 millones, un 58% de los usuarios de Internet registrados en todo el mundo, lo que supone un incremento del 21% respecto de los datos registrados en junio de 2007.

- En España, las fuentes estadísticas son diversas, pero todas coinciden que en 2008 el número de usuarios españoles de Internet que utiliza habitualmente redes sociales se sitúa entre el 40% y el 50%[1]. Dando la cifra de una fuente concreta, tomaremos la que ofrece el estudio anteriormente citado: el 44,6% de los internautas españoles tiene un perfil en alguna red social.

- Además, se constata que el porcentaje de usuarios de redes sociales es más alto entre los más jóvenes y decrece con la edad: 7 de cada 10 son internautas menores de 35 años.

[1] Por ejemplo, un 50 % según Zed Digital (El fenómeno de las redes sociales. Percepción, usos y publicidad. Noviembre 2008) o un 45 %, según The Cocktail Analysis (Observatorio de evaluación de redes sociales: Herramientas de comunicación on-line: Las Redes Sociales. Noviembre 2008).

II Análisis de los aspectos más relevantes y problemática específica de las redes sociales

La notoriedad de estos espacios sociales online no queda exenta de riesgos o posibles ataques malintencionados. Es una preocupación de las organizaciones nacionales, europeas e internacionales con competencias en las materias afectadas por el uso de estas redes, que han impulsado la elaboración de normas y recomendaciones[2] dirigidas a garantizar el acceso seguro de los usuarios –con especial atención a colectivos de menores e incapaces -a estas nuevas posibilidades online.

Partiendo de esas premisas, este capítulo ofrece un **análisis en profundidad sobre las cuestiones jurídicas más relevantes que afectan directamente a las redes sociales**:

Protección del honor, la intimidad personal y familiar y la propia imagen de los usuarios

El **derecho al honor** es aquel que tiene toda persona a su buena imagen, nombre y reputación, de tal forma que toda persona puede exigir que se respete su esfera personal, con independencia de las circunstancias particulares, siendo un derecho irrenunciable. El **derecho a la intimidad** tiene por objeto la protección de la esfera más íntima de la persona, y se encuentra íntimamente ligado a la protección de la dignidad del individuo. Por último, el **derecho a la propia imagen** pretende salvaguardar un ámbito propio y reservado del individuo, aunque no íntimo, frente a la acción y conocimiento de los demás.

En España, la protección de estos derechos se encuentra amparada en 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***, donde el legislador español desarrolla la disposición constitucional recogida en el artículo 18.1 CE. Sin embargo, no se regulan de forma expresa determinadas situaciones que pueden llegar a derivarse del uso de las redes sociales y sitios webs colaborativos, lo que unido a la rápida evolución de los

[2] Las principales iniciativas regulatorias provienen del plano internacional, especialmente de la Comisión Europea y del Grupo de Trabajo del Artículo 29, que en los últimos meses ha hecho pública su intención de regular en el menor plazo posible todos los aspectos relacionados con la seguridad y protección de los usuarios de las redes sociales, sitios web colaborativos, blog y demás medios de interacción de usuarios en Internet.

Así, el pasado 15-17 de octubre de 2008, se celebró la 30 Conferencia Internacional de Autoridades de Protección de Datos y privacidad en Estrasburgo. En ella se acordó llevar a cabo una propuesta de regulación normativa de este tipo de plataformas que cumpla con los siguientes requisitos: ser una normativa mundial, legalmente exigible a cualquier tipo de prestador, con independencia de dónde se encuentre ubicado; que dote a los usuarios de una serie de protecciones consideradas básicas a la hora de desarrollar su actividad en la Red; que garantice una protección mínima y básica para los menores, usuarios nativos de este tipo de servicios y especialmente desprotegidos ante éstos, así como que los prestadores establezcan una serie de medidas tecnológicas encaminadas a la protección de los usuarios. De esta forma, el próximo mes de noviembre del año 2009 se celebrará en Madrid, la 31 Conferencia Internacional de Protección de Datos, en la que se propondrá un primer borrador de la regulación mundial en materia de protección de datos, para su posterior debate y aprobación a nivel internacional.

servicios de la Sociedad de la Información, lo que puede conllevar situaciones que pongan en entredicho la defensa de los derechos de los usuarios, a la hora de hacer efectiva la aplicación normativa. Entre las **posibles situaciones de riesgo para la protección de la intimidad**, cabe señalar:

- En el *momento del registro de alta como usuario*, en la medida en que no sea configurado correctamente el nivel de privacidad del perfil, así como por el hecho de que sea publicada información sensible desde el inicio de la actividad en la red.

- En el *momento de participación en la red como usuario*, en la medida en que el grado de información, datos e imágenes publicados pueden ser excesivos y afectar a la privacidad, tanto personal como de terceros.

    - Por lo que respecta a la privacidad personal: a pesar de que sean los usuarios los que voluntariamente publican sus datos, los efectos sobre la privacidad pueden tener un alcance mayor al que consideran en un primer momento ya que estas plataformas disponen de potentes herramientas de intercambio de información, la capacidad de procesamiento y el análisis de la información facilitada por los usuarios.

    - Por lo que respecta a la privacidad de terceros: es esencial que los usuarios tengan en cuenta que la publicación de contenidos con información y datos respecto a terceros no puede ser realizada si éstos no han autorizado expresamente su publicación, pudiendo solicitar su retirada de forma inmediata.

  Por último, es importante tener en cuenta que en la gran mayoría de ocasiones, las redes sociales permiten a los motores de búsqueda de Internet indexar en sus búsquedas los perfiles de los usuarios, junto con información de contacto y de perfiles amigos, lo que puede suponer otro riesgo para la protección de la privacidad, además de dificultar el proceso de eliminación de su información en Internet.

- En el *momento de darse de baja de la plataforma* en la medida en que el usuario solicite dar de baja su perfil, pero aún así continúen datos publicados por éste, o información personal e imágenes propias publicadas en los perfiles de otros usuarios.

Además existe en España, desde el punto de vista normativo, una **protección especial para el caso de *menores*,** usuarios masivos de este tipo de servicios online, que les otorga un *estatus de protección más elevado que al resto de usuarios, en la medida en que el consentimiento para la disposición de los derechos requiere de la intervención de sus padres o tutores legales.*

En los últimos años el nivel de concienciación respecto a la protección de derecho a la intimidad y a la protección de datos personales está siendo mucho mayor. Prueba de ello, es la publicación de la **Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE)** al considerar la nueva realidad social que ha supuesto el uso de las TIC, en general, e Internet, en particular y disponer las bases normativas para una regulación de Internet y sus servicios, de manera completa, íntegra y efectiva.

Sin embargo, y como se recoge en el Estudio, la adecuación práctica al rápido desarrollo de los nuevos servicios que conlleva la Sociedad de la Información, entre los que se encuentran las redes sociales, provoca situaciones complejas para la aplicación e interpretación práctica de las normativa. Por ello, *se hace necesario emprender y desarrollar "tecnología jurídica", tomando como base actividades de I+D+i, que garantice la protección de los usuarios sin que ello suponga un obstáculo para el desarrollo de este tipo de servicios*.

Protección de datos de carácter personal

Este **derecho fundamental a la protección de datos, regulado específicamente en el artículo 18.4 de la Constitución**, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley. De esta forma, supone el "derecho a controlar el uso que se realice de sus datos personales, comprendiendo, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención"[3].

Dada la gran cantidad de datos personales que los usuarios publican en sus perfiles, éstos se convierten en auténticas "*identidades digitales*" que facilitan un rápido conocimiento de datos de contacto, preferencias y hábitos del usuario.

La protección de datos de carácter personal es un derecho ampliamente desarrollado legislativamente en el ámbito comunitario y nacional. En España, su regulación se lleva a cabo mediante **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y por Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos**

[3] Extracto de la Sentencia del Tribunal Constitucional 292/2000 donde se reconoce el Derecho a la Protección de Datos, como un derecho fundamental absolutamente independiente del Derecho al Honor, Intimidad y Propia Imagen, otorgando así a la protección de datos de carácter personal, una entidad absolutamente independiente del resto de derechos.

(RDLOPD) y además existe un amplio desarrollo interpretativo por parte de la Agencia Española de Protección de Datos (AEPD), que mediante sus resoluciones ha dado respuesta a casos de vulneración de derechos de protección de datos derivados del uso de los nuevos servicios que ofrece la Sociedad de la Información lo que permite a los usuarios contar con la máxima garantía en la protección de sus derechos personales.

No obstante, tal y como se ha constatado durante las entrevistas y los grupos de trabajo realizados, es en materia de protección de datos donde acontece el mayor número de situaciones desfavorables para la protección de los derechos de los usuarios, ya que las redes sociales fundamentan todos sus contenidos en los perfiles que los propios usuarios dan de alta y actualizan con asiduidad. Así, entre las **posibles situaciones de riesgo para la protección de datos de carácter personal**, y sin perjuicio de las situaciones citadas anteriormente por su relación con el derecho a la intimidad se encuentran:

- Casos de *phishing* y *pharming*. Ambos fenómenos, muy explotados por los ciberdelincuentes para lograr la obtención de datos personales de los usuarios de Internet, así como de datos de carácter sensible o relativos a aspectos económicos (tarjetas de crédito, PIN de usuarios, etcétera).

- *Social Spammer y spam*. El uso de las redes sociales como plataformas para el envío de correos electrónicos no deseados.

- *Indexación no autorizada por parte de buscadores de Internet*.

- *Acceso al perfil incontrolado*. La mayoría de redes sociales analizadas disponen del perfil completo del usuario, o al menos de parte de este, en formato público, de forma que cualquier usuario de Internet o de la red social puede acceder a información de carácter personal ajena sin que el propietario de los datos tenga que dar su consentimiento expreso.

- *Suplantación de identidad*. Cada vez es más frecuente que usuarios que nunca se habían registrado en redes sociales online, comprueben como en el momento en el que intentan acceder, su "identidad digital", ya está siendo utilizada.

- *Publicidad hipercontextualizada*. Esta aporta, a priori, una ventaja para los usuarios, ya que con ella evitan que se muestren durante su navegación contenidos, para ellos, irrelevantes e incluso ofensivos. Sin embargo, desde el punto de vista legal podría considerarse una práctica ilegal, ya que para poder contextualizar la publicidad que se va a mostrar a un usuario se tienen que examinar sus datos y preferencias.

- *La instalación y uso de "cookies" sin conocimiento del usuario*. Otro posible riesgo relacionado con la participación del usuario en la red social radica en la posibilidad

de que el sitio web utilice cookies que permitan a la plataforma conocer cuál es la actividad del usuario dentro de la misma. Mediante estas herramientas, las redes sociales pueden conocer el lugar desde el que el usuario accede, el tiempo de conexión, el dispositivo desde el que accede (fijo o móvil), el sistema operativo utilizado, los sitios más visitados dentro de una página web, el número de clicks realizados, e infinidad de datos respecto al desarrollo de la vida del usuario dentro de la red.

Por lo que respecta a las *medidas existentes en materia de protección de datos personales de especial protección para colectivos considerados especialmente vulnerables –menores e incapaces-* , cabe señalar que desde el punto de vista normativo, tiene una especial importancia la aprobación del Real Decreto 1720/2007 que introduce una importante especialidad en lo que respecta a la prestación del consentimiento por parte de estos menores al disponer que para recabar los datos de cualquier menor de 14 años es necesario contar con el consentimiento de los padres o tutores.

Además, esta norma señala de manera expresa que para recabar el consentimiento del menor debe utilizarse un lenguaje sencillo y fácilmente comprensible para él y que no se podrá obtener a partir de ellos información respecto a sus familiares y allegados.

Protección de la propiedad intelectual e industrial de los contenidos

Por lo que respecta a la protección de la propiedad intelectual en este tipo de plataformas, se está produciendo un aumento en el número de contenidos protegidos por el derecho de propiedad intelectual que están siendo utilizados, compartidos y difundidos a través de las redes sociales y sitios web colaborativos.

La protección se centra, por tanto, en el **derecho que el autor tiene sobre su creación literaria, artística o científica**.

En España, la **Ley de Propiedad Intelectual** concede a los *autores de las obras derechos en exclusiva sobre éstas, lo que supone que cualquier tratamiento, reproducción, puesta a disposición o transmisión de la obra deberá ser realizada con la autorización de los titulares de derechos*. Tanto la normativa nacional, como la comunitaria, parten de un grado elevado de restricción de los derechos de explotación, de forma que *nadie puede explotar derechos de propiedad intelectual sin autorización por parte del autor*.

No obstante, dentro de las posibles vulneraciones de derechos en materia de propiedad intelectual e industrial, y tal y como se ha extraído de las entrevistas y de los grupos de trabajo para analizar los aspectos jurídicos, es necesario diferenciar entre aquellas situaciones en las que son los propios usuarios los que ponen en entredicho la integridad y derechos de propiedad intelectual de los autores y, aquellas en las que son las redes

sociales las que, a través de sus condiciones generales ponen en riesgo los derechos de propiedad intelectual de los usuarios.

Ante estas situaciones, las redes sociales, como medio de colaboración y lucha contra la distribución no autorizada de contenidos a través de sus plataformas, han dispuesto mecanismos automáticos para que los propios usuarios procedan a la autorregulación de los contenidos que desean que existan en la red social. Para ello, se permite *"denunciar" internamente contenidos* que no cumplan con las condiciones de registro de la plataforma o que atenten tanto contra los derechos que ostentan los usuarios sobre sus obras de propiedad intelectual, como contra los de terceros.

Protección de los consumidores y usuarios

Se ha de tener en cuenta que una de las principales ventajas que presenta este tipo de plataformas es la capacidad de obtener beneficios económicos derivados de la publicidad y de las aplicaciones internas desarrolladas por los propios usuarios de la red.
La facilidad con la que los usuarios pueden anunciar o ser receptores de anuncios de productos y servicios es muy elevada si se compara con el mundo físico, ya que junto a la sencillez con la que se pueden comercializar productos y servicios a distancia, las redes sociales cuentan con una base de datos de usuarios (potenciales clientes), perfectamente segmentados por gustos y perfiles, lo que implica que las capacidades de éxito del procedimiento comercial sean muy altas.

Según se ha constatado a partir de las entrevistas y los grupos de trabajo realizados con usuarios y juristas, el aumento de la colaboración de los usuarios a la hora de detectar y controlar el tipo de publicidad, así como los productos y servicios comercializados a través de la red, permitiría una autorregulación interna de la plataforma desde el punto de vista comercial, que aumentaría el grado de seguridad de los usuarios.

Del mismo modo, es esencial para un correcto desarrollo de la Sociedad de la Información y por tanto para que la venta de productos y servicios a través de redes sociales sea exitosa, que los potenciales clientes confíen plenamente en el sitio web, para lo que éste deberá garantizar a todos los potenciales clientes que observa y cumple la normativa legal vigente, así como los requisitos tecnológicos necesarios.

III Propuestas y recomendaciones de actuación dirigidas a los agentes intervinientes en las redes sociales

Tras el análisis de la información recabada durante la investigación cualitativa –redes sociales y plataformas colaborativas, servicios ISP o proveedores de acceso a Internet, fabricantes y proveedores de servicios de seguridad informática, administraciones e instituciones públicas y usuarios y asociaciones– se formulan una serie de recomendaciones a los diferentes agentes intervinientes en el proceso:

- **Dirigidas a la industria**

Redes sociales y plataformas colaborativas: La propuesta de *recomendaciones de carácter general* dirigida a este colectivo está enfocada: a la adecuación de sus servicios respecto de la normativa europea y nacional, al conocimiento de las implicaciones jurídico tecnológicas que conlleva la realización de determinadas prácticas, a la identificación del tipo de herramientas tecnológicas necesarias en sus servicios, y a aumentar el grado de concienciación respecto de la necesidad de incrementar las medidas de seguridad y protección de los usuarios.

Por lo que respecta a las *recomendaciones específicas* extraídas de las entrevistas y de los grupos de trabajo, cabe señalar:

Recomendaciones tecnológicas y de seguridad

1. Transparencia y facilidad de acceso a la información

    - Resulta fundamental que este tipo de plataformas expongan toda la información relativa a sus servicios de forma clara y comprensible, de manera que el lenguaje empleado en sus condiciones de uso y políticas de privacidad sea absolutamente comprensible para cualquier tipo de usuario.

    - Es esencial que las redes sociales destaquen dentro de sus páginas de inicio un apartado específico destinado a informar a los usuarios.

    - Se recomienda la creación de "microsites"[4] con acceso directo desde la página principal de la red social, en los que se exponga información mediante "preguntas frecuentes" y contenidos multimedia.

    - Es esencial que las redes sociales mantengan su política de privacidad y condiciones de uso sin cambios importantes y trascendentales para los usuarios.

2. Garantizar a los usuarios el control absoluto del tratamiento de sus datos e información publicada en la red poniendo a su disposición el mayor número de herramientas tecnológicas, encaminadas a hacer efectivos sus derechos de forma automática, sencilla y rápida.

3. Establecer, por defecto, estándares de seguridad y privacidad, referidos a la no indexación por defecto de los datos personales o a la especial protección de los datos sensibles.

[4] Pequeñas páginas web, con contenidos específicos que dependen de una principal.

4. Garantizar la seguridad tecnológica de la plataforma. En este sentido, es vital la correcta elección por parte de la plataforma, de un prestador de servicios de Internet (Internet Service Provider o ISP) que cuente con un elevado nivel de seguridad: servidores seguros, centros de respaldo y accesos seguros, entre otras medidas.

5. Eliminación de la información después de un tiempo prudencial sin que el usuario haya entrado en la plataforma.

6. Respetar los derechos de acceso y cancelación.

Recomendaciones en materia de formación y concienciación

1. Desarrollo interno de espacios web dedicados a poner a disposición de los usuarios el máximo y más claro posible nivel de información posible respecto al tratamiento de datos personales, los sistemas publicitarios empleados en la plataforma, las situaciones de riesgo a las que se pueden enfrentar derivadas del uso de este tipo de servicios online, así como de las implicaciones que pueden derivarse de la publicación de contenidos en la red social.

2. Puesta a disposición de los usuarios de información relativa a las medidas de seguridad que la plataforma ha implementado para actuar en caso de que se produzca la vulneración de alguno de sus derechos.

3. Teniendo en cuenta que la gran mayoría de usuarios de las redes sociales generalistas son menores de edad, resulta fundamental que las redes sociales y plataformas colaborativas, junto con las autoridades públicas, asociaciones y organizaciones cuya finalidad sea la protección de este tipo de colectivos, lleven a cabo iniciativas conjuntas encaminadas a fomentar la formación entre los menores y tutores respecto a la seguridad de los usuarios, investigando las posibilidades tecnológicas existentes para lograr la identificación de la edad de los usuarios del servicio.

4. Programas de voluntariado dentro de la empresa para colaborar con las instituciones escolares y centros de formación con el fin de difundir la importancia de la seguridad, así como para informar sobre las principales recomendaciones a tener en cuenta en el uso de este tipo de servicios.

Dirigidas a fabricantes y proveedores de servicios de seguridad informática

Los fabricantes y proveedores de seguridad deben tener en cuenta dos aspectos clave para lograr el máximo nivel de seguridad: a) *la prevención del fraude online* y b) la investigación y desarrollo en materia de seguridad tecnológica. De esta forma, se recomienda que fomenten en el sector los siguientes aspectos:

1. Que las aplicaciones comercializadas entre las redes sociales y plataformas colaborativas, así como entre los usuarios, hayan sido desarrolladas, revisadas y evaluadas conforme a estándares de calidad y seguridad que garanticen que su utilización es segura y respetuosa con los derechos de los usuarios.

2. El fomento de la interoperabilidad de sus sistemas de seguridad.

3. La colaboración activa y directa con las Fuerzas y Cuerpos de Seguridad del Estado en la investigación de nuevas situaciones de riesgo para los usuarios.

4. La proactividad en la detección de códigos maliciosos de programación que permitan agujeros de seguridad en las plataformas, así como la elaboración de listados (“Black Listed”), en los que sean incluidos todos los nombres de dominio que cuenten con contenidos no autorizados, o en su caso, que no superen los criterios de seguridad previamente establecidos.

5. El desarrollo de parches de seguridad y actualizaciones.

6. El desarrollo de aplicaciones remotas que permitan el control pleno por parte de los tutores de los contenidos y de las operaciones realizadas por los menores a través de Internet.

7. El desarrollo de aplicaciones que permitan a las plataformas controlar la edad de los usuarios que intentan acceder al servicio.

8. Incluir en la descripción técnica de los productos de software destinados al tratamiento de datos personales la descripción técnica del nivel de seguridad, básico, medio o alto que permitan alcanzar de acuerdo con el Reglamento de desarrollo de la LOPD.

9. Igualmente, se recomienda que los fabricantes de aplicaciones software de seguridad, junto con las administraciones públicas competentes, fomenten el desarrollo de herramientas encaminadas a reducir la recepción de correos electrónicos no deseados (spam) a través de redes sociales y plataformas semejantes.

Dirigidas a los prestadores de servicios de acceso a Internet (ISP)

La propuesta de recomendaciones dirigidas a este colectivo incluye:

1. La creación de plataformas de comunicación fehaciente y segura con las Fuerzas y Cuerpos de Seguridad del Estado, Ministerio Fiscal y Autoridades Judiciales.

2. El apoyo y asistencia plena a las Fuerzas y Cuerpos de Seguridad del Estado.

3. Prestar información a todos los usuarios y clientes directos sobre las medidas de seguridad que mantienen respecto al servicio concreto.

4. Atender inmediatamente las reclamaciones de bloqueo de servicios cuando se reciban por cualquier método que deje constancia de la identidad del remitente y se identifique de forma clara y concisa el emisor del mismo.

Dirigidas a las administraciones e instituciones públicas

Como garantes de los derechos de los ciudadanos las recomendaciones que se proponen a las autoridades se catalogan desde el:

Punto de vista normativo:

Por lo que respecta a la *protección de datos personales,* entre las propuestas cabe citar:

- Las autoridades competentes deben promover la elaboración de informes, recomendaciones y dictámenes públicos.

- Seguridad jurídica global: que se fomente el establecimiento internacional, al menos a nivel comunitario, de los principios normativos básicos.

- Deberán instrumentarse y reforzarse las sanciones para aquellas plataformas o usuarios que compartan u obtengan información de forma ilegal.

- Se recomienda a las autoridades trabajar en favor de un derecho internacional homogéneo en materia de protección de datos personales, honor, intimidad y propia imagen

Propiedad Intelectual:

- Fomentar, y en su caso disponer como obligatorio, que este tipo de plataformas hagan públicas y destaquen con especial énfasis que dichos contenidos pasarán a ser propiedad de la plataforma.

- Se recomienda que las autoridades competentes promocionen, desde el punto de vista normativo, acuerdos directos entre la industria audiovisual y musical, y las grandes plataformas de difusión de contenidos.

- Se recomienda la obligación de todo prestador de servicios de la Sociedad de la Información a que dispongan de medios automatizados, gratuitos, sencillos y eficaces para que los titulares de obras de propiedad intelectual puedan denunciar la retirada de contenidos.

- Que se garantice la justa remuneración de los titulares de los derechos.

Consumidores y Usuarios

- Se recomienda al legislador que se delimite claramente qué autoridad es competente para atender las reclamaciones de los consumidores o usuarios.

- Promover mecanismos eficaces y eficientes respecto a la posibilidad de bloquear el acceso a la plataforma online.

Punto de vista ejecutivo y administrativo:

- Formación específica en Derecho Tecnológico destinada a jueces, magistrados, forenses, fiscales y secretarios judiciales.

- Dotar a las brigadas tecnológicas de las Fuerzas y Cuerpos de seguridad del Estado, tanto estatales y autonómicas, como internacionales, de herramientas tecnológicas que les permitan investigar, mantener la cadena de custodia de las pruebas electrónicas y bloquear situaciones que pudieran ser susceptibles de delitos y/o perjudiciales para los usuarios de redes sociales.

- Desarrollo y articulación de procedimientos judiciales rápidos.

Punto de vista formativo y divulgativo:

- Realizar campañas de concienciación sobre los riesgos de la difusión de datos personales en las redes sociales.

- Llevar a cabo jornadas de formación y programas de difusión relativos a la seguridad.

- Incluir en los planes oficiales de estudio el conocimiento de aspectos relacionados con la seguridad de las tecnologías de la información y la protección de datos personales fomentando la formación específica en este campo.

- Llevar a cabo acciones de sensibilización y fomento de la seguridad en Internet a través de los propios medios 2.0.

Dirigidas a los usuarios y asociaciones

La propuesta de recomendaciones dirigidas a este colectivo se formula con la intención de que puedan conocer todos y cada uno de los beneficios que este tipo de servicios online pueden aportar a sus vidas, pero sin descuidar el conocimiento sobre la existencia de determinadas situaciones desfavorables, que sin embargo pueden ser fácilmente evitables.

Estas propuestas se estructuran atendiendo a la protección de datos personales, honor, intimidad y propia imagen, a la propiedad intelectual, recomendaciones de carácter tecnológico y de seguridad y a la protección de los menores.

1. Se recomienda a todos los usuarios recurrir al uso de seudónimos o nicks personales con los que operar a través de Internet, permitiéndoles disponer de una auténtica "identidad digital", que no ponga en entredicho la seguridad de su vida personal y profesional. De esta forma, únicamente será conocido por su círculo de contactos, que conocen el nick que emplea en Internet.

2. Se recomienda a los usuarios tener especial cuidado a la hora de publicar contenidos audiovisuales y gráficos en sus perfiles, dado que en este caso pueden estar poniendo en riesgo la privacidad e intimidad de personas de su entorno.

3. Se recomienda revisar y leer, tanto en el momento previo al registro de usuario, como posteriormente, las condiciones generales de uso y la política de privacidad que la plataforma pone a su disposición en sus sitios web.

4. Se recomienda configurar adecuadamente el grado de privacidad del perfil de usuario en la red social, de tal forma que éste no sea completamente público, sino que únicamente tengan acceso a la información publicada en el perfil aquellas personas que hayan sido catalogadas como *"amigos"* o *"contactos directos"* previamente por el usuario.

5. Se recomienda aceptar como contacto únicamente a aquellas personas conocidas o con las que mantiene alguna relación previa, no aceptando de forma compulsiva todas las solicitudes de contacto que recibe e investigando siempre que fuera posible y necesario, quién es la persona que solicita su contacto a través de la red social.

6. Se recomienda no publicar en el perfil de usuario información de contacto físico, que permita a cualquier persona conocer dónde vive, dónde trabaja o estudia diariamente o los lugares de ocio que suele frecuentar.

7. A los usuarios de herramientas de *microblogging*[5] se recomienda tener especial cuidado respecto a la publicación de información relativa a los lugares en que se encuentra en todo momento.

8. Se recomienda utilizar y publicar únicamente contenidos respecto a los que se cuente con los derechos de propiedad intelectual suficientes. En caso contrario, el usuario estará cometiendo un ilícito civil protegible por parte de los tribunales nacionales.

9. Se recomienda a los usuarios emplear diferentes nombres de usuario y contraseñas para entrar en las distintas redes sociales de las que sea miembro.

10. Se recomienda utilizar contraseñas con una extensión mínima de 8 caracteres, alfanuméricos y con uso de mayúsculas y minúsculas.

11. Se recomienda a todos los usuarios disponer en sus equipos de software antivirus instalado y debidamente actualizado.

12. Los menores no deben revelar datos personales excesivos. Nunca se deben suministrar los datos a desconocidos.

13. Se debe leer toda la información concerniente a la página web. En ella se explica quiénes son los titulares de la misma y la finalidad para la que se solicitan los datos.

14. Si el usuario es menor de catorce años, se necesita también el consentimiento de los padres o tutores. En estos casos, siempre que se soliciten datos por parte de una red social debe preguntarse a los padres o tutores para ver si ellos aprueban la suscripción o no.

15. No deben comunicarse a terceros los nombres de usuario y contraseña, ni compartirlos entre amigos o compañeros de clase. Estos datos son privados y no deben ser comunicados a terceros y/o desconocidos.

16. Siempre que se tenga cualquier duda respecto a alguna situación que se derive del uso de las redes sociales y herramientas colaborativas, debe preguntarse a los padres o tutores.

[5] Este tipo de plataformas basan su servicio en la actualización constante de los perfiles de usuarios. Más información: Capítulo 3 de este Estudio.

17. Se debe mantener el ordenador en una zona común de la casa.

18. Se deben establecer reglas sobre el uso de Internet en casa.

19. Los padres deben conocer el funcionamiento y las posibilidades de este tipo de plataformas, tanto positivas como negativas.

20. Activar el control parental y las herramientas de control de la plataforma, así como establecer el correo del padre o tutor como correo de contacto secundario.

21. Asegurarse de que los controles de verificación de la edad están implementados.

22. Asegurar la correcta instalación del bloqueador de contenidos.

23. Concienciar e informar a los menores sobre aspectos relativos a la seguridad.

24. Explicar a los menores que nunca han de quedar con personas que hayan conocido en el mundo online y que si lo hacen debe ser siempre en compañía de sus padres o tutores.

25. Asegurarse de que los menores conocen los riesgos e implicaciones de alojar contenidos como vídeos y fotografías, así como el uso de cámaras web a través de las redes sociales.

26. Controlar el perfil de usuario del menor.

27. Asegurarse de que el menor sólo accede a las páginas recomendadas para su edad.

28. Asegurarse de que los menores no utilizan su nombre completo.

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Presentación

1.1.1 Instituto Nacional de Tecnologías de la Comunicación

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), sociedad estatal promovida por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología con un doble objetivo: por una parte, contribuir a la convergencia de España con Europa en la Sociedad de la Información y, de otra parte, promover el desarrollo regional, enraizando en León un proyecto con vocación global.

La misión de INTECO es impulsar y desarrollar proyectos de innovación relacionados con el sector de las Tecnologías de la Información y la Comunicación (TIC) y en general, en el ámbito de la Sociedad de la Información, que mejoren la posición de España y aporten competitividad, extendiendo sus capacidades tanto al entorno europeo como al latinoamericano. Así, el Instituto tiene la vocación de ser un centro de desarrollo de carácter innovador y de interés público a nivel nacional que constituirá una iniciativa enriquecedora y difusora de las nuevas tecnologías en España en clara sintonía con Europa.

El objeto social de INTECO es la gestión, asesoramiento, promoción y difusión de proyectos tecnológicos en el marco de la Sociedad de la Información. Para ello, INTECO desarrollará actuaciones, al menos, en líneas estratégicas de Seguridad Tecnológica, Accesibilidad y Calidad de Software.

El **Observatorio de la Seguridad de la Información** se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica.

El Observatorio tiene por objetivo describir de manera detallada y sistemática el nivel de seguridad y confianza en la Sociedad de la Información y de generar conocimiento especializado en la materia. De este modo, se encuentra al servicio de los ciudadanos, las empresas y las administraciones públicas españolas para describir, analizar, asesorar y difundir la cultura de la Seguridad de la Información y la e-Confianza.

El Observatorio ha diseñado un *Plan de Actividades y Estudios* con el objeto de producir conocimiento especializado y útil en materia de seguridad por parte de INTECO, así como de elaborar recomendaciones y propuestas que definan tendencias válidas para la toma de decisiones futuras por parte de los poderes públicos.

Dentro de este plan de acción se realizan labores de investigación, análisis, estudio, asesoramiento y divulgación que atenderán, entre otras, a las siguientes estrategias:

- Elaboración de estudios e informes propios en materia de seguridad de las Tecnologías de la Información y la Comunicación, con especial énfasis en la Seguridad en Internet.

- Seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la confianza en el ámbito nacional e internacional.

- Generación de una base de datos que permita el análisis y evaluación de la seguridad y la confianza con una perspectiva temporal.

- Impulso de proyectos de investigación en materia de seguridad TIC.

- Difusión de estudios e informes publicados por otras entidades y organismos nacionales e internacionales, así como de información sobre la actualidad nacional y europea en materia de la seguridad y confianza en la Sociedad de la Información.

- Asesoramiento a las Administraciones Públicas en materia de seguridad de la información y confianza, así como el apoyo a la elaboración, seguimiento y evaluación de políticas públicas en este ámbito.

Más información: http://www.inteco.es

Más información: http://observatorio.inteco.es

1.1.2 Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos, es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones, y que tiene por objeto la garantía del cumplimiento y aplicación de las previsiones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y sus normas de desarrollo.

Sus funciones son, en general, velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

Entre sus funciones está también la obligación de atender las peticiones y reclamaciones que puedan ser formuladas por las personas afectadas por esta cuestión y la potestad sancionadora de las infracciones que puedan ser cometidas en la materia, así como la recogida de datos estadísticos e informar los proyectos de normas que incidan en materias de protección de datos, así como dictar instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD y seguridad y control de acceso a los ficheros.

Más información: http://www.agpd.es

1.2 Situación de partida. Contextualización del Estudio

Actualmente Internet se configura como un escenario de relaciones sociales sustentado en la creciente participación de los usuarios. Esta participación proactiva se materializa en:

- La edición, validación y publicación de contenidos en diferentes formatos: texto, audio, video.

- La especialización de contenidos. La participación, se segmenta en una diversidad de portales que van desde la creación de comunidades genéricas, pasando por las específicas de entretenimiento hasta llegar a las de contenido profesional. Además, los usuarios se segmentan entre diversos sitios web en atención a rangos de edad: jóvenes y adolescentes, adultos, etc.

Los cambios tecnológicos y sociales han contribuido a la implantación y crecimiento popular de esta nueva forma de creación, colaboración y acceso a la información.

La tendencia actual de los servicios que la Red pone al alcance del usuario -foros, blogs, wikis o redes sociales- se construye a partir de un nexo común que tiene en su base la *actividad colaborativa*, es decir, todas aquellas utilidades y servicios de Internet que se sustentan en una base de datos, la cual puede ser modificada por los usuarios del servicio, ya sea en su contenido (añadiendo, cambiando o borrando información así como asociando datos a la información existente), o en la forma de presentarlos.

Sin embargo, la notoriedad de estos espacios sociales no queda exenta de peligros o posibles ataques malintencionados. Así:

- Los usuarios facilitan una serie de datos de carácter personal al inscribirse en estos portales que deben ser convenientemente protegidos conforme a la legislación española. Además, la propia naturaleza de estos portales implica que los usuarios incluyan amplia información sobre sus preferencias y necesidades, que también ha de ser protegida, especialmente en el caso de los menores y personas sin capacidad legal de obrar.

  El hecho de que las redes sociales se fundamenten en el *principio de puesta a disposición pública* de la máxima cantidad de información, provoca, tanto de forma directa como indirecta, la aparición de innumerables situaciones jurídicas, novedosas hasta el momento, pero que sin embargo tienen cabida y regulación expresa en la normativa española.

- Algunos de los portales más representativos han sido objetivo de ataques de fraude online. Se han producido situaciones en las que una persona se hace pasar por un amigo confiable o empresa legítima en una red social, con el objeto de conseguir información personal o claves bancarias.

- Es frecuente que los usuarios utilicen la misma contraseña de acceso en su participación como miembros de diferentes comunidades virtuales, lo que implica que un fallo de seguridad en una de estas puede afectar a todos los datos que el usuario haya facilitado en todos los demás portales. La situación se agrava cuando los usuarios utilizan la misma contraseña para gestionar su actividad financiera.

En este contexto, la seguridad de los usuarios y de los sistemas de información, a la vez que la protección y privacidad de los datos de carácter personal, con especial atención en menores y personas sin capacidad de obrar, se configuran como aspectos relevantes de análisis.

Ante esta situación surge la necesidad de realizar un estudio en el que se examine, investigue, y desarrolle la situación de seguridad, naturaleza jurídica y aspectos de carácter social y tecnológicos de las redes sociales que operan en España, con especial atención a su efecto y uso por parte de menores e incapaces.

Asimismo, con este Estudio se dará a conocer el estado de opinión del sector, con la finalidad de orientar futuras iniciativas de carácter privado, así como políticas públicas, dirigidas a lograr el equilibrio entre las posibilidades que ofrecen estas nuevas herramientas de participación colaborativa y los límites y derechos fundamentales de los usuarios.

1.3 Objetivos del Estudio

El **objetivo general** del estudio es la elaboración de un análisis del estado de la seguridad en redes sociales y plataformas análogas, con especial atención a los usuarios menores e incapaces, mediante una evaluación y diagnóstico de carácter jurídico, tecnológico, sociológico y de seguridad de los contenidos, los agentes participantes, así como de la privacidad y la protección de datos de los usuarios que se relacionan a través de estos sitios web.

Este objetivo general se desglosa operativamente en los siguientes **objetivos específicos**:

- Análisis jurídico de las redes sociales para determinar las obligaciones y responsabilidades legales de los prestadores de servicios en España.

- Estudio de derecho comparado de estos portales de encuentro en el ámbito de la Unión Europea y EE.UU. con especial atención a la penetración de las redes sociales en estos países, así como a las iniciativas legislativas y proyectos existentes.

- Análisis de los diferentes agentes que intervienen en las web colaborativas (ISP, agencias de publicidad, agencias de contenidos, etc.) respecto a la legitimidad y responsabilidad de cada uno en el funcionamiento de las mismas.

- Análisis tecnológico y sociológico de las redes sociales donde se describa el funcionamiento de estas nuevas formas de interacción social: flujos de información y herramientas disponibles para publicar información o comunicarse con otros usuarios.

- Análisis de la privacidad y protección de datos de los usuarios y de las personas que se relacionan a través de las redes sociales.

- Análisis de seguridad: evaluación específica de los riesgos que pueden llegar a alcanzar este tipo de portales sociales de encuentro para menores y personas sin capacidad de obrar.

- Análisis del caso especial de menores y personas legalmente incapaces respecto a la protección de los derechos de carácter personal y de protección del honor, la intimidad y la propia imagen.

- Delimitación de las amenazas y riesgos en el uso de este tipo de redes colaborativas. Medidas para buscar un equilibrio entre las posibilidades de estas herramientas, su legitimación y la privacidad y protección de datos de los usuarios y de los titulares de los datos.

Con la consecución de estos objetivos, se pretende facilitar información y recomendaciones de actuación respecto a la situación jurídica, tecnológica y de seguridad en la que se encuentran este tipo de plataformas.

1.4 Diseño metodológico

La metodología empleada para realizar el presente Estudio ha sido configurada con una finalidad última, lograr que su contenido ofrezca información actual y valiosa sobre la situación y visión de los usuarios, agentes del mercado y entidades públicas intervinientes, así como el más riguroso análisis de cada uno de los factores jurídico-tecnológicos que tienen incidencia en las redes sociales y sitios web colaborativos.

Concretamente, el estudio y análisis ha sido elaborado conforme a las siguientes fases:

1.4.1 Fase I. Obtención de información y trabajo de campo

El objetivo de esta fase es la obtención de la máxima cantidad de información posible, respecto al fenómeno de las redes sociales. Para ello se han realizado las siguientes tareas:

1. **Búsqueda documental** de recursos relacionados con las redes sociales

    a) Documentación oficial publicada por la Unión Europea e instituciones internacionales[6].

    b) Informes realizados por entidades privadas.

    c) Fuentes secundarias sobre análisis estadísticos respecto a las redes sociales.

    d) Artículos de opinión y noticias relacionadas.

2. **Identificación de los principales agentes implicados** en el fenómeno de las redes sociales. Análisis específico de las redes sociales que operan en España, determinando su grado de cumplimiento inicial de la normativa nacional, así como sus aspectos prácticos concretos que posteriormente serán tenidos en cuenta ampliamente en el informe.

3. Realización de una **encuesta a 2.860 usuarios de Internet** mayores de 15 años, sobre el uso de las redes sociales entre abril y junio de 2008[7]. Las características del trabajo de campo de dicha encuesta se describen seguidamente:

    - Universo: Usuarios españoles con acceso frecuente a Internet desde el hogar, mayores de 15 años. Para delimitar con mayor precisión el concepto de usuario frecuente, se exige una conexión a Internet desde el hogar de, al menos, una vez al mes.

    - Tamaño y distribución muestral: Se ha extraído una muestra representativa de 2.860 usuarios de Internet, mediante afijación muestral según un modelo polietápico:

        o Estratificación por Comunidades Autónomas para garantizar un mínimo de sujetos en cada una de estas entidades.

[6] Entre otros: Grupo de Trabajo del Artículo 29; European Network and Information Security Agency, Foro de Cooperación Económica Asia Pacífico (APEC), entre otras.

[7] Los datos de los resultados cuantitativos obtenidos de la muestra, tienen su base en opiniones y percepciones de los usuarios encuestados.

- Muestreo por cuotas de tamaño del hogar, edad, sexo, actividad laboral y tamaño del hábitat[8].

Tabla 1: Distribución muestral por CCAA (%)

CCAA	Muestra Obtenida	Muestra Teórica
Andalucía	15,2	15,2
Aragón	3,5	3,0
Asturias	3,6	2,5
Baleares	1,9	2,7
Canarias	4,3	4,7
Cantabria	1,4	1,3
Castilla-La Mancha	3,0	2,9
Castilla y León	6,2	5,4
Cataluña	17,0	18,5
País Vasco	5,1	4,7
Extremadura	1,6	1,4
Galicia	6,4	4,5
Madrid	16,8	18,6
Murcia	2,2	2,5
Navarra	1,0	1,4
La Rioja	0,4	0,7
Comunidad Valenciana	10,2	10,0

Fuente: INTECO

Aunque las desviaciones entre la muestra obtenida y la teórica han sido pequeñas, la muestra se ha equilibrado al universo en base a los datos poblacionales por CCAA, para el universo descrito anteriormente, y a las variables de cuota, para alcanzar un ajuste más perfecto.

[8] Estas cuotas se han obtenido de datos representativos a nivel nacional de internautas mayores de 15 años que se conectan más de una vez al mes desde el hogar facilitados por Red.es, entidad pública empresarial del Ministerio de Industria, Comercio y Turismo. ("Las TIC en los hogares españoles: 11ª Oleada-Octubre 2006").

Tabla 2: Distribución muestral por categorías sociodemográficas (%)

Concepto	Muestra Obtenida	Muestra Teórica
Actividad		
Ocupados	83,9	71,7
Parado	7,8	4,6
Estudio	3,2	16,1
Jubilado	2,7	3,0
Otros Inactivos	2,4	4,6
Tamaño hogar		
1	8,2	3,2
2	22,6	15,4
3	24,3	28,7
4 y mas	45,0	52,7
Sexo		
Hombre	51,0	53,7
Mujer	49,0	46,3
Hábitat		
Hasta 20.000	28,1	24,8
De 20.001 a 100.000	24,8	24,1
Más de 100.000 y capitales	47,2	51,1
Edad		
Hasta 24	21,6	23,4
De 25-35	37,1	28,2
De 35-49	32,4	31,8
De 50 y mas	8,8	16,6

Base muestra =2.860 *Fuente: INTECO*

- Captura de información: Entrevistas online a partir de un panel de usuarios de Internet con un total 2.860 encuestados.

- Trabajo de campo: Realizado entre abril y junio de 2008.

- Error muestral: De acuerdo con los criterios del muestreo aleatorio simple para variables dicotómicas en las que p=q=0,5 y para un nivel de confianza del 95,5%, se establece el siguiente cálculo del error muestral:

  Muestra total n= 2.860, error muestral ±1,87%.

4. Realización de **35 entrevistas** en profundidad a:

   a) Responsables jurídicos y tecnológicos de distintas redes sociales.

b) Usuarios de redes sociales.

c) Profesionales del Derecho Tecnológico y Seguridad de la Información.

d) Instituciones públicas y entidades sin ánimo de lucro implicadas.

5. Creación de **3 grupos de trabajo**:

a) Grupo jurídico y de la seguridad de la información.

b) Grupo de usuarios de redes sociales.

c) Grupo de usuarios menores de redes sociales.

1.4.2 Fase II. Procedimiento de análisis de la información

Tras la realización del trabajo de campo y la recopilación de los recursos informativos disponibles sobre el fenómeno, se ha procedido al análisis de las redes sociales desde los siguientes puntos de vista:

Aspectos Jurídicos

- Protección de los derechos al honor, propia imagen, intimidad y privacidad de los usuarios.
- Protección de Datos de Carácter Personal.
- Protección de los consumidores y usuarios y, en su caso, condiciones generales de la contratación.
- Protección de la propiedad intelectual e industrial.
- Protección de menores e incapaces.
- Protección de los trabajadores.

Aspectos relativos a la seguridad de la información

- Sistemas de seguridad configurados por parte de los sitios web.
- Sistemas de protección interna de usuarios, contenidos y denuncias.
- Sistemas previstos para la resolución de controversias.
- Sistemas específicos para la protección de menores e incapaces.

Aspectos relativos a los modelos de negocio y medios de explotación

- Financiación de las redes sociales.
- Comercio electrónico a través de las redes sociales.
- Vías de negocio y cadena de valor.
- Nuevas líneas de negocio y problemas relativos a su seguridad.

Aspectos relativos a la percepción social de las redes sociales

- La red social como nueva forma de contacto.
- Las redes sociales como generadoras de tendencia.
- Los peligros sociológicos de las redes sociales.

Con todo ello se ha realizado un análisis de las redes sociales en su conjunto como realidad social y como movimiento en el que los usuarios pueden llegar a desarrollarse como individuos; desde la óptica de los usuarios de niveles básico, medio y avanzado. De igual forma se ha analizado la industria poniendo de relieve los principales problemas y vulnerabilidades que las propias entidades desarrolladoras del objeto del estudio detectan a la hora de llevar a cabo su actividad.

1.4.3 Fase III. Fase de recomendaciones y conclusiones

Tras el análisis de toda la información clasificada, y esclarecidos los resultados de las entrevistas, se han establecido una serie de puntos comunes en cuanto a las observaciones de los usuarios y a los propósitos de las propias plataformas.

Las *recomendaciones* se centran, de un lado, en las principales vías de mejora de las plataformas y, de otro, en que los intervinientes en las mismas dispongan de información respecto de las actuaciones que pueden realizar y de las conductas que se deberían evitar. Así, las recomendaciones se dirigen a:

- La **industria:** centradas en las soluciones a los principales problemas observados tanto en la realización del informe así como a las recomendaciones específicas extraídas de las entrevistas y de los grupos de trabajo dirigidas a las redes sociales y plataformas colaborativas.
- Las **Administraciones Públicas:** recomendaciones a los distintos órganos de la Administración para que dispongan de conocimientos necesarios para la mejor defensa de los intereses de los particulares, ante los actos que realizan estas plataformas.

- Los **usuarios y asociaciones:** se aportan recomendaciones para que los usuarios y las entidades que los representan dispongan de información válida de cómo operar en el entorno de las distintas redes sociales y/o plataformas análogas.

Por lo que respecta a las *conclusiones*, se ha procurado la obtención de aquellas que conlleven un carácter general, aplicable al mayor número posible de redes sociales y sitios web colaborativos, sin caer en el error metodológico de reducir el documento hasta un nivel de concreción que provoque que el informe pierda su verdadera finalidad.

1.5 Estructura de contenidos

El presente Estudio se estructura en los siguientes bloques de información:

Situación y definición de las redes sociales

Ofrece, de forma clara y sencilla, una visión global de la situación actual del sector: las tipologías de redes existentes y los principales modelos de negocio para comprender la situación y/o problemática de este tipo de plataformas y su posición actual en el mercado.

Análisis de los aspectos más relevantes y de la problemática específica de las redes sociales

En este apartado se analizan los principales derechos protegidos desde la óptica jurídica haciendo especial hincapié en la situación en la que se encuentran el colectivo de usuarios especialmente vulnerables -menores e incapaces- y los trabajadores.

A la hora de realizar el análisis, se ha tenido en cuenta cuál es el derecho, qué medidas de defensa le son aplicables y cuáles son las actitudes de las diferentes plataformas respecto a dichos aspectos concretos. Se han valorado principalmente cuatro temáticas:

- **Derecho al honor, intimidad y propia imagen:** se tienen en consideración las actuaciones que, tanto los usuarios, como las redes, realizan respecto de la imagen y otros datos que se escapan de la propia esfera de la protección de datos, como por ejemplo las cesiones de imágenes para finalidad comercial.

- **Protección de datos de carácter personal:** se estudian las actividades que realizan las diferentes plataformas teniendo en cuenta, entre otros: el tipo de usuarios, los datos recabados o la cesión de estos.

- **Propiedad intelectual e industrial**: desde la óptica de la propiedad intelectual se analiza el tipo de cesiones de derechos que se realizan a favor de la plataforma y los usos que pueden realizarse de estas. Desde la óptica de la propiedad industrial se examinan los usos de las denominaciones comerciales y de marcas por parte de las plataformas y de los usuarios de las mismas.

- **Consumidores y usuarios:** se analizan las diferentes medidas de defensa con las que cuentan los usuarios de las redes sociales, aplicando las medidas normativas de defensa y protección de los mismos.

Recomendaciones y conclusiones

Las **recomendaciones** se centran, de un lado, en las principales vías de mejora de las plataformas y, de otro, en que los intervinientes en las mismas dispongan de información respecto de las actuaciones que pueden realizar y de las conductas que se deberían evitar. Tales recomendaciones están dirigidas a la industria, a las Administraciones Públicas y a los usuarios y asociaciones. De otro lado, las **conclusiones** han sido extraídas atendiendo a un criterio general, de forma que resulten de aplicación al mayor número posible de redes sociales y sitios web colaborativos.

2 SITUACIÓN: DEFINICIÓN DE LAS REDES SOCIALES

Este capítulo ofrece una visión global de la situación actual de las distintas redes sociales, las tipologías de redes que se presentan al público y los principales modelos de negocio empleados en el sector, permitiendo comprender la situación y problemática de este tipo de plataformas así como su posición actual en el mercado.

2.1 Caracterización de las redes sociales

2.1.1 Fundamentación teórica

Cuando se habla de redes sociales, se hace referencia a las plataformas online desde las que los usuarios registrados pueden interactuar mediante mensajes, compartir información, imágenes o vídeos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios de su grupo.

El análisis de las redes sociales ha irrumpido en muchas ciencias sociales en los últimos veinte años como una nueva herramienta de análisis de los individuos y de sus relaciones sociales. Al centrarse en las relaciones de los individuos (o grupos de individuos) y no en las características de los mismos (raza, edad, ingresos, educación) se han utilizado para el estudio de hábitos, gustos y formas de relacionarse de los grupos sociales.

Toda red social se fundamenta en la *teoría de los seis grados de separación*[9], en virtud de la cual, cualquier individuo puede estar conectado a cualquier otra persona en el planeta, a través de una cadena de conocidos con no más de cinco intermediarios (con un total de seis conexiones). La cifra de conocidos aumenta a medida que lo hacen los eslabones de la cadena. Los individuos de primer grado serán los más próximos y, según se avanza en el grado de separación, disminuye la relación y la confianza.

Internet y el desarrollo de potentes aplicaciones informáticas que generan plataformas de intercambio de información e interacción entre individuos ha supuesto una auténtica revolución para la aparición del concepto de red social tal y como se conoce hoy en día. La universalidad que ofrece la Red permite ampliar el número de contactos y estrechar lazos de unión entre aquellos usuarios que tienen intereses comunes.

2.1.2 Origen y evolución

El origen de las redes sociales en Internet se remonta, al menos, al año 1995, cuando Randy Conrads crea el sitio web “classmates.com”. Con esta red social se pretendía que los usuarios pudiesen recuperar o mantener el contacto con antiguos compañeros del colegio, instituto, universidad, etc.

[9] Teoría inicialmente propuesta en 1929 por el escritor húngaro Frigyes Karinthy. Recogida también en el libro "Six Degrees: The Science of a Connected Age” del sociólogo Duncan Watts, quien asegura que es posible acceder a cualquier persona del planeta en tan solo seis “saltos”.

En el año 2002 comienzan a aparecer sitios web que promocionan las *redes de círculos de amigos en línea,* adquiriendo popularidad en el año 2003 con la llegada de portales web como *MySpace* o *Xing*.

La popularidad de estas plataformas creció exponencialmente. Grandes empresas y multinacionales de Internet emprendieron entonces nuevos proyectos en el entorno de las redes sociales. Así, cabe señalar como claros ejemplos el lanzamiento de *Orkut* por Google o Yahoo! 360º por parte de Yahoo!. A esto se une la creación de otras muchas redes sociales verticales que han ido apareciendo, dedicándose a sectores concretos[10].

Tabla 3: Cronología de las redes sociales

1995	**Classmates**			
1997	**SixDegress**			
2002	**Friendster**	**Fotolog**		
2003	**MySpace**	**LinkedIn**	**Hi5**	**SecondLife**
2004	**Orkut**			
2005	**Yahoo!360º**	**Bebo**		
2006	**Facebook**	**Twitter**	**Tuenti**	
2007	**Lively**			

Fuente: INTECO a partir de Panda Security

El aumento de popularidad de las redes sociales ha trascurrido en paralelo al aumento en los niveles de intercambio de contenidos a través de la Red. Esto ha hecho de Internet un medio más social que permite comunicar, entretener y compartir. Los usuarios han pasado de una etapa en la que eran considerados meros consumidores de contenidos creados por terceros usuarios con ciertos conocimientos de programación, a una etapa en la que los contenidos son producidos por los propios usuarios equipados con un ordenador, conexión y conocimientos básicos en el uso de Internet.

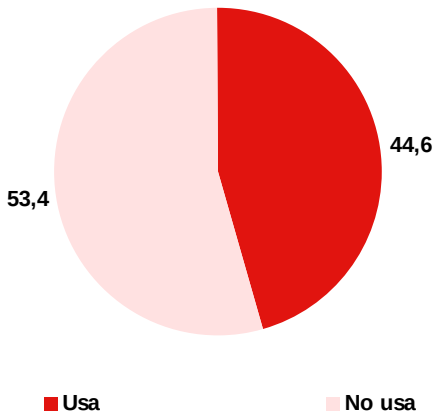
La expansión de este fenómeno es tal que las últimas estadísticas a nivel mundial (3ª Oleada del Estudio *Power to the people social media. Wave 3* de Universal McCann de marzo 2008) cifran el número de usuarios de redes sociales en 272 millones, un 58% de los usuarios de Internet registrados en todo el mundo, lo que supone un incremento del 21% respecto de los datos registrados en junio de 2007.

En el caso de España, las fuentes son diversas, pero todas coinciden que en 2008 el número de usuarios españoles de Internet que utiliza habitualmente redes sociales se

[10] Así, cabe destacar la aparición en España de redes sociales como Minube.com, Patatabrava.com, Moterus.com, VIVO.com, dedicada a sectores concretos como los viajes, la universidad, las motos y el mundo del espectáculo.

sitúa entre el 40% y el 50%[11]. En concreto, siguiendo con el estudio de Universal McCann se señala que el 44,6% de los internautas españoles utiliza estos servicios (Gráfico 1).

Gráfico 1: Porcentaje de usuarios españoles de redes sociales. Marzo 2008



Fuente: INTECO a partir de Universal McCann

Estos nuevos servicios se configuran como poderosos canales de comunicación e interacción, que permiten a los usuarios actuar como grupos segmentados (ocio, comunicación, profesionalización, etc.). La Red se consolida, por tanto, como un espacio para formar relaciones, comunidades y otros sistemas sociales en los que rigen normas similares a las del mundo real y en los que la participación está motivada por la reputación, tal como ocurre en la sociedad.

2.1.3 Definiciones

El concepto de red social ha sido ampliamente analizado por profesionales de diferentes sectores, no existiendo en la actualidad un concepto absolutamente cerrado y aceptado por todos ellos.

Antes de analizar el concepto de red social, se debe tener en cuenta el tipo de red que se va a definir, por lo que es necesario diferenciar en un primer momento si se trata de una red social tradicional o de una red social online[12]. En este sentido, conviene señalar que

[11] Por ejemplo, un 50 % según Zed Digital (El fenómeno de las redes sociales. Percepción, usos y publicidad. Noviembre 2008) o un 45 %, según The Cocktail Analysis (Observatorio de evaluación de redes sociales: Herramientas de comunicación on-line: Las Redes Sociales. Noviembre 2008)

[12] A pesar de que el concepto de red social es utilizado indistintamente para las redes sociales online y las tradicionales, este hecho supone incurrir en un error que puede provocar que el análisis posterior de los elementos que la componen y caracterizan se vea desvirtuado.

una red social es, ante todo, una forma de interacción entre miembros y/o espacios sociales. A partir de esta premisa, se recogen a continuación algunas definiciones de redes sociales:

"*Formas de interacción social, que se definen fundamentalmente por los intercambios dinámicos entre los sujetos que las forman. Las redes son sistemas abiertos y horizontales y aglutinan a conjuntos de personas que se identifican con las mismas necesidades y problemáticas. Las redes, por tanto, se erigen como una forma de organización social que permite a un grupo de personas potenciar sus recursos y contribuir a la resolución de problemas*"[13].

"Las Redes son formas de interacción social, definidas como un intercambio dinámico entre personas, grupos e instituciones en contextos de complejidad. Un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos"[14].

"En términos generales, el concepto de red se utiliza para hacer referencia a dos fenómenos: por un lado, se consideran redes todos los conjuntos de interacciones que se dan de forma espontánea, y por el otro, y este es el aspecto que interesa destacar, las redes pretenden organizar esas interacciones espontáneas con un cierto grado de formalidad, en el sentido de establecer intereses, problemáticas, preguntas y fines comunes"[15].

Dada la importancia de este fenómeno, el Grupo Internacional sobre protección de datos en las Telecomunicaciones de Berlín aprobó, en su reunión del 4 de marzo de 2008 el "*Rome Memorandum*[16]. En esta posición común, que destaca que *"uno de los desafíos que pueden observarse es que la mayoría de la información que se publica en las redes sociales, se hace bajo la iniciativa de los usuarios y basado en su consentimiento"*, se analizan los riesgos para la privacidad y seguridad de las redes sociales, y se apuntan unas pautas a los reguladores, a los proveedores y a los usuarios. En este documento se establece que la aparente gratuidad de los servicios no se da siempre, dado que los

---

En este sentido, se puede afirmar que las redes sociales online son *"servicios de la Sociedad de la Información, consistentes en la creación de comunidades online de personas que comparten intereses, actividades, o que están interesados en explorar y conocer los intereses de los demás*".

[13] Definición extraída de "Redes. Una aproximación al concepto". Dra. Marta Rizo García, Universidad Autónoma de la Ciudad de México.

[14] Concepto extraído del Estudio "Castilla y León 2.0. Hacia la Sociedad de la Colaboración". Edición 2008.

[15] Concepto extraído del artículo "*Redes. Una aproximación al concepto*" escrito por Marta Rizo García, doctora en Comunicación por la Universidad Autónoma de Barcelona y profesora-Investigadora de la Academia de Comunicación y Cultura y del Centro de Estudios sobre la Ciudad de la Univ. Autónoma de México. Miembro de la Red de Formación en Teoría de la Comunicación y Comunicología (REDECOM, México) y de la Red de Estudios en Cibercultura y Nuevas Tecnologías de Información y Comunicación (RECIBER, México).

[16] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

usuarios, de hecho, pagan a través de usos secundarios con sus perfiles personales como puede ser el marketing dirigido o personalizado.

Por otro lado, la European Network and Information Security Agency (ENISA) publicó en octubre de 2007 un documento de síntesis "Recomendaciones y seguridad para las redes sociales *online*"[17] dirigido tanto a los proveedores de redes sociales como a los órganos encargados de dictar normas al respecto, en el que se realizan una serie de recomendaciones, entre las que se destaca la inversión en educación de los usuarios de estas redes o la promoción de mayores controles de acceso y autenticación.

Partiendo de las reflexiones anteriores, puede considerarse que:

"Las redes sociales online son servicios prestados a través de Internet que permiten a los usuarios generar un perfil, desde el que hacer públicos datos e información personal y que proporcionan herramientas que permiten interactuar con otros usuarios y localizarlos en función de las características publicadas en sus perfiles"

2.1.4 Claves de éxito

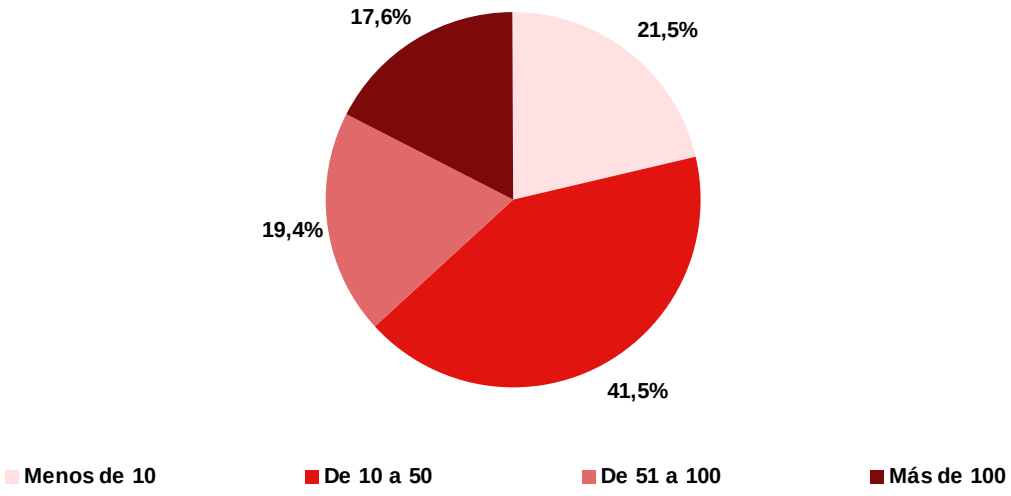
Entre los aspectos que han propiciado el auge de este fenómeno online, cabe destacar:

- El modelo de crecimiento de estas plataformas se basa fundamentalmente en la técnica popularmente conocida como "*boca a boca*" o proceso viral[18], en el que un número inicial de participantes invita a sus conocidos, mediante correo electrónico, a unirse al sitio web. Los nuevos participantes repiten el proceso, incrementándose rápidamente el número total de miembros. El Gráfico 2 ilustra esta idea. Así, se comprueba que más de uno de cada tres usuarios españoles de redes sociales (un 37,0%) tiene más de 50 contactos en ellas y sólo uno de cada cinco (un 21,5%) tiene menos de 10, lo que da una idea del nivel de dispersión y la velocidad de penetración que tienen estos servicios.

[17] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[18] Cuando se habla de viralidad respecto a las redes sociales, se hace referencia a la capacidad que tienen este tipo de redes para lograr el máximo crecimiento en número de usuarios, en el menor tiempo posible. Se trata de un concepto que se encuentra directamente relacionado con el marketing.

Gráfico 2: Número de contactos de los usuarios españoles de redes sociales. Octubre 2008



Fuente: INTECO a partir de Zed Digital

- Ofrecen aplicaciones y funcionalidades diversas, entre otras: actualizaciones automáticas de la libreta de direcciones de las cuentas de correo electrónico, perfiles públicos y visibles para todos los visitantes, la capacidad de crear nuevos contactos mediante *servicios de presentación* y otras formas de conexión social en línea. Estas aplicaciones se fundamentan en tres variables conocidas como *"las 3Cs"*:
    - *Comunicación* (ayudan a la puesta en común de conocimientos).
    - *Comunidad* (ayudan a encontrar e integrar comunidades).
    - *Cooperación* (ayudan a realizar actividades juntos).

Un objetivo de las redes sociales se centra en conseguir **que sus miembros utilicen el medio online para convocar actos y acciones que tengan efectos en el mundo offline.** Buen ejemplo de esta circunstancia son las *"Redes Sociales de Compras",* en las que los usuarios pueden poner en común sus opiniones, gustos y experiencias respecto a productos y servicios determinados, pudiendo organizar compras en grandes grupos a través de las que se logran grandes descuentos por volumen. Este tipo de redes permite también que los usuarios reciban recomendaciones para realizar actividades en su vida cotidiana (recomendaciones de ocio, gastronómicas, etc.) según las preferencias del usuario.

2.2 Tipología de las redes sociales

Las redes sociales se pueden categorizar atendiendo al público objetivo al que se dirigen, o al tipo de contenido que albergan. De esta forma, se distinguen al menos, dos grandes grupos de redes sociales: generalistas o de ocio y profesionales.

A pesar de que cada tipo presenta una serie de aspectos particulares, ambos grupos cuentan con una serie de características básicas y estructurales comunes:

- Tienen como finalidad principal **poner en contacto e interrelacionar a personas.** La plataforma facilita la conexión de forma sencilla y rápida.

- Permiten la **interacción** entre todos los usuarios de la plataforma, ya sea compartiendo información, permitiendo el contacto directo o facilitando nuevos contactos de interés.

- Permiten y fomentan la posibilidad de que los usuarios inicialmente contactados a través del medio online, **acaben entablando un contacto real.**

- Permiten que el contacto entre usuarios sea **ilimitado**, en la medida en la que el concepto espacio y tiempo se convierte en relativo, al poder comunicar desde y hacia cualquier lugar, así como en cualquier momento, con la única condición de que ambas partes acepten relacionarse entre sí.

- Fomentan la **difusión viral de la red social**, a través de cada uno de los usuarios que la componen, empleando este método como principal forma de crecimiento del número de usuarios.

En las siguientes páginas se define exhaustivamente cada uno de los dos grupos anteriores conforme a su público objetivo y a los contenidos alojados en las mismas.

2.2.1 Redes sociales generalistas o de ocio

Este tipo de redes se caracteriza porque su objetivo principal radica en el hecho de *facilitar y potenciar las relaciones personales* entre los usuarios que la componen. El grado de crecimiento de estas redes ha sido muy elevado en los últimos años, llegando a constituirse plataformas como Facebook en las que en diciembre de 2008 se produce la entrada diaria de más de 120 millones de usuarios activos que crean el contenido que define su sitio web[19].

Según muestran los datos de los últimos estudios realizados en el sector[20] este tipo de

[19] Datos publicados en The Facebook Blog y en cnet news.

[20] Según el último estudio publicado por la entidad Pew Internet & American Life Project denominado "*Social Networking Websites and Teens: An Overview*" y elaborado por Amanda Lenhart & Mary Madden, el 55% de

redes complementa e incluso sustituye, especialmente en el rango de edad de usuarios más jóvenes, a otros medios de comunicación como la mensajería instantánea, ampliamente utilizada durante los últimos años. Este hecho se debe en gran medida a los **aspectos que caracterizan a las redes sociales generalistas o de ocio**:

- Ofrecen gran variedad de aplicaciones y/o funcionalidades que permiten a los usuarios prescindir de herramientas de comunicación externas, poniendo a su disposición una plataforma que integra todas las aplicaciones necesarias en una misma pantalla.

- Ofrecen y fomentan que los usuarios no se centren únicamente en operar de forma online, sino que este medio sirva de plataforma a través de la que poder convocar y organizar aspectos de su vida cotidiana[21].

- Ponen a disposición de la comunidad de usuarios parte del código[22] usado para programar la plataforma, de modo que los usuarios puedan desarrollar aplicaciones propias, que sean ejecutadas dentro de la red social, o aplicaciones externas que se interconecten con la plataforma, logrando así el aumento de la utilidad y con ello de la difusión.

Dentro de la gran modalidad de las redes sociales generalistas o de ocio, se puede establecer, al menos, una **subclasificación, atendiendo a la finalidad o temática de las mismas:**

Plataformas de intercambio de contenidos e información

Servicios como Youtube, Dalealplay.com, Google Vídeo, etc., que se caracterizan principalmente por la puesta a disposición de los usuarios de herramientas gratuitas y sencillas para el intercambio y la publicación de contenidos digitales (vídeos, fotos, textos, etc.).

En sentido estricto, no se puede considerar que este tipo de plataformas sean redes sociales, ya que únicamente permiten el alojamiento de contenidos para que el resto de usuarios puedan visionarlo, limitándose la interacción entre los usuarios a la posibilidad de incluir comentarios respecto a los contenidos y otorgar puntuaciones a los mismos.

---

los menores de edad que se encuentran conectados a Internet ha creado y actualiza con frecuencia su perfil de usuario en al menos una red social.

[21] Un claro ejemplo de este hecho es la red social española www.salir.com donde los usuarios organizan y recomiendan lugares que visitar en una ciudad determinada o los acontecimientos vividos durante el 2008 en relación con los secuestrados por parte del grupo terrorista las FARC, llevándose a cabo por parte de usuarios de la red social de Facebook concentraciones online que posteriormente fueron realizadas en las plazas y otros lugares.

[22] Un claro ejemplo de esta práctica es la plataforma OpenSocial, propiedad de Google y cuya potencialidad es realmente alta. Para más información acceda a la siguiente dirección.
http://code.google.com/apis/opensocial.

No obstante, y aunque estas plataformas eran inicialmente independientes de las redes sociales, permiten actualmente enlazar los contenidos y publicarlos directamente en el perfil de la red utilizada por el usuario[23].

Redes sociales basadas en perfiles

Redes como Facebook, Tuenti, Wamba, Orkut, etc. Este tipo de servicio es el más utilizado en Internet,[24] por encima de cualquier otro tipo de red social y es además el más representativo dentro del grupo de redes sociales de ocio.

Las aplicaciones que terceros están desarrollando para algunas de estas redes permite que ofrezcan cada vez un mayor número de posibilidades, lo que unido a su idiosincrasia está sustituyendo, como ya se ha comentado, el uso de herramientas de comunicación tradicionales en Internet.

Este tipo de redes, con frecuencia, se encuentra dirigido a temáticas concretas, creando grandes comunidades de usuarios con altos niveles de especialización en determinados temas, convirtiéndose en grandes fuentes de información y conocimiento[25].

Redes de microblogging o nanoblogging

Plataformas como Twitter o Yammer. Este tipo de redes basan su servicio en la actualización constante de los perfiles de los usuarios mediante pequeños mensajes de texto, que no superan los 160 caracteres. Esto permite poner a disposición del resto de usuarios información clara, concisa, sencilla y rápida, sobre las actividades que se están realizando en ese momento, impresiones, pensamientos, publicaciones, etc.

Todas las actualizaciones son mostradas en la página web del perfil del usuario, al mismo tiempo que son publicadas en la página web de seguimiento de otros usuarios de forma inmediata.

Estrictamente, este tipo de redes no puede ser considerada una red social, ya que no conlleva una interacción entre los usuarios de la misma, limitándose ésta, como máximo, al envío de mensajes de texto o, a lo sumo, a la actualización de los perfiles mediante el

[23] Cabe destacar que en la gran mayoría de las plataformas de intercambio de contenidos como Youtube, DevianArt o Fotolog, se ponen a disposición de los usuarios los iconos de acceso directo a las principales redes sociales.

[24] Así lo determina el estudio recientemente publicado por el Diario Le Monde, *"Réseaux sociaux: des audiences différentes selon les continents"*. En dicho informe se aprecia claramente como las redes sociales más visitadas en cada uno de los continentes son las redes sociales basadas en perfiles tales como MySpace, Facebook, Tuenti, Friendster, Netlog, Bebo.

[25] Ejemplos de este tipo de plataformas son: Devianart (exposiciones virtuales de fotografía) o Myartinfo.com (obras plásticas), Moterus (rutas en moto por España y comparativas de motos).

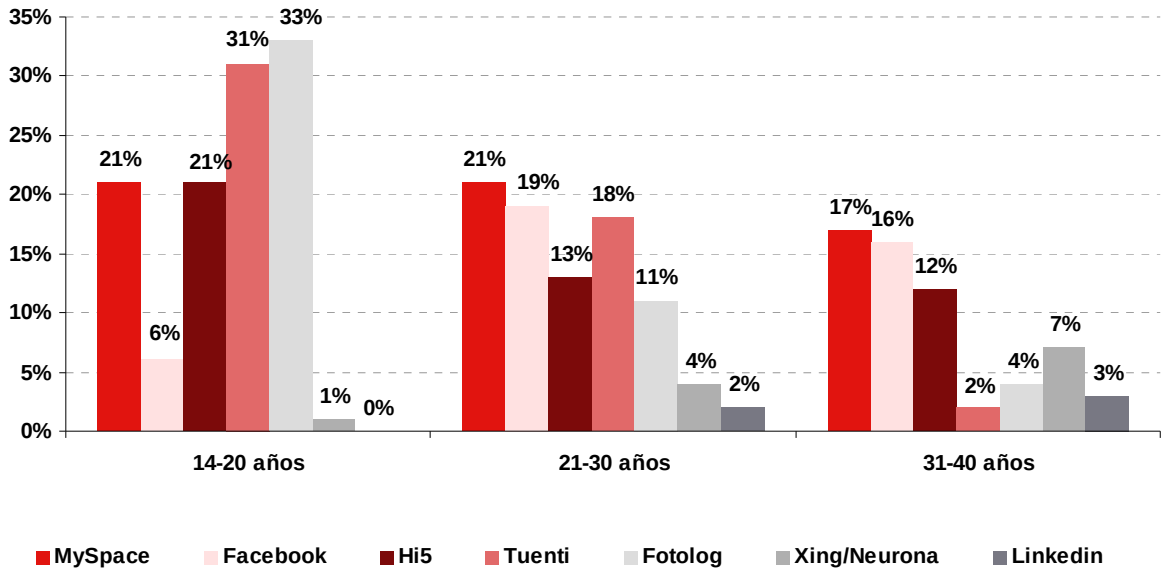
uso de fotografías comentadas, aprovechando que los dispositivos móviles actuales disponen de cámaras fotográficas y conexión a Internet.

2.2.2 Redes sociales de contenido profesional

Se configuran como nuevas herramientas de ayuda para establecer contactos profesionales con otros usuarios. Entre ellas se encuentran webs como Xing o Linkedin y constituyen el segundo gran bloque de redes sociales.

Están creadas y diseñadas con la finalidad de poner en contacto y mantener la relación a nivel profesional con diferentes sujetos que tengan interés para el usuario. Es por ello que la edad es un factor determinante en el uso de estas redes. Como se aprecia en el Gráfico 3, las redes de contenido profesional apenas son utilizadas por los menores de 20 años, incrementándose el porcentaje de internautas usuarios a medida que aumenta su edad. De manera inversa, el porcentaje de usuarios de las redes sociales de ocio disminuye con la edad o sufre una migración desde las redes más orientadas a adolescentes (Tuenti, Fotolog) hacia otras con mayor número de servicios (Facebook).

Gráfico 3: Penetración por grupos de edad en España de las diferentes redes. Julio 2008 (%)



Fuente: INTECO a partir de Observatorio sobre la Evolución de las redes sociales (The cocktail analysis)

Así, entre las principales utilidades cabe citar:

- *Desde el lado del trabajador*: la búsqueda de nuevas oportunidades de empleo, el establecimiento de nuevos contactos profesionales o la promoción laboral. Permiten a los usuarios entrar en contacto con otros profesionales de su sector a través de conocidos comunes de confianza, ayudando a mejorar las conexiones con otras

personas que en circunstancias habituales serían inaccesibles debido a su cargo o responsabilidad.

- *Desde el lado del empleador*: la presencia en este tipo de redes sociales resulta cada vez más importante, ya que con mayor frecuencia, las empresas utilizan este nuevo recurso para identificar posibles candidatos participantes en sus procesos de selección o profundizar en la información disponible del perfil de los candidatos seleccionados en un proceso de contratación determinado.

Este tipo de redes está en auge. En el año 2007 se consolidaron como uno de los servicios de mayor crecimiento, produciéndose durante los meses de junio y julio grandes fusiones e inversiones económicas en el sector[26].

Los beneficios que este tipo de redes sociales de carácter profesional pueden suponer y reportar al entorno empresarial no radican exclusivamente en servir como herramienta complementaria en un proceso de selección de personal, ni se quedan en las posibilidades que evidencian los datos indicados, sino que además resultan especialmente atractivas como alternativa de negocio, ya que además permiten:

- La realización de acciones de marketing personalizado.
- La creación de servicios premium de suscripción.
- La publicación de contenidos destacados y la promoción de contenidos propios.
- La venta de bonos de "*aumento de confianza del usuario*". Se trata de una especie de certificación proveniente de la propia red social que asegura que el usuario es de confianza y que sus finalidades no son mal intencionadas[27].

En particular, el uso de los servicios premium en este tipo de redes, a diferencia de otro tipo de plataformas, dispone de un alto rendimiento del número de usuarios premium, que abonan una cantidad mensual, para acceder a servicios avanzados[28].

[26] Durante los meses de junio y julio de 2007, Xing, una de las principales redes sociales del mundo adquirió dos de sus principales redes sociales profesionales competidoras, Neurona y eConozco. Esta fusión empresarial ha supuesto que Xing haya superado los 500.000 usuarios únicos.

[27] La red social Netlogm ha iniciado una nueva vía de monetización de servicios adicionales comercializando unos certificados que garantizan la confianza de un individuo. www.netlog.com

[28] *"Los más de un millón de usuarios de pago demuestran claramente que los profesionales aprecian la utilidad de xing.com como herramienta profesional de uso diario e invierten 5,95 € mensuales para tener acceso a las funciones avanzadas de la plataforma". "La lealtad del suscriptor es uno de los mayores artífices de la rentabilidad de este negocio; más de un 75% de los usuarios de pago siguen suscritos al servicio Premium de XING después de 3 años de suscripción."* Palabras que señala Lars Hinrichs, Consejero Delegado y fundador de XING AG.

2.3 Cadena de valor y modelos de negocio

Otro de los temas ampliamente debatidos y tratados en relación con este tipo de plataformas -además de la necesidad de protección de los datos de carácter personal y la privacidad e intimidad de los usuarios- es su viabilidad económica, es decir, si pueden llegar a convertirse en negocios rentables desde el punto de vista económico.

En este sentido, y aunque son numerosos los artículos escritos en relación a las posibilidades de monetización de este tipo de plataformas y las capacidades de explotación real, se continúa trabajando en el estudio e identificación de las claves para rentabilizar al máximo la presencia y participación del número de usuarios que las integran y de los contenidos de que se proveen diariamente.

2.3.1 Cadena de valor de las redes sociales

Como paso previo al análisis del modelo de negocio de las redes sociales conviene conocer los diferentes elementos que integran la cadena de valor:

- **Proveedores de Servicios de Internet** (Internet Services Provider o ISP). Son aquellas entidades encargadas de proveer de tecnología (servidores, conectividad, ancho de banda, etc.) a las redes sociales, garantizando que cualquier usuario pueda acceder a dichas plataformas. Son organizaciones que ofrecen, entre otros servicios, el soporte tecnológico para alojar los sitios web.

  La selección de un ISP adecuado puede suponer el éxito o fracaso de un proyecto de red social, dado que los requerimientos tecnológicos que este tipo de plataformas deben soportar diariamente son exigentes en lo que a transferencia de información se refiere.

  Realizada la selección del ISP, se ha de atender al modelo que va a ser utilizado para el alojamiento de la información en la plataforma. Este alojamiento puede realizarse mediante un *contrato de arrendamiento de servidor dedicado (housing)*[29] o mediante un *contrato de alojamiento de sitio web (hosting)*[30], en función del tráfico previsto de la plataforma online y de las necesidades tecnológicas de la misma.

  El servicio ISP y la propia plataforma tecnológica de la red social, constituyen los elementos técnicos más importantes de la cadena de valor de la red social, sobre los que se articula y construye el resto de elementos que la componen.

[29] En la web del observatorio de INTECO se puede encontrar un modelo de contrato de housing. Este tipo de contrato regula el alojamiento del sitio Web del cliente en un servidor propio del ISP y no compartido con ningún otro cliente.

[30] En la web del observatorio de INTECO se puede encontrar un modelo de contrato de hosting. Este tipo de contrato está destinado a regular la relación jurídica entre el proveedor de servicios de Internet (ISP) y el propietario de un sitio Web que desee alojarlo en un servidor para que sea accesible desde Internet.

- **Plataformas colaborativas y redes sociales**. A la hora de desarrollar y plantear la estrategia de este tipo de plataformas online, se debe considerar de antemano el público objetivo y el tipo de herramientas que pondrá a su disposición. De esta forma, planteará su estrategia de cara a otras actuaciones, como puede ser el desarrollo de aplicaciones o la publicidad.

- **Empresas de marketing y publicidad online**. Son las organizaciones encargadas de realizar y gestionar las campañas publicitarias y las estrategias comerciales que la red social va a emplear para maximizar los beneficios de la monetización de la plataforma a largo plazo de manera sostenible.

  Constituye, junto con la propia red social, el elemento de planificación del modelo de rentabilización económica de la red social. Dentro de este grupo se incluyen los creadores de las aplicaciones.

- **Empresas desarrolladoras de aplicaciones**. Deciden qué tipo de aplicaciones (API) van a desarrollarse, así como el perfil del usuario al que van destinadas.

- **Usuarios**. Son el principal elemento a monetizar por parte de la plataforma. Cuanto mayor sea el número de usuarios estables y recurrentes, mayor será el valor de la plataforma, por lo que para todas las partes implicadas en esta cadena de valor es importante que este número vaya en aumento. También interesa que los usuarios (intervinientes en el proceso de monetización) continúen considerando la plataforma interesante para seguir recomendándola y usándola.

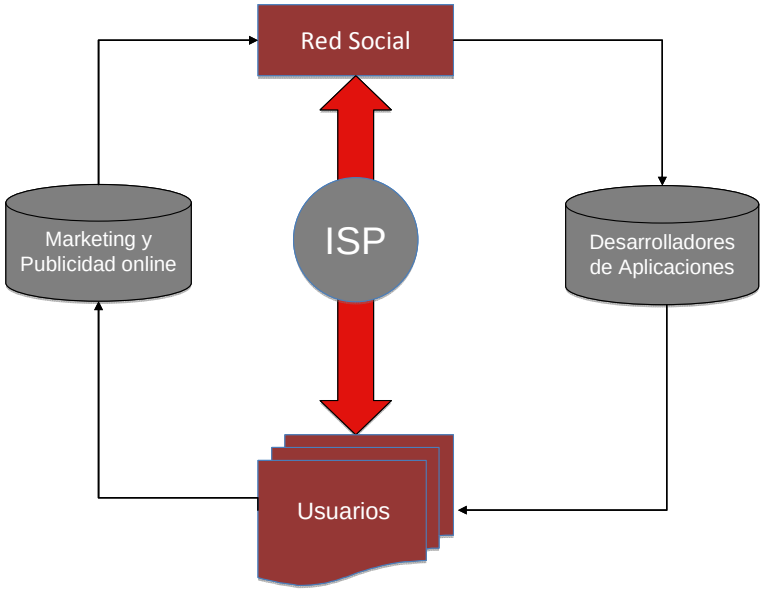
La relación entre los distintos miembros de la cadena de valor se muestra en el Gráfico 4 donde puede apreciarse la intervención de un gran número de sujetos, entre los que cabe destacar a los proveedores del servicio, los ISP´s donde se alojan las plataformas, los usuarios, la masa de desarrolladores de aplicaciones y las centrales de medios y publicidad.

Todo el valor de la red social radica en el número de usuarios registrados, su fidelización, el nivel de actualizaciones y la facilidad de implantar sistemas de explotación económica.

De igual forma, en la cadena de valor de las redes sociales repercute, cada vez más, el papel de los desarrolladores de aplicaciones internas generándose, en algunos casos, un número importante de transacciones económicas a través de ellas.

Por último, y a pesar de que aún no se pueda hablar de un modelo claro de explotación de este tipo de plataformas, parece que la publicidad y los servicios "*premium*" estarán a la cabeza de los sistemas elegidos para obtener la máxima rentabilidad económica.

Gráfico 4: Cadena de valor de las Redes Sociales



Fuente: INTECO

2.3.2 Modelos de negocio de las redes sociales

A continuación se presenta un análisis de la situación actual y futura de los modelos de negocio aplicados en las principales redes sociales online, así como de la eficacia de los mismos.

Modelo actual de negocio y situación de las redes sociales

El modelo de negocio actual de las redes sociales se estructura en fases que integran el siguiente esquema:

Fase I: Alcanzar una masa crítica de usuarios

Siguiendo un modelo de negocio tradicional, las redes sociales avanzan en una línea de trabajo dirigida a la fidelización e incremento del número de usuarios habituales de la plataforma para garantizar su sostenibilidad a largo plazo y, de esta forma, optimizar su explotación comercial.

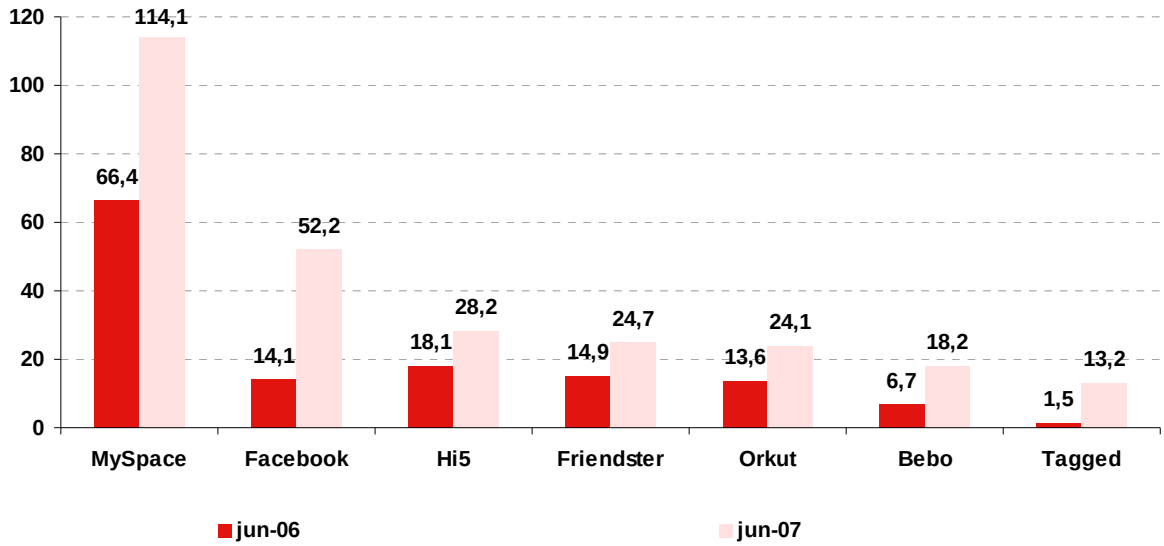
La búsqueda de nuevos usuarios tiene su razón de ser en el hecho de que estos diariamente intercambian información, documentos, vídeos, imágenes y experiencias que, con un tratamiento apropiado, pueden reportar a la plataforma el éxito de una campaña comercial.

La magnitud del fenómeno de las redes sociales, webs colaborativas y plataformas análogas a nivel internacional ha alcanzado en los últimos años niveles importantes. Así,

y aunque las fuentes de datos son diversas[31], todas coinciden en el incremento de estos servicios avanzados online.

Recientes estudios de medición y análisis del tráfico en Internet[32] informan de que dentro de los 500 sitios web más visitados del mundo se encuentran al menos 5 redes sociales[33] (*Facebook*, *MySpace*, *Hi5*, *Orkut),* entre las veinte primeras posiciones. En este sentido, tal y como se observa en el Gráfico 5, es significativo el crecimiento experimentado en el número de visitas a las principales redes sociales durante el periodo comprendido entre junio de 2006 y junio del año 2007.

Gráfico 5: Evolución del número de visitas en las principales redes sociales (millones)



Fuente: INTECO a partir de Alexa Internet

Por continentes, se puede afirmar que los contenidos con mayor número de usuarios recurrentes registrados en redes sociales se encuentran en América del Norte y América Latina, seguidos de Asia y Europa. Además, se observa cómo las redes más utilizadas varían en cada región del mundo. El Gráfico 6 muestra la procedencia que tiene el tráfico en las principales redes sociales, observándose como *Facebook* y *MySpace* reciben la

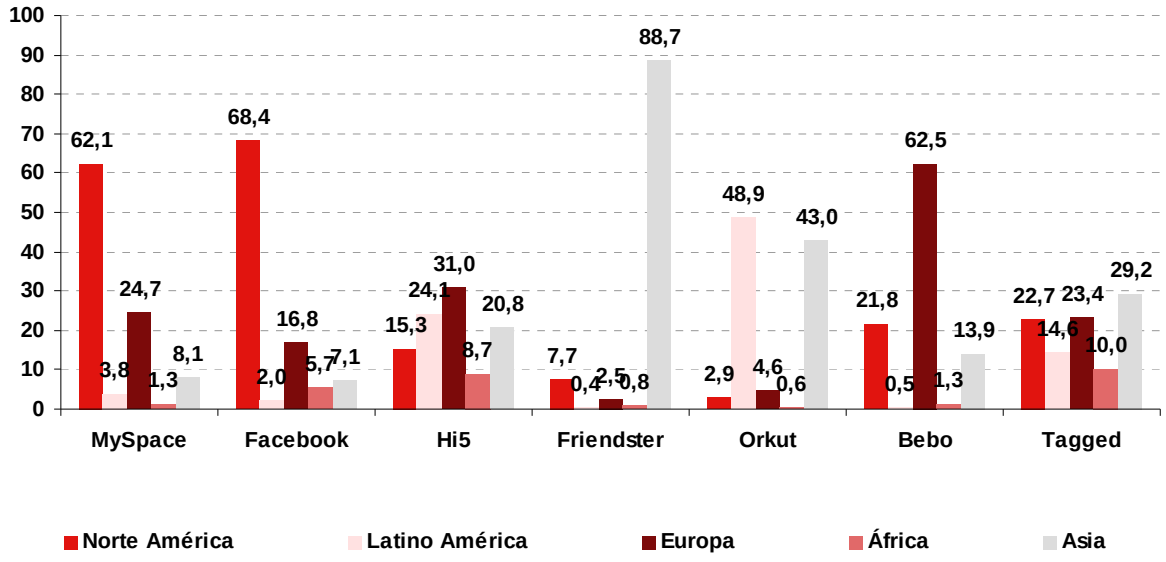
[31] En este sentido, es importante señalar la ausencia de un organismo que de forma global e imparcial ofrezca información y análisis estadístico de los aspectos claves de las redes sociales, permaneciendo estos datos en manos de las propias redes sociales o consultoras de marketing y publicidad.

[32] Alexa Internet Inc: Compañía del Grupo Empresarial Amazon, siendo una de los principales referentes en lo que respecta a medición y análisis del tráfico en Internet.

[33] Más información en http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none. Dichas estadística son de gran importancia debido a que la gran mayoría de las campañas publicitarias, de activismo político o social, utilizan estos datos para fijar nichos de mercado u objetivos de personas a quienes dirigir sus campañas.

mayoría de sus visitas de Norteamérica y de Europa, mientras que la red social *Orkut* lo hace de Latinoamérica y Asia.

Gráfico 6: Distribución geográfica del negocio de las redes sociales en 2007



Fuente: INTECO a partir de Alexa Internet

Puede concluirse que a pesar del carácter global de las redes sociales, se podría llegar a hablar de un cierto *"localismo"* en lo que respecta a la popularidad de las redes sociales en las diferentes áreas geográficas.

Por edades, puede verse que la mayoría de los usuarios de redes sociales, 7 de cada 10, son internautas menores de 35 años:[34] un 36,5% entre 15 y 24 años y un 32,5% entre 25 y 34 años. (Gráfico 7).

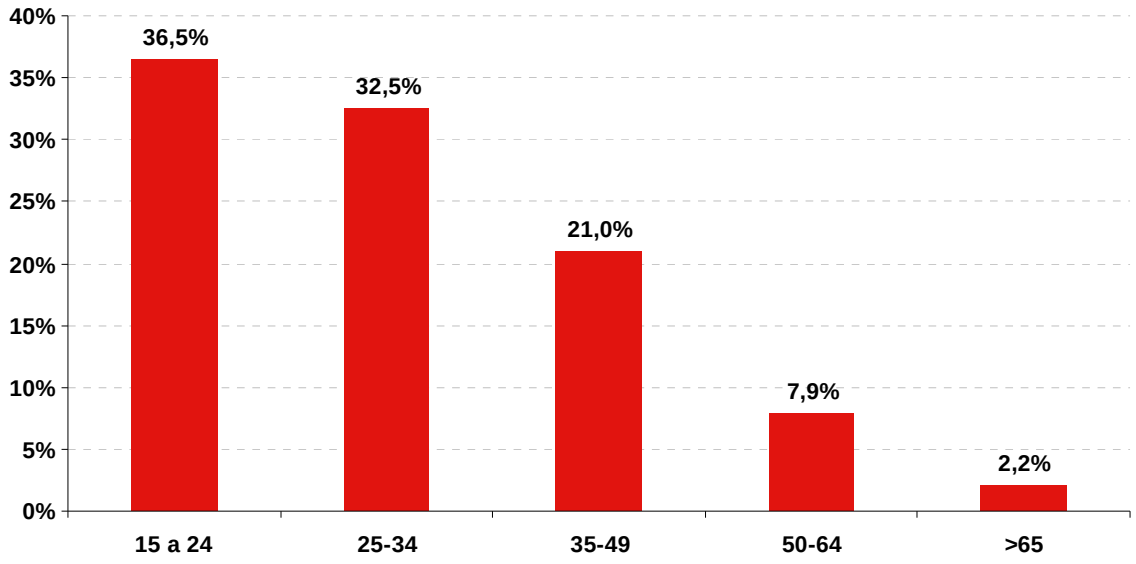
Más aún, según las últimas cifras del Instituto Nacional de Estadística[35], 1 de cada 3 jóvenes en España usa redes sociales; en concreto, el porcentaje de usuarios de redes sociales sobre el total de la población española entre 15 y 24 años es el 29%. De hecho, estudios nacionales e internacionales[36] consideran a este grupo como los usuarios mayoritarios.

[34] La ausencia de datos sobre el uso de redes por parte de menores de 15 años de edad, no debe entenderse como el no uso de este tipo de servicios por parte de esta población; sino que la encuesta que ha servido de base para la elaboración del presente Estudio (Epígrafe 1.4.1), parte del rango de edad de 15 a 24 años.

[35] Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los hogares (octubre 2008).

[36] Por ejemplo, un 35% en Reino Unido según Ofcom ("Social Networking" abril 2008) o incluso un 55% en EEUU según el Pew Internet & American Life Proyect (Informe "*Social Networking Website and Teens: An*

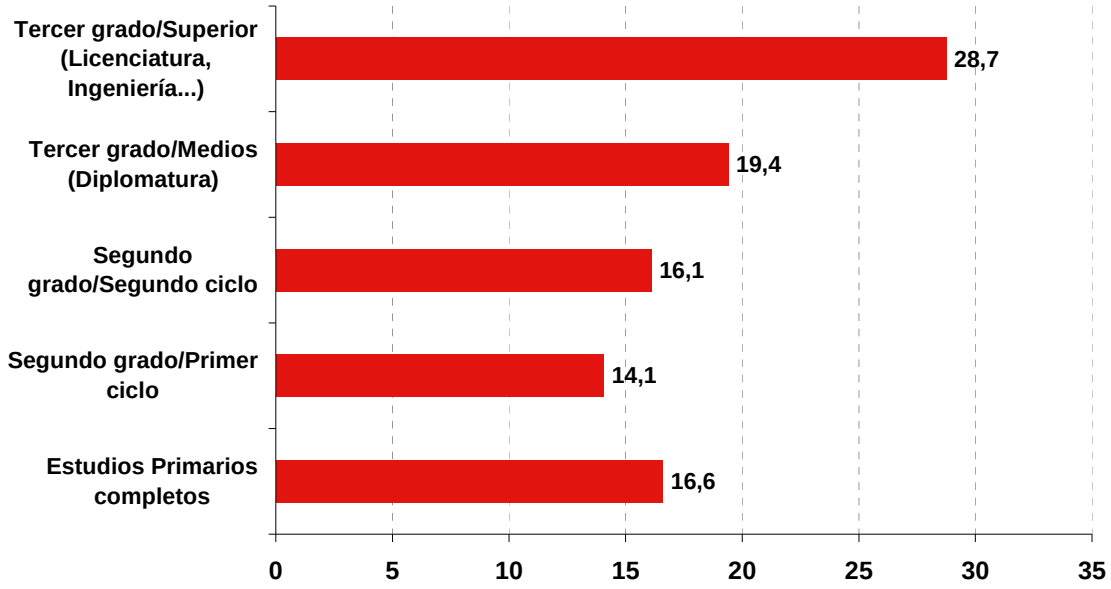
Gráfico 7: Segmentación por edad de los usuarios de redes sociales en España (junio 2008)



Fuente: INTECO

Por otro lado, respecto al nivel de estudios, se constata que el uso de las redes sociales en España se incrementa a medida que lo hace la formación académica de los usuarios (Gráfico 8).

Gráfico 8: Uso de las redes sociales en España según nivel de estudios (junio 2008)

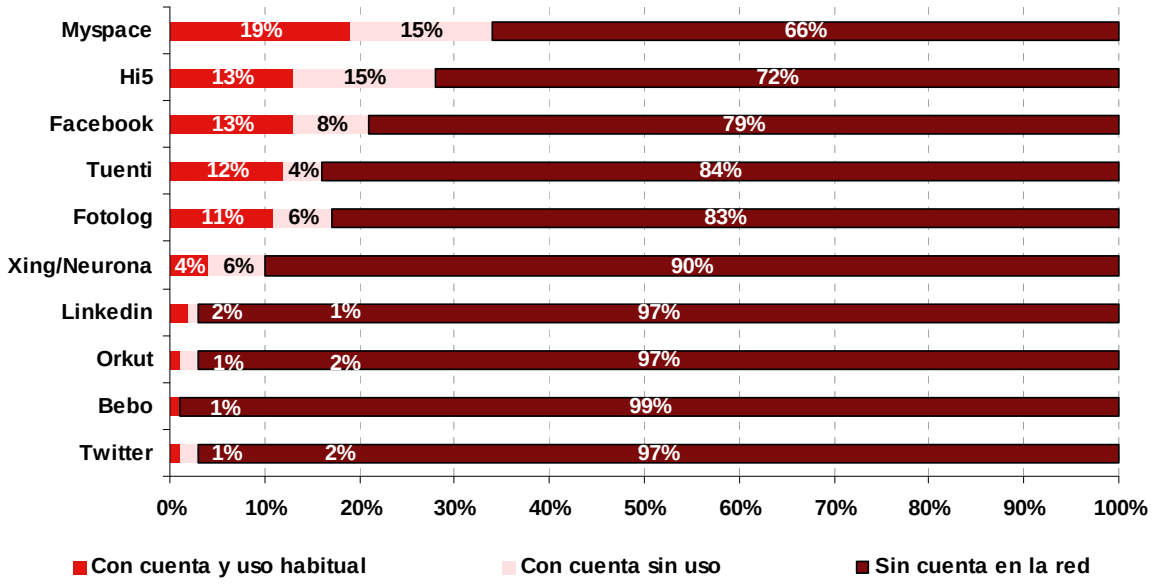


Fuente: INTECO

Overview"). El dato que INTECO ofrece en el caso de España es que el 36,5%de los usuarios de redes sociales son jóvenes entre 15 y 24 años.

Además, como muestra el Gráfico 9 y a diferencia de otros países, en España existen una serie de redes sociales nacionales, entre las que destaca Tuenti, con gran penetración para el total del los usuarios e incluso con niveles de popularidad cercanos a los de redes sociales internacionales como MySpace, Hi5 y Facebook.

Gráfico 9: Penetración de las diferentes Redes Sociales en España (Julio 2008)



Fuente: INTECO a partir de Observatorio sobre la Evolución de las redes sociales (The cocktail analysis)

Así, y aunque el fenómeno de las redes sociales ha llegado a España con posterioridad, respecto a otros Estados de nuestro entorno, se aprecia un crecimiento constante desde el año 2007 que incluso ha planteado que se considere que estas plataformas, pasen a ocupar el lugar de otro tipo de herramientas e incluso medios de comunicación para difundir mensajes[37].

El interés por parte de los medios de comunicación y de los usuarios en el fenómeno, ha contribuido a que en los últimos tiempos otras redes sociales nacionales como Wamba, Moterus o PatataBrava hayan crecido de manera significativa, llegando a ser algunas de ellas mayoritarias a nivel nacional.

[37] Ejemplo de la influencia que una red social puede llegar a tener en la sociedad, es el movimiento realizado por el ente público Radio Televisión Española y *YouTube España,* creando un micrositio denominado *"Elecciones '08[37]"*. Éste tenía por objeto que los candidatos a la presidencia del Gobierno de España del 2008, fueran preguntados por los votantes, respecto a aquellas cuestiones que más les inquietaban a éstos últimos. La finalidad de toda esta campaña fue acercar a los votantes y a los candidatos por medio de una de la principales plataformas de intercambio de contenidos, pudiéndoles plantear situaciones y preguntas para que, tras ser seleccionadas las mejores de ellas, los candidatos, sin disponer de un guión de por medio, contestaran a las mismas con la mayor sinceridad posible. De ésta forma, se dotó de un mayor interés a la participación de aquellos usuarios que subían sus videos de preguntas y de mayor transparencia a las respuestas dadas por los candidatos usando las herramientas de una red social de intercambio de videos.

Visto lo anterior, cabe señalar a modo de conclusión, que en esta primera fase el esfuerzo que realizan las redes sociales y sitios web colaborativos se centra en emprender acciones encaminadas a aumentar el número de miembros de la red social y a que todos ellos se consoliden mediante la participación activa y continuada de sus perfiles de manera que estos se encuentren permanentemente actualizados.

Fase II: Explotación y monetización de la red social online

En el momento en el que la red social cuenta con un número suficiente de usuarios y perfiles actualizados, la plataforma inicia una segunda fase en la que procede a su explotación y monetización. Actualmente se están planteando debates de interés entre los profesionales del sector acerca de cuál es el modelo de explotación más rentable para este tipo de redes.

El Gráfico 10 recoge las variables económicas del modelo de negocio sobre las que hoy en día se asienta la explotación y monetización de las redes sociales y que se describen previamente:

- Publicidad: que puede estar basada en el comportamiento de los usuarios dentro de la plataforma (supone la principal fuente de ingresos).

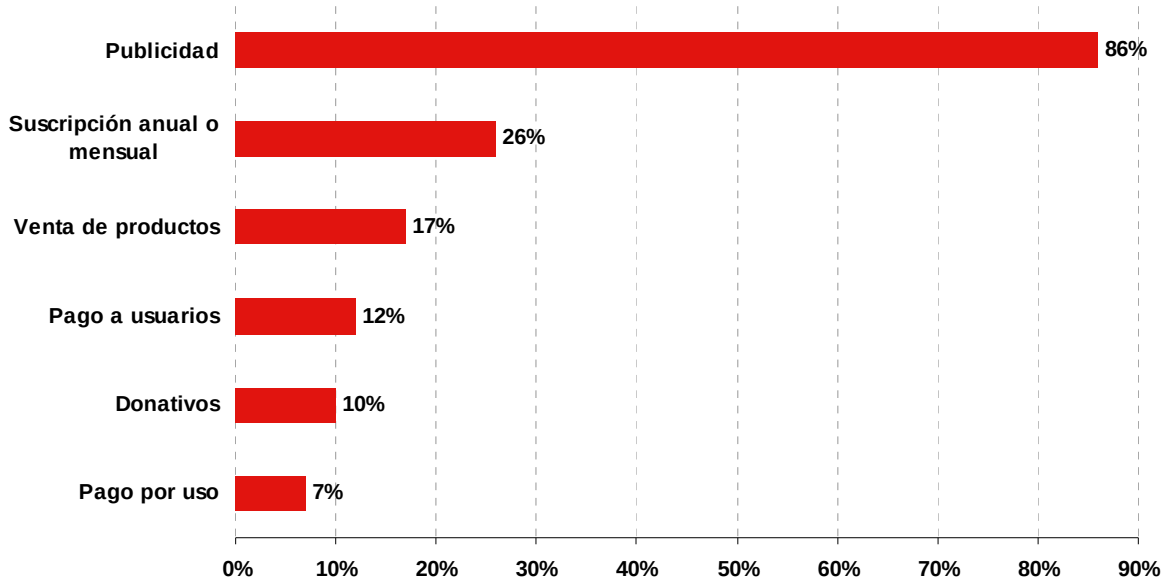
- Suscripciones *premium:* la plataforma tiene dos tipos de contenidos, para una versión más completa, más avanzada o con más aplicaciones, el usuario se tiene que suscribir a las opciones de pago.

- Donativos: los usuarios, de forma espontánea, realizan donativos por medio de instrumentos similares al servicio de *Paypal*[38] para el mantenimiento de la plataforma.

- Pago por uso: cuando el usuario quiera acceder a determinadas herramientas tendrá que pagar por su uso, mediante mensajes sms de móvil o servicios PayPal.

[38] PayPal es una empresa perteneciente al sector del comercio electrónico por Internet que permite la transferencia de dinero entre usuarios que tengan correo electrónico, una alternativa al tradicional método en papel como los cheques o giros postales. PayPal también procesa peticiones de pago en comercio electrónico y otros servicios webs, por los que factura un porcentaje. La mayor parte de su clientela proviene del sitio de subastas en línea eBay.

Gráfico 10: Sistemas de monetización en las redes sociales y de la web 2.0 (Sept 2008)



Fuente: INTECO a partir de Multiplica.com

Sin embargo, y al ritmo al que avanzan las nuevas tecnologías y los servicios prestados a través de Internet así como las demandas de los usuarios; estos medios de explotación se están demostrando insuficientes, o al menos no plenamente garantizadores de una estabilidad a largo plazo. Por este motivo, y a pesar de que se estima que actualmente el valor de *Facebook* se sitúa en los 15.000 millones de dólares,[39] son las inversiones de grandes corporaciones de capital riesgo, las que se encargan de mantener económicamente la infraestructura hasta el momento en el que se alcance la fórmula ideal de monetización.

En este sentido, las empresas y organizaciones titulares de estas plataformas continúan trabajando en el análisis estratégico de los modelos de rentabilización de las redes sociales, ya que esperan recibir una tasa de retorno de las inversiones que maximice los costes asumidos en la creación y puesta en funcionamiento de las plataformas.

Dentro de los cambios más significativos que están aplicando las grandes redes sociales se encuentra el hecho de que están cambiando el modelo de plataformas cuyo software se encontraba completamente cerrado para evolucionar hacia modelos en los cuales los usuarios también colaboran en el desarrollo, la ampliación y la mejora de la propia

[39] Es innegable el verdadero interés que las grandes corporaciones de Internet y dedicadas a la comunicación, muestran por las redes sociales y las plataformas colaborativas como muestra la *lucha titánica* que se está llevando a cabo por Facebook desde que en el año 2006 Yahoo intentara comprarla y hasta que, en el año 2008, Microsoft adquiriera un 1,6% de sus accionariado, haciendo subir el valor de Facebook hasta los 15.000 millones de dólares.

plataforma, programando a partir de la API ("*aplicación programming interface*") hecha pública por la red social en cuestión.

Este trabajo colaborativo de algunos usuarios resulta especialmente relevante, ya que ha permitido que las redes sociales, entendidas tanto desde el punto de vista de la comunidad de usuarios como desde el punto de vista más estrictamente empresarial, hayan llegado a contar con aplicaciones informáticas muy valoradas y ventajosas, tanto por su utilidad de cara al usuario final como por el ahorro en costes para las organizaciones titulares de las mismas-[40].

Este modelo de generación y crecimiento presenta importantes beneficios:[41]

- Ausencia de gastos iniciales de producción.
- Configuración ad-hoc de la red social: son los propios usuarios los que configuran la plataforma a su gusto y desarrollan aplicaciones realmente útiles para el desarrollo de su identidad digital.
- Implicación plena de los usuarios en la red social, lo que conlleva una plena identificación del usuario con la red en cuestión, llegando a considerar a la plataforma como un desarrollo propio y personal.

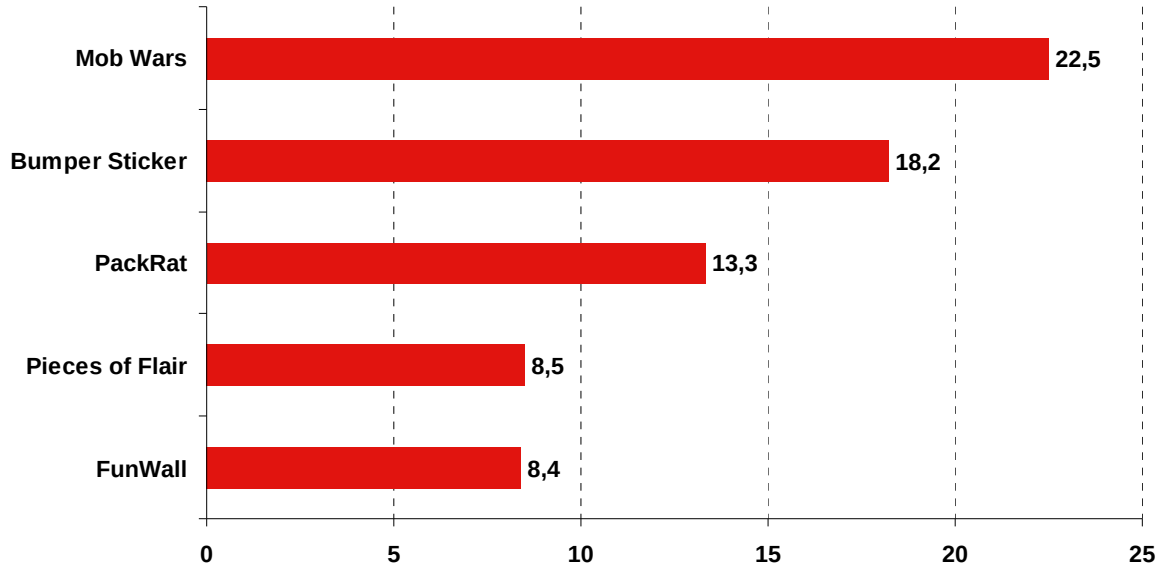
[40] Así por ejemplo en el caso de *Second Life* o de *World of Warcraft* –juego online- han llegado a realizar subastas a través de *eBay* para comprar dinero u objetos pertenecientes al mundo online y que nada tienen que ver con el mundo real.

[41] Este modelo ha sido recientemente presentado por Google, mediante su plataforma *OpenSocial*, fundamentándose esencialmente en la puesta a disposición de toda la comunidad de usuarios de Internet del código abierto de la plataforma mediante su API. En este modelo, es la comunidad la que desarrolla por completo la plataforma a su modelo y semejanza, previendo todas las necesidades que, como usuarios, consideran esenciales para el correcto funcionamiento de la aplicación. Este movimiento estratégico, nace de la alianza entre las principales redes sociales del mundo (*Orkut*[41], *Bebo*[41], *Engage.com*[41], *Friendster*[41], *Hi5*[41], *imeem*[41], *LinkedIn*, *Ning*, *Plaxo*, *Six Apart*, *Tianji*, *Viadeo* y *Xing*), como medio para lograr la definición de herramientas comunes para desarrollar aplicaciones que sirvan en todas las redes sociales, es decir, para el desarrollo de aplicaciones interoperables entre las distintas plataformas. Este hecho supone una línea paralela a la seguida en el sector del software de consumo, donde cada vez más, la colaboración de la comunidad en el desarrollo y los lenguajes abiertos de programación (Software Libre), se han instaurado en los equipos personales de los usuarios. Con *OpenSocial*, se busca ayudar a los desarrolladores de software y aplicaciones de redes sociales a transformar sus ideas en rédito económico. De tal forma, en noviembre de 2007 el anuncio de lanzamiento de esta plataforma se dirigió en un primer momento sólo a desarrolladores de software (siendo la intención de Google la de convertirse en el estándar de los desarrolladores de aplicaciones para redes sociales). En los primeros momentos, y tal y como era de esperar, tras el lanzamiento de *OpenSocial* se descubrieron sus primeros fallos de seguridad, sufriendo su primer crackeo el 5 de noviembre de 2007, produciendo gravísimos daños a la red social propiedad de Google, Orkut, única red en la que operaba en ese momento *OpenSocial*. Después de los primeros errores iniciales, por otro lado, lógicos y evidentes dada la complejidad del desarrollo, en la actualidad *OpenSocial* se describe como la alternativa a *Facebook*.

- Garantiza la interoperabilidad de las diferentes plataformas, permitiendo al usuario la actualización centralizada de su perfil, que se actualiza automáticamente en las plataformas en las que disponga de usuario registrado.

Además del trabajo colaborativo de los usuarios miembros de las plataformas, otra variable que evidencia el cambio en el modelo de negocio actual de las redes sociales está en el potencial de sus aplicaciones. Ejemplo de ello es la conocida como *"Gift"* (regalo) de Facebook, que permite a los usuarios realizar regalos a otros miembros por una cantidad económica que es recaudada por la empresa propietaria de la plataforma. La citada aplicación produce para la plataforma, según la consultora independiente Lightspeed Venture Partners,[42] cerca de 15 millones de dólares al año. El Gráfico 11 recoge los ingresos diarios de otras aplicaciones.

Gráfico 11: Ganancias diarias en miles de dólares por aplicaciones internas de Facebook



Fuente: INTECO a partir de developerAnalitycs.com (Agosto 2008)

Modelo futuro de negocio y estrategia de las redes sociales

El modelo de negocio futuro pasa por ofrecer un servicio, sobre el que, tanto la red social, como los propios usuarios, construyan servicios adicionales capaces de producir beneficios económicos en relación al número de usuarios que los utilizan. El principal reto está en que las redes sociales alcancen ingresos proporcionales al crecimiento del número de usuarios de que disponen.

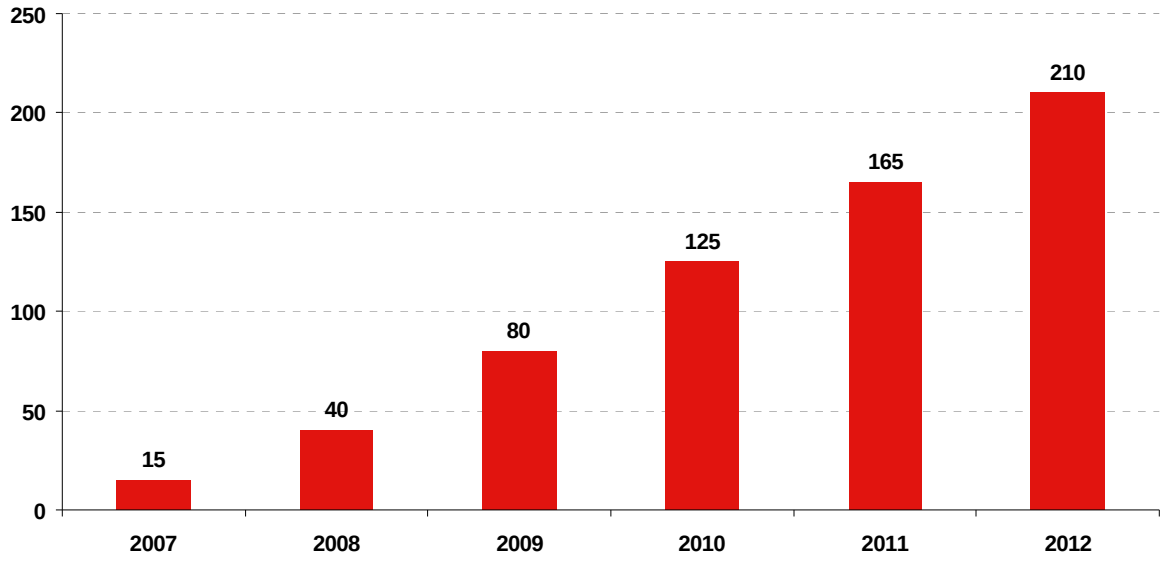
En este sentido, se enumeran a continuación las principales tendencias de futuro que han sido consideradas durante la fase de investigación del Estudio como alternativas válidas

[42] Más información de esta compañía en http://lsvp.wordpress.com/about/.

para la construcción del modelo futuro de negocio de las redes sociales y sitios web colaborativos, considerando de antemano que de igual manera, y por analogía, les serán de aplicación las tendencias previstas para la Web 2.0[43] como servicios avanzados e integrados en esta.

Crecimiento de la publicidad y el marketing online. El auge de la publicidad en Internet continúa en aumento. El Gráfico 12 muestra la previsión del mercado estadounidense de publicidad B2B[44] en las redes sociales, para el 2008, que será de 40 millones de dólares, aumentando hasta 210 millones de dólares en el año 2012.

Gráfico 12: Previsión del volumen de negocio publicitario online entre Empresarios (B2B) entre el 2007 y 2012 en millones de dólares



Fuente: IINTECO a partir de E-Market

Las propias redes sociales y plataformas análogas colaborarán activamente en las campañas publicitarias de las agencias interactivas alojadas en sus portales. De igual forma, éstas percibirán que los anuncios publicitarios o *banners* se verán desplazados y sustituidos por nuevas aplicaciones publicitarias que impliquen en mayor medida a los usuarios finales a interactuar con ellas de forma más activa y efectiva.

En este contexto, las redes sociales pretenden ampliar este potencial de generación de ingresos mediante:

[43] La Web 2.0 y sus modelos de negocio. Estudio comparativo sobre las fuentes reingreso y los modelos de negocio de las 100 webs 2.0 más importantes (multiplica[x])

[44] Abstracción de Business to Business que significa entre empresas.

- El análisis del comportamiento de los usuarios, identificando subsegmentos de mercado a partir de las necesidades y preferencias personalizadas de los mismos.

- La creación de mercados online internos en los que los usuarios puedan participar activamente en transacciones económicas.

- La explotación publicitaria y promocional de los perfiles de los usuarios mediante acuerdos comerciales con marcas y empresas externas.

En función de este modelo de negocio, la posibilidad de monetización de una red social estará determinada por la existencia y consolidación de tres capacidades:

- La capacidad de análisis de las necesidades y preferencias de sus usuarios.

- La capacidad de ofertar nuevos servicios de interés.

- La capacidad de incrementar y fidelizar el número de miembros activos y recurrentes que participa en la red social.

Oferta fragmentada de aplicaciones propias de la red social ejecutadas a través de la misma plataforma. Aumento de la oferta y desarrollo de nuevas aplicaciones y funcionalidades segmentadas, conforme a colectivos más concretos y fragmentados.

Aumento del nivel de captación de masa crítica. Numerosos sitios web (*MySpace*, *Facebook*, *Xing* o cualquiera de las demás redes sociales o webs colaborativas detectadas) son elementos claves de la "cultura 2.0". Este tipo de herramientas busca una captación masiva de usuarios para disponer de masa crítica con la que lograr el máximo ratio de monetización (*"a mayor número de usuarios recurrentes, mayor valor de la plataforma").*

Potenciar y rentabilizar el valor añadido del conocimiento colectivo. Emplear el conocimiento colectivo que sustenta el fundamento de las redes sociales para personalizar y realizar propuestas más idóneas a los usuarios[45].

Atendiendo a los gustos, necesidades y preferencias del usuario, la red social le dirigirá una serie de mensajes personalizados, conocidos como mensajes contextualizados, según su tipo de navegación. Línea de tendencias tecnológicas en las redes sociales y sitios webs colaborativos.

Las tecnologías móviles se vislumbran como nuevo canal de acceso. La web 2.0, y por analogía las redes sociales y plataformas análogas apostarán por el éxito de las

[45] Ejemplo de esta lógica fue aplicada por el sitio web Amazon para recomendar libros de texto a partir de la compra de estos por otros usuarios.

tecnologías móviles y la difusión de la conectividad a Internet sin cables, logrando con ello que el número de accesos y de actualizaciones de los perfiles de los usuarios alcance límites cercanos al tiempo real.

Interoperabilidad de las redes sociales. Aumento y desarrollo de herramientas que permitan a los usuarios prescindir por completo de aplicaciones locales (instaladas en sus equipos informáticos) utilizadas para comunicarse con sus contactos, pasando a realizar dichas comunicaciones directamente a través de la propia red social.

Este tipo de aplicaciones, a diferencia de la creación de la plataforma inicial sobre la que se encuentra montada la red social, serán diseñadas y desarrolladas por los propios usuarios de la red, empleando lenguajes de programación capaces de ser ejecutados en otro tipo de plataformas, pudiendo afirmar que la tendencia será lograr que las redes sociales sean interoperables entre sí[46].

Dispositivos multimedia y geoposicionamiento. Por otro lado, y según el reciente estudio "España 2008" publicado por la Fundación Orange, el avance y evolución de los sistemas de conexión móvil de nueva generación (3G y 4G), así como la aparición de nuevos dispositivos móviles cada vez con más elementos multimedia, provocan que las redes sociales y sus usuarios comiencen a desarrollar aplicaciones que permiten el acceso y actualización de los perfiles de usuarios desde cualquier parte y con una simple conexión a Internet, sin que ni siquiera fuera necesaria una conexión de alta velocidad.

Según un reciente estudio publicado por la consultora tecnológica ABI Research (01/08/2008), las Tecnologías de la Información móviles y las redes sociales, así como las plataformas de contenidos multimedia, experimentarán en los próximos años un crecimiento que supondrá unos beneficios de 3,3 billones de dólares para el año 2013[47].

Soluciones de seguridad informática. La oferta de servicios y soluciones de seguridad informática para los usuarios de redes sociales se vislumbra como otra posible fuente de oportunidades de negocio. El crecimiento de estas plataformas facilitaría el nacimiento de iniciativas bien dedicadas al desarrollo del software para garantizar la seguridad informática de las redes sociales o bien enfocadas en la creación de programas para proteger la intimidad, privacidad y datos personales de sus usuarios, especialmente de menores[48].

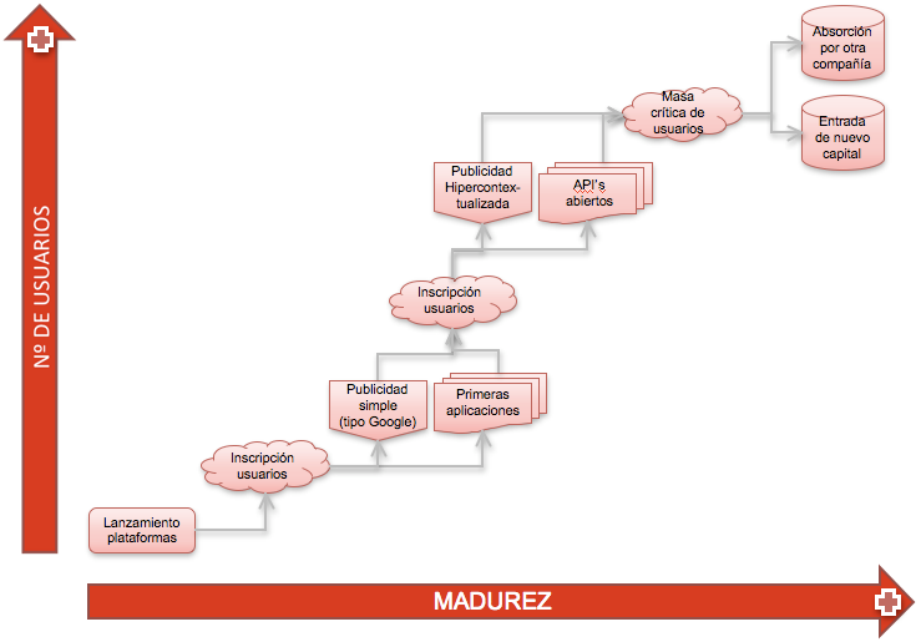
A modo de resumen visual, el Gráfico 13 recoge el que podría considerarse como modelo estándar de crecimiento de una red social.

[46] Ejemplo de esta tendencia es la plataforma creada por Google, Open Social.

[47] Para más información visite el sitio web de ABI Research.

[48] Más información: Libro blanco de los contenidos digitales en España 2008. Red.es

Gráfico 13: Modelo de crecimiento de las redes sociales

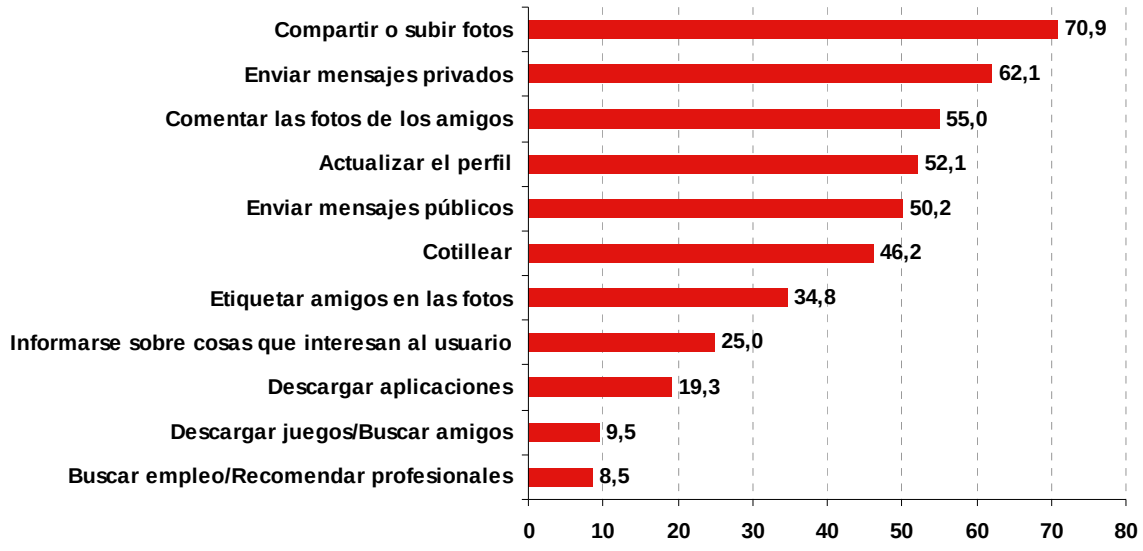


Fuente: INTECO

2.4 Riesgos de las redes sociales

Las redes sociales ofrecen múltiples funcionalidades. Entre ellas, las más usadas, tal y como se muestra en el Gráfico 14 están el compartir y subir fotos (usadas por un 70,9% de los usuarios), seguido del envío de mensajes privados con un 62,1%.

Gráfico 14: Usos de las redes sociales por los usuarios españoles (%). Octubre 2008



Fuente: INTECO a partir de Zed Digital

Sin embargo, a pesar de las oportunidades y ventajas de estas funcionalidades, conviene señalar que, este tipo de plataformas, no se encuentran exentas de ***riesgos*** tal y como se explica a continuación.

Las redes sociales generalistas o de ocio cuentan con un nivel de riesgo superior al de las redes sociales profesionales, dado que los usuarios exponen no sólo sus datos de contacto o información profesional (formación, experiencia laboral), sino que se pueden exponer de manera pública las vivencias, gustos, ideología y experiencias del usuario, lo que conlleva que el número de datos de carácter personal puestos a disposición del público es mayor que en las redes sociales de tipo profesional. Asimismo, se tratan datos especialmente protegidos, lo que supone un mayor nivel de riesgo para la protección de dichos datos personales y, por ende, del ámbito de la privacidad e intimidad de los usuarios.

Entre las principales situaciones, cabe señalar que:

- Existe un problema derivado de la falta de toma de conciencia real por parte de los usuarios de que sus datos personales serán accesibles por cualquier persona y del valor que éstos pueden llegar a alcanzar en el mercado. En muchos casos, los usuarios hacen completamente públicos datos y características personales que en ningún caso expondrían en la vida cotidiana como ideología, orientación sexual y religiosa, etc.

- Los datos personales pueden ser utilizados por terceros usuarios malintencionados de forma ilícita.

- Existe la posibilidad de que traten y publiquen en la Red información falsa o sin autorización del usuario, generando situaciones jurídicas perseguibles que pueden llegar a derivarse de este hecho[49].

- El hecho de que, a través de las condiciones de registro aceptadas por los usuarios, éstos cedan derechos plenos e ilimitados sobre todos aquellos contenidos propios que alojen en la plataforma, de manera que pueden ser explotados económicamente por parte de la red social[50].

Por todo ello, y a pesar de que las redes sociales descritas anteriormente cuentan con una infinidad de beneficios para sus usuarios, éstos no deben obviar el hecho de que se

[49] Ejemplo de este supuesto lo constituye la implicación en delitos de estafa online, como el *"Phishing Car",* donde los estafadores utilizan perfiles de cierto renombre en la Red, para otorgar una mayor entidad y credibilidad al negocio ficticio.

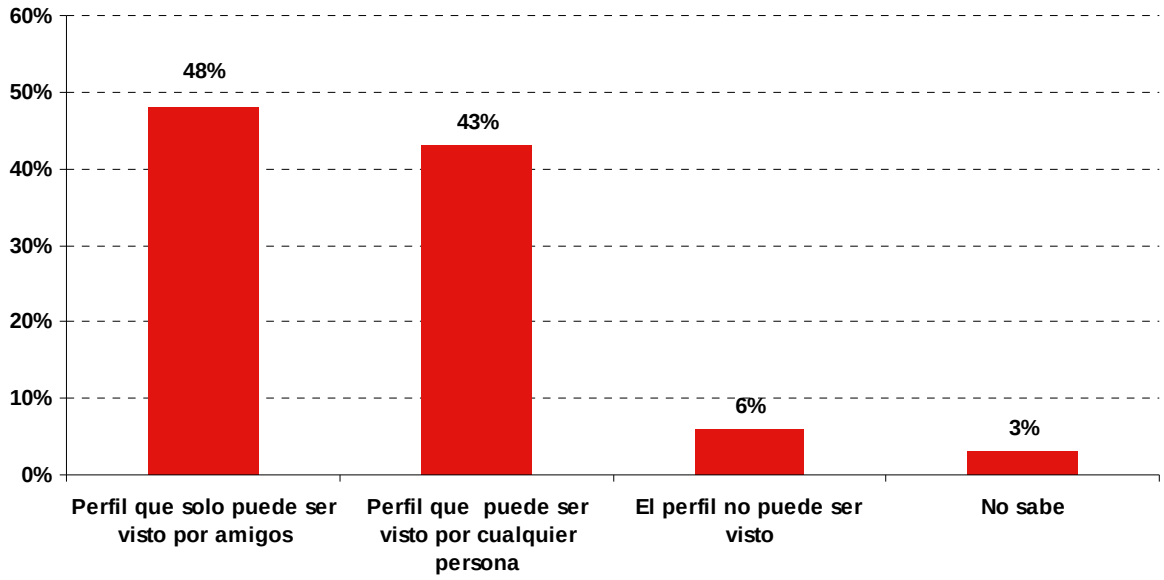
Más información en http://www.legaltoday.com/index.php/actualidad/noticias/phishing-una-alarma-constante.

[50] En este sentido, una de las polémicas más relevantes fue la ocurrida en el año 2006 con el grupo musical *"Artic Monkeys",* que estuvo al borde de perder los derechos sobre sus propias canciones, al haberlas alojado en una importante red social para darse a conocer en sus comienzos.

trata de herramientas públicas y accesibles para cualquier tipo de persona, con independencia de que las intenciones con las que se accede sean negativas o ilícitas.

De hecho, es habitual que los usuarios de redes sociales no sean conscientes o descuiden la privacidad de sus perfiles. Así, como se muestra en el Gráfico 15, en el reciente Estudio "Redes Sociales Análisis cuantitativo y cualitativo sobre hábitos, usos y actuaciones" publicado por Ofcom (Office of Communications) se afirma que casi la mitad de los usuarios de redes sociales analizados (43%) tienen su perfil de usuario sin restricciones de privacidad y disponible para que pueda ser visitado por cualquier otro usuario.

Gráfico 15: Tipo de configuración de perfil aplicado por los usuarios de redes sociales respecto de su visibilidad y nivel de seguridad (octubre-diciembre 2007)



Fuente: INTECO a partir de Ofcom. Office of Communications

En otro orden de cosas, un hecho añadido que debe considerarse de forma destacada en el análisis de los posibles peligros de las redes sociales generales y de ocio es la frecuente participación del colectivo de menores de edad, como se vio anteriormente, (Gráfico 7).

El uso de las redes sociales por parte de los menores de edad se está convirtiendo en una actividad habitual para el desarrollo social de los jóvenes. Esta actividad reporta grandes ventajas para los menores, al ofrecerles acceso a un nuevo medio de comunicación y relación social, que les permite, de forma descentralizada, crear y mantener tanto el contacto directo con sus amigos y conocidos como una nueva forma de

identidad digital[51]. Sin embargo, y como se señala en el Estudio "Redes Sociales Análisis cuantitativo y cualitativo sobre hábitos, usos y actuaciones" publicado por Ofcom (Office of Communications) el 2 de abril de 2008, los menores a pesar de tener ciertas nociones de seguridad descuidan ciertos aspectos y en ocasiones no otorgan la importancia que se merece a los datos personales.

En este sentido, el capítulo 3 analiza en profundidad las especialidades que se establecen en la normativa española respecto de los colectivos considerados especialmente vulnerables.

En efecto, basta con atender a los datos expuestos en este informe para darse cuenta de que el crecimiento de las redes sociales en el último año ha sido realmente imparable. Ha sido hasta el momento un crecimiento positivo, sin grandes ni numerosos casos que hayan supuesto un riesgo o peligro para los usuarios. No obstante, los riesgos son constatables y cada vez más frecuentes en este tipo de plataformas.

Al tiempo que el número de usuarios de redes sociales aumenta, los casos en los que sus datos son utilizados para finalidades ilegítimas y los usuarios son víctimas de casos de fraudes o incluso de secuestros o delitos semejantes aumentan.

Recientemente, la compañía ScanSafe, consultora en seguridad web, ha publicado un estudio[52] en el que pone de manifiesto que, tras el análisis de más de cinco mil millones de peticiones de páginas web realizadas en julio de 2006, más de 600 páginas webs consideradas redes sociales, incluían algún tipo de código malicioso (malware).

La mayor parte del código malicioso identificado se encuentra dentro de los considerados como programas espía (spyware) y adware (publicidad en formato de ventana emergente, generalmente), encontrándose adherido a aplicaciones internas ejecutadas desde los navegadores de los usuarios.

La mayor parte del código malicioso identificado por ScanSafe, han sido programas espía y adware acoplado a programas benignos, pero que pueden afectar seriamente la experiencia de un usuario en Internet, por ejemplo redireccionando el navegador. Sin olvidar que además su eliminación suele ser una tarea difícil.

[51] Según la consultora especializada en usabilidad Evolucy Technology Consulting S.L, (www.evolucy.com) *"por definición, identidad es aquel conjunto de rasgos propios de un individuo o colectividad que los caracterizan frente a los demás. La verificación de estos rasgos es lo que nos permite determinar que un individuo es quien dice ser. Algunos de estos rasgos son propios del individuo, otros son adquiridos con el tiempo. Por supuesto, no todos los rasgos son igualmente apreciables. Hay rasgos que son apreciables a simple vista, mientras que otros están ocultos y es necesario un conocimiento y, en ocasiones, herramientas para poder verificarlos. Al conjunto de rasgos que caracterizan a un individuo o colectivo en un medio de transmisión digital se le conoce como Identidad Digital."*

[52] Más información en http://www.scansafe.com/.

De igual forma, el informe constata el hecho de que la mayor parte de las redes sociales que contenían este tipo de *"software maligno"* eran redes sociales consideradas generalistas o de ocio, dejando constancia expresa en el informe de que las redes sociales profesionales no muestran software maligno que pueda afectar la seguridad de los usuarios.

Desde el punto de vista práctico parece razonable que los objetivos principales de los delincuentes informáticos sean las redes sociales de carácter generalista o de ocio, dado que éstas cuentan con un número de usuarios más elevado que las redes profesionales[53].

Los posibles peligros asociados a las redes sociales de contenido profesional están especialmente relacionados con la protección de datos de carácter personal, puesto que los usuarios publican datos personales en la plataforma, que pueden animar la proliferación de los denominados *"coleccionistas de contactos"* o *"social spammers"*, dedicados a recabar contactos disponibles en las redes sociales, en principio sin otra finalidad que la de figurar como usuarios con más contactos en dicha red social.

Esta forma de actuar puede no parecer, a priori, dañina para los usuarios ni para la propia red social, sin embargo ese tipo de actuación supuso un grave problema para una de las más importantes redes sociales profesionales del mundo (Linkedin), que desembocó en que la empresa propietaria de la plataforma tuviera que cambiar completamente el modo de interrelación entre los diferentes usuarios, exigiendo para poder realizar contactos directos, que previamente ambos usuarios hubieran aceptado la existencia de una *relación de confianza mutua*[54], lo que no era inicialmente un requisito, puesto que pretendían la puesta en contacto del mayor número de profesionales posible.

[53] Según información oficial publicada por Facebook, el número actual de usuarios alcanza los 110 millones, mientras que la red social profesional Xing cuenta en la actualidad de algo más de 500.000 usuarios.

[54] Más información en: http://www.ejournal.unam.mx/rms/2005-1/RMS005000104.pdf

3 ANÁLISIS DE LOS ASPECTOS MÁS RELEVANTES Y PROBLEMÁTICA ESPECÍFICA DE LAS REDES SOCIALES

La tendencia actual de los servicios que la Red pone al alcance del usuario -foros, blogs, wikis o redes sociales- se construye a partir de un nexo común que tiene en su base la *actividad colaborativa*, a la vez que los cambios tecnológicos y sociales han contribuido a la implantación y crecimiento popular de esta nueva forma de creación, colaboración y acceso a la información.

Pero la notoriedad de estos espacios sociales no queda exenta de riesgos o posibles ataques malintencionados. En este sentido, debe subrayarse el carácter pionero y la importancia del artículo 18.4 de la Constitución Española al prever la necesidad de que el legislador regule aquellos usos de la informática susceptibles de repercutir en los derechos fundamentales. Asimismo, la aprobación del Convenio 108 de 1981 del Consejo de Europa, el conjunto de normas dictadas por las Comunidades Europeas en materia de protección de datos, sociedad de la información o propiedad intelectual, y las normas españolas que las desarrollan definen un horizonte normativo cuya proyección sobre la Web. 2.0 y las redes sociales resulta fundamental analizar.

Partiendo de esas premisas, este capítulo ofrece un ***análisis en profundidad sobre las cuestiones más relevantes que afectan directamente a las redes sociales*** y sitios web colaborativos, de forma que tanto las propias plataformas, como los usuarios de éstas, cuenten con información clara respecto de sus derechos y obligaciones.

El criterio seleccionado para el análisis, desde un punto de vista normativo, es el de los derechos constitucionales concernidos, abordando su examen en función del orden de enunciación que la propia Constitución Española (CE) de 1978 establece para cada uno de estos bienes, derechos y libertades de los ciudadanos:

- La protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- El secreto de las comunicaciones.
- La protección de datos de carácter personal.
- La protección de la producción y creación literaria, artística, científica y técnica mediante los instrumentos reguladores de la propiedad Intelectual e Industrial de las Obras.
- La protección de los derechos de consumidores y usuarios.

El análisis en profundidad de cada derecho atiende a un planteamiento metodológico estructurado de la siguiente forma:

- Definición del derecho.
- Marco jurídico aplicable: normativa y evolución legislativa.
  - Normativa internacional[55].
  - Normativa europea.
  - Normativa nacional.
- Posibles riesgos a los que puede verse sometido el derecho.
- Colectivos especialmente vulnerables: menores de edad e incapaces.
- Otros supuestos: trabajadores.
- Medidas empleadas para salvaguardar el derecho: posicionamiento de los diferentes actores que intervienen en la cadena de valor.

3.1 Protección del Derecho al honor, a la Intimidad Personal y Familiar y a la Propia Imagen

El **artículo 18 de la Constitución Española** se ordena a la protección de distintos bienes de la personalidad siendo su objeto garantizar una esfera de libertad individual que protege por una lado la vida privada de las personas y les otorga, de otro, facultades que permiten ejercer un control material sobre el tratamiento de su información personal. En el precepto conviven manifestaciones clásicas de los derechos de la personalidad, -*derechos al honor, a la intimidad personal y familiar y a la propia imagen*-, una esfera de protección frente a las injerencias en ámbitos específicos, -*inviolabilidad del domicilio y secreto de las comunicaciones*-, y un derecho de última generación definido por el Tribunal Constitucional *como derecho fundamental a la protección de datos*. Las tecnologías de la información no sólo se proyectan sobre el último derecho citado, sino que afectan también a la conformación constitucional de las dos primeras categorías.

Los derechos fundamentales establecidos por el artículo 18 CE, no son absolutos, de modo que pueden ser limitados por otros bienes o derechos constitucionalmente relevantes cuando se cumplan las condiciones que define la propia Constitución, esto es

[55] Dentro del presente estudio de la normativa internacional también se incluirá la normativa estadounidense, ya que el mayor número de redes sociales y de usuarios de estas se encuentran nacionalizadas en Estados Unidos. Además desde los atentados del 11 de septiembre su normativa se está centrando en las comunicaciones vía Internet así como, en la defensa de los menores.

que se establezcan mediante ley, que en todo caso respetará su contenido esencial, y se den condiciones de proporcionalidad en la adopción de las medidas limitadoras que se adopten. Ello, sin perjuicio de que en caso de conflicto con otros bienes y/o derechos constitucionales deban ceder ante otros intereses dignos de protección.

Estos derechos han sido desarrollados en el ámbito civil, penal y procesal, por leyes con contenidos y objetivos muy diversos, así como por leyes de desarrollo específico y singular, -como la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal-, conformando un complejo entramado normativo. De este modo, basta con considerar los contenidos y servicios existentes en las redes sociales para preguntarse de qué modo estas normas se proyectarán sobre las mismas y sobre la actividad de los usuarios.

3.1.1 Definición del derecho

La definición del bien jurídico protegido en el artículo 18 CE resulta particularmente complicada habida cuenta de su complejidad estructural y de la influencia que sobre el ejercen los usos de las tecnologías de la información y las comunicaciones. En este sentido, y por razones puramente pedagógicas debería decirse que el conjunto del artículo 18 se ordena a la protección de la vida privada, como manifestación de la personalidad del individuo ligada a la protección de la dignidad y libertad del ser humano[56]. Son derechos que se integran en la categoría de los derechos de la personalidad, su titularidad, -salvo excepciones-, se atribuye únicamente a personas físicas, y se caracteriza por las notas de irrenunciabilidad, intransmisibilidad, imprescriptibilidad, inalienabilidad e inembargabilidad.

La vida privada se manifiesta de modo individualizado a través de distintos derechos. En primer lugar, el artículo 18.1 CE establece los derechos al honor, la intimidad personal y familiar y a la propia imagen. La jurisprudencia ha subrayado que si bien tales derechos poseen un mismo fin deben ser considerados independientes aunque profundamente interrelacionados[57]. El nexo entre estos derechos, e incluso con la inviolabilidad del domicilio, el secreto de las comunicaciones y el derecho fundamental a la protección de

[56] "Junto al valor de la vida humana y sustancialmente relacionado con la dimensión moral de ésta, nuestra Constitución ha elevado también a valor jurídico fundamental la dignidad de la persona, que, sin perjuicio de los derechos que le son inherentes, se halla íntimamente vinculada con el libre desarrollo de la personalidad (art. 10) y los derechos a la integridad física y moral (art. 15), a la libertad de ideas y creencias (art. 16), al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1). Del sentido de estos preceptos puede deducirse que la dignidad es un valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respeto por parte de los demás." (STC 53/1985 FJ núm. 8)

[57] "El derecho a la propia imagen, consagrado en el art. 18. 1 CE junto con los derechos a la intimidad personal y familiar y al honor, contribuye a preservar la dignidad de la persona (art. 10. 1 CE), salvaguardando una esfera de la propia reserva personal, frente a intromisiones de terceros. Sólo adquiere así su pleno sentido cuando se le enmarca en la salvaguardia de «un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" (STC 99/1994).

datos, no es otro que el uso de la información personal. Esta realidad no conlleva obligatoriamente que no puedan ser analizados de forma independiente.

El **derecho al honor** es aquel derecho a la protección de la imagen pública de una persona, -de la consideración social en la que es tenido-, de su nombre y su reputación, de tal forma que el resto de individuos lo respeten durante su vida. Dicha protección, como excepción a lo usual en los derechos de la personalidad, se extiende más allá del fallecimiento por medio de acciones concedidas por el Ordenamiento a sus causahabientes.

El **derecho a la propia imagen** atribuye al individuo la capacidad de ejercer un control sobre la captación, grabación, uso y difusión de su imagen entendida como representación gráfica de la figura humana, y también de su voz. El Tribunal Constitucional cuando se ocupa del derecho a la propia imagen no sólo atiende a los aspectos más concretos y definitorios del mismo, la facultad de consentir en la captación o difusión de imágenes que reproduzcan la figura humana, sino también a la información que éstas revelan y a su directa relación con las intromisiones en la vida privada. De hecho, debe considerarse que es esta relación con la vida privada la que dota de relevancia constitucional a la protección de la imagen y, en su caso, de la voz.

El **derecho a la intimidad** se entendió inicialmente por doctrina y jurisprudencia como un bien ordenado a la protección de lo más interno y reservado de las personas. Posteriormente la jurisprudencia y la evolución social han definido un derecho a la intimidad de contenido amplio y textura abierta cuyas manifestaciones son múltiples. En tal sentido, la relación de la intimidad con la propia imagen, los conflictos que se dan en el caso del ejercicio del derecho a la información y de la libertad de expresión, la práctica de pruebas corporales en el ámbito penal, la protección de la salud y la investigación genética, y la protección de la dimensión familiar han extendido la tutela de este derecho a un ámbito más amplio.

Finalmente, el Tribunal Constitucional ha dotado de autonomía propia al derecho fundamental a la protección de datos, del que se ocupa un epígrafe posterior, configurándolo como un derecho que, si bien guarda una relación instrumental con los derechos del párrafo primero del artículo 18 CE posee una configuración constitucional propia y definida.

Por último, aunque este informe no profundice en esta materia debe señalarse que la tutela constitucional de la vida privada se proyecta sobre otros dos derechos.

En primer lugar, hay que referirse **a la inviolabilidad del domicilio**. En palabras del Tribunal Constitucional *"a través de este derecho no sólo es objeto de protección el espacio físico en si mismo considerado, sino lo que en él hay de emanación de la*

persona y de esfera privada de ella. Interpretada en este sentido la regla de la inviolabilidad del domicilio es de contenido amplio e impone una extensa serie de garantías y de facultades, en las que se comprenden las de vedar toda clase de invasiones incluidas las que puedan realizarse sin penetración directa por medio de aparatos mecánicos, electrónicos u otros análogos. La regla segunda establece un doble condicionamiento a la entrada y al registro, que consiste en el consentimiento del titular o en la resolución judicial"[58]. Debe notarse por tanto, que no se requiere de penetración física en el domicilio y ello debe ponerse en directa relación en el mundo de las redes con la presencia de miles de webcam o de grabaciones de vídeo susceptibles de lesionar este derecho.

La última manifestación fenoménica de la vida privada en sede constitucional es la protección del secreto de las comunicaciones. Este derecho protege tanto el propio hecho de la comunicación como su contenido. Así, *"el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje -con conocimiento o no del mismo- o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo)"*[59].

El secreto del art. 18.3 tiene un carácter "formal", "en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado", opera mediante "la presunción iuris et de iure de que lo comunicado es "secreto", en un sentido sustancial". No obstante, el secreto de las comunicaciones no se proyecta sobre los interlocutores sobre los cuales puede pesar la obligación de no revelar lo comunicado so pena de vulnerar el derecho a la intimidad de alguno de ellos. Otro detalle relevante de la doctrina del Tribunal Constitucional, es que acoge la idea de que cuando se está hablando de tutelar el secreto de las comunicaciones no se prejuzga el concreto medio tecnológico empleado. El Alto Tribunal ha completado su jurisprudencia en las SSTC 70/2002 y 123/2002. En ambas realiza una interpretación del derecho tecnológicamente actualizado entendiendo que tutela frente a las interferencias en todo tipo de comunicación *"cualquiera que sea la técnica de transmisión utilizada" y con independencia del contenido del mensaje: "conversaciones, informaciones, datos, imágenes, votos, etc.".*

---

[58] STC 22/84. FJ 5. Postura que reafirma con toda rotundidad el fundamento jurídico quinto de la STC 50/1995 que afirma:

"*El domicilio, lugar de residencia habitual, según definición legal (art. 40 C.C.), acota el espacio donde el individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales, haciéndolo con la libertad más espontánea (STC 82/1984) y, por ello, su protección tiene un carácter instrumental para la defensa del ámbito en el cual se desarrolla la vida privada. Existe, pues, un nexo indisoluble de tal sacralidad de la sede existencial de la persona, que veda toda intromisión y, en concreto, la entrada y el registro en ella y de ella, con el derecho a la intimidad, por lo demás contenido en el mismo precepto que el otro (art. 18.1 y 2 C.E.)*".

En el mismo sentido véase la STC 133/1995.

[59] STC 114/1984.

Por tanto, el secreto de las comunicaciones se proyectará sobre todos aquellos servicios de las redes sociales que comporten una comunicación interpersonal que excluya a terceros distintos de los interlocutores, como los basados por ejemplo en herramientas de mensajería privada.

Dar traslado y protección eficiente a estos derechos en el ámbito de las redes sociales y, en general, en el de la Sociedad de la Información, conlleva la necesidad de *reinterpretar, adecuar y fortalecer el concepto de protección existente hasta el momento*, en la medida en que las redes sociales fundamentan su contenido principal en el fomento de la publicación de información personal por parte de los usuarios, siendo en muchos casos información perteneciente a la esfera más íntima y personal: ideología, orientación sexual, creencias religiosas, etc.

3.1.2 Marco jurídico aplicable: normativa y evolución legislativa

A continuación, se presenta el análisis normativo y la evolución legislativa del derecho al honor, a la intimidad personal y familiar y a la fropia imagen, haciendo especial hincapié en la protección de este derecho en Internet y en los servicios asociados a ésta.

Para contar con una visión global de la situación se analiza el ámbito internacional, comunitario o europeo y el nacional.

Normativa internacional

La protección de estos derechos no se encuentra restringida a determinados Estados, sino que son reconocidos por la mayor parte de la comunidad internacional, siendo protegidos expresamente en las constituciones y legislaciones nacionales de muchos países.

La **Declaración de Derechos Humanos de 10 de diciembre de 1948** establece la primera fuente normativa respecto a los derechos objeto de este apartado, disponiendo que: *"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"*.

Del mismo modo, aunque de forma específica para los menores de edad, el **Pacto Internacional de Derechos Civiles y Políticos de 19 de diciembre de 1966** y el **Pacto Internacional de Derechos Económicos, Sociales y Culturales de 19 de diciembre de 1966** disponen el derecho de todos los menores a contar con un grado de protección mayor, dadas sus características particulares.

Este reconocimiento normativo en favor de los menores se recoge de forma expresa en el documento aprobado por la **Convención de Derechos del Niño de 20 de noviembre de 1989**, donde se dispone que *"ningún niño será objeto de injerencias arbitrarias o ilegales*

en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación. El niño tiene derecho a la protección de la Ley contra tales injerencias".

Normativa europea

En primer lugar, debe hacerse referencia al Convenio de Roma de 1950 (CEDH)[60] que puede citarse como el primer texto europeo que consagra la tutela de la vida privada y junto con el Convenio núm. 108 del Consejo de Europa define el contexto normativo de la protección de la privacidad en relación con las tecnologías de la información y las comunicaciones. Frente a la escasa virtualidad de otros textos Internacionales el Convenio de 1950 ha resultado particularmente eficaz en el ámbito de la protección de los derechos humanos en aquellos estados que han aceptado ser vinculados por sus mandatos.

La importancia del Convenio para el Ordenamiento jurídico nacional deriva de su doble naturaleza como norma incorporada al Derecho español por la vía prevista del artículo 96 de la Constitución Española y como criterio de interpretación de los derechos fundamentales a la luz de lo dispuesto por el art. 10.2 de la Constitución. Esta doble naturaleza se deja sentir en los efectos de las sentencias emanadas del Tribunal Europeo de Derechos Humanos en aplicación del Convenio ya que, de un lado, producen efectos jurídicos en el ordenamiento interno, y de otro, han venido inspirando la labor del Tribunal Constitucional en la interpretación de los derechos fundamentales.

En el ámbito comunitario, debe tenerse en cuenta lo dispuesto en la **Carta de los Derechos Fundamentales de la Unión Europea**, de 7 de diciembre de 2000 **(2000/C 364/01)**[61] donde se dispone que "*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones*".

De igual forma, en la **Carta Europea de Derechos del Niño (Resolución del Parlamento Europeo A3-0172/92 de 8 de julio de 1992)** se declara que *"Todo niño*

[60] El Convenio de Roma de 1950 regula el derecho a la vida privada en su artículo 8 en los siguientes términos:

Derecho al respeto a la vida privada y familiar

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, sino en tanto en cuanto 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 del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

Convenio de Roma de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Instrumento de Ratificación de 26 de septiembre de 1979.

[61] Publicada en el Diario Oficial de las Comunidades Europeas el 18 de diciembre de 2000.

tiene derecho a no ser objeto por parte de un tercero de intrusiones injustificadas en su vida privada, en la de su familia, ni a sufrir atentados ilegales contra su honor", reconociéndose igualmente el derecho y protección de su imagen.

Debe tenerse en cuenta que las normas comunitarias no suelen referirse exclusivamente a la intimidad o al derecho a la protección de datos, sino que suelen emplear la expresión vida privada en normas que materialmente se ocupan de los datos personales, por lo que se remite a la exposición contenida en el epígrafe 3.2.2.

EE.UU

En EE.UU la protección normativa de la vida privada resulta de una compleja interpretación del Tribunal Supremo que tras una labor de casi medio siglo alumbró el reconocimiento constitucional del derecho a la privacy. Y lo hizo deduciéndolo de "las sombras y penumbras" contenidas en los textos de distintas enmiendas a la Constitución En principio, la Constitución de EEUU no reconoce expresamente el derecho a la intimidad así que este se construye por el Tribunal Supremo deduciéndolo implícitamente a partir de derechos explícitamente reconocidos por el texto constitucional, de su combinación, y de las "penumbras" de los preceptos constitucionales.

En concreto el Tribunal Supremo ha partido del hecho de que la Constitución Norteamericana no contiene una lista cerrada de derechos sino que al contrario la Novena Enmienda se erige en cláusula de apertura a la incorporación de nuevos derechos ya que señala que aunque "la Constitución enumera ciertos derechos" no "ha de entenderse que niega o menosprecia otros que retiene el pueblo". Por otra parte, la Decimocuarta Enmienda ha provisto al Tribunal de un argumento procesal para examinar los casos en los que se planteen cuestiones relativas a la vida privada, ya que concede a los ciudadanos el derecho a no ser privados "de la vida, la libertad o la propiedad sin el debido proceso legal". Así, La Due Process Clause actúa como una cláusula de garantía de la libertad de los ciudadanos frente a los poderes del Estado. Estas dos cláusulas en relación con concretos derechos, -libertad de expresión y participación del pueblo en la Primera enmienda, límites al uso militar de las viviendas privadas en tiempos de paz en la Tercera y protección del domicilio en la Cuarta- han servido para inferir la presencia de la privacy como derecho constitucional.

Debe señalarse que analizar legislativamente la regulación de la vida privada en estados Unidos no es sencillo ya que la consideración normativa del fenómeno se produce de modo parcial en normas estatales y, sobre todo, resulta acogida por normas sectoriales de carácter federal[62].

[62] Pueden citarse, en una lista no exhaustiva, entre otras: Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 (1970). Privacy Act, 5 U.S.C. § 552 (1974). The Freedom of Information Act (FOIA), 5 U.S.C. § 552 (1974).

Del mismo modo, disponen de normativa encargada de velar por la protección de la privacidad e intimidad de los usuarios en situaciones concretas. En este sentido, cabe destacar 2 normas principales:

- **Telecommunications Act** de 1996 *(Ley de Telecomunicaciones, aprobada el 13 de junio de 1996)*. Esta norma regula de forma expresa todos los aspectos relacionados con la publicación en Internet de contenidos violentos y/o pornográficos que puedan dañar la ética y la moral de las personas, estableciendo la protección de los ISP respecto a los contenidos publicados por terceros.

- **Children's Online Privacy Protection Act** de 1998 *(Ley de Privacidad para la Actividad de los Menores en la Red),* donde se establece la regulación específica respecto a aquellos actos encaminados a obtener información o engañar a los menores, cuando éstos se encuentren en el medio online.

En materia de intimidad, es necesario tener en cuenta la denominada *"USA Patriot Act (UPA)"* aprobada el día 24 de octubre de 2001, tras los atentados del 11 de septiembre. Dicha norma supone una clara limitación del derecho a la intimidad personal y familiar y al secreto de las comunicaciones de cualquier persona que se encuentre en los Estados Unidos, dado que el Gobierno Federal cuenta con plenos poderes para intervenir cualquier tipo de comunicación, interna o externa, de correo electrónico, conversación telefónica, ya sean mensajes de voz o texto, los históricos de navegación web, así como de consultas en los principales buscadores de Internet. Todo ello tiene como finalidad aumentar el grado de seguridad del Estado frente a actos de delincuencia organizada y terrorismo.

Normativa nacional

A nivel nacional el reconocimiento normativo del derecho al honor, a la intimidad personal y familiar y a la fropia imagen se consagraba en el **artículo 18.1 CE**.

Posteriormente, mediante **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**, el

Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g et seq. (1974). Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq. (1978). Privacy Protection Act, 42 U.S.C. § 2000aa et seq. (1980). Cable Communications Policy Act 47 U.S.C. § 551 et seq. (1980). Electronic Communications Privacy Act (ECPA), 18 USC §§ 2701-11 (1986). Video Privacy Protection Act, 18 U.S.C. § 2710 (1988). Employee Polygraph Protection Act, 29 U.S.C. § 2001 et seq. (1988). Telephone Consumer Protection Act, 47 U.S.C. § 227 (1991). Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725 (1994). Telecommunications Act, 47 U.S.C. §222 (1996). Electronic Freedom of Information Act Amendments of 1996, Public Law No. 104-231, 110 Stat. 3048 (1996). Financial Modernization Services Act ,Public Law 106-102**,** Gramm-Leach-Billey Act of 1999. Department of Transportation and Related Agencies Appropriations Act of 2000 § 350, Pub. L. No. 106-69; 113 Stat. 986 (1999). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USAPA), H.R. 3162, (2001) o USA Patriot Act. Pen/trap Statute 18 USC §§ 3121-27 (2002). Wiretap Statute, 18 USC §§ 2510-22, (2002).

legislador español desarrolla este derecho fundamental, estableciéndose la protección específica en materia civil.

El **Código Penal** se dispone la regulación específica de los delitos relacionados con la violación de los derechos al Honor, Intimidad y Propia Imagen, con independencia del medio a través del que sean cometidos.

Desde el punto de vista del secreto de las comunicaciones y el derecho fundamental a la protección de datos, a esta norma, se une la publicación de la **Ley 25/2007, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones**, en la que se dispone la obligación de los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones de conservar los datos de tráfico generados por los usuarios a través de sus dispositivos telefónicos o de conexión a Internet, 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.

3.1.3 Posibles riesgos. ¿Cómo puede verse afectado el derecho al honor, a la intimidad personal y familiar y a la propia imagen en una red social?

Como se ha señalado al inicio del capítulo, las redes sociales y sitios web colaborativos en las que los usuarios exponen sus experiencias no quedan exentas de peligros o posibles ataques malintencionados y pueden generarse situaciones que amenacen la integridad de los derechos al honor, intimidad personal y familiar y propia imagen del usuario, así como los derechos de terceros.

A continuación, y tomando como base el análisis y las entrevistas realizadas en el sector, se exponen las situaciones que pueden dañar la integridad de los derechos de los usuarios. La metodología empleada para el análisis toma como punto de partida el momento en el que el usuario se registra en la red social, su participación en la plataforma, y finaliza en el momento en el que éste desea darse de baja del servicio.

De esta forma, el primer momento crítico se sitúa **en el registro del usuario y la configuración del perfil**, dado que es la fase en la que el usuario debe valorar qué información personal desea publicar, así como configurar el grado de publicidad con el que contará dicha información. Este punto es muy importante, y ha de ser tenido en cuenta por los usuarios, pues será esencial para la posterior protección de su intimidad y de la de todos los miembros de su red.

En este momento inicial de toma de datos se incidirá en el derecho a la intimidad personal y familiar únicamente si se solicitan datos íntimos. Por otra parte, también se

incidirá si el servicio ofrece al usuario la posibilidad de adoptar decisiones sobre su entorno. Por ejemplo, si el espacio puede ser configurado como de acceso restringido o acceso público, el uso posterior podría repercutir no ya en la intimidad sino también en el honor o en la propia imagen personal o de las personas a las que eventualmente el usuario haga referencia.

Así, un posible riesgo que se puede plantear es que el usuario no establezca adecuadamente su perfil de privacidad en el momento del registro, bien por desconocimiento o porque la propia red no disponga de estas opciones de configuración.

Una correcta configuración del perfil de privacidad del usuario es fundamental, puesto que, con frecuencia, esta se encuentra activada por defecto en la plataforma en la modalidad que permite el máximo de publicidad. Por tanto, la no configuración o la configuración incorrecta de este aspecto puede afectar no sólo a los contenidos propios que hubiera publicado el usuario, sino también al resto de los usuarios con los que hubiera publicado información compartida, puesto que ésta será accesible por parte del resto de los miembros de la plataforma.

El **uso habitual que se realice de la plataforma** es el segundo momento en el que la intimidad y la propia imagen, pueden verse vulnerados, lo que dependerá del tipo de actividades que los usuarios lleven a cabo.

Así, se puede menoscabar la protección de estos derechos con la publicación de contenidos e información íntima en la plataforma. En este sentido, y si bien es cierto que en principio cualquier usuario controla los contenidos que desea publicar, no siempre aquel valora a priori las implicaciones que puede conllevar la exposición de determinados contenidos. Además, el control de la información publicada en una red social es limitado, en la medida en que cualquier persona o contacto de la red puede publicar fotografías, vídeos y comentarios en los que aparecen imágenes o etiquetas con el nombre de otro usuario. Este último hecho, sin duda alguna, puede poner en riesgo la integridad de los derechos mencionados, así como otros que se analizarán con posterioridad.

Además, y en línea con lo anterior, cabe señalar que el grado de información, datos e imágenes publicados pueden ser excesivos y afectar a la privacidad, tanto personal como de terceros.

- Por lo que respecta a la privacidad personal: a pesar de que sean los usuarios los que voluntariamente publican sus datos, los efectos sobre la privacidad pueden tener un alcance mayor al que consideran en un primer momento ya que estas plataformas disponen de potentes herramientas de intercambio de información, la capacidad de procesamiento y el análisis de la información facilitada por los usuarios.

- Por lo que respecta a la privacidad de terceros: es esencial que los usuarios tengan en cuenta que la publicación de contenidos con información y datos respecto a terceros no puede ser realizada si éstos no han autorizado expresamente su publicación, pudiendo solicitar su retirada de forma inmediata.

Es importante tener en cuenta que en la gran mayoría de ocasiones, las redes sociales permiten a los motores de búsqueda de Internet indexar en sus búsquedas los perfiles de los usuarios, junto con información de contacto y de perfiles amigos, lo que puede suponer otro riesgo para la protección de la privacidad, además de dificultar el proceso de eliminación de su información en Internet.

Otro riesgo que puede aparecer durante la participación en la red social tiene relación con la posibilidad que tienen estas plataformas de ubicar geográficamente al usuario a través de la dirección IP y conocer el dispositivo desde el que se conecta, para contextualizar los contenidos y la publicidad mostrada. Este hecho puede considerarse como una intromisión en las rutinas del usuario que puede suponer un grave menoscabo del derecho a la intimidad.

En último lugar, **en el momento en que el usuario solicite la baja del servicio**, la intimidad y propia imagen también pueden verse afectadas. Esto ocurre porque a pesar de la cancelación de la cuenta, en ocasiones, la información íntima del usuario pueda continuar publicada y ser accesible desde los perfiles de otros usuarios, además de indexada y almacenada en la caché de los distintos buscadores existentes en Internet.

3.1.4 Colectivos especialmente vulnerables. Menores e incapaces.

Este epígrafe pone especial atención en tres colectivos que, por sus características propias, pueden verse afectados en mayor medida que otros perfiles de usuario. Se trata de sujetos menores, incapaces y trabajadores, cuya presencia y participación en este tipo de plataformas es habitual.

Menores e incapaces

Desde el **punto de vista normativo** en materia de protección del honor, intimidad y propia imagen, se ha de tener en cuenta la regulación específica existente.

Así, la Ley Orgánica 1/1982 de *Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen*, regula de manera expresa la forma en que se debe prestar el consentimiento de los menores e incapaces para que sea adecuado en relación con la protección de los derechos al honor, intimidad y propia imagen. En este sentido, se dispone que: *"El consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil".*

Por otra parte, esta Ley, establece dos principios que requieren ser contrastados con la realidad de Internet. En primer lugar, considera su artículo. 1 que la "protección civil del honor, de la intimidad y de la propia Imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia". Además, refiriéndose a los menores el artículo. 3 fija un criterio, la posibilidad de que un menor maduro pueda consentir en aquello que afecte a su honor, intimidad y propia imagen, y que en los casos en los que el menor no disponga de capacidad suficiente para consentir, la norma dispone que *"el consentimiento habrá de otorgarse mediante escrito por su representante legal, quien estará obligado a poner en conocimiento previo del Ministerio Fiscal el consentimiento proyectado. Si en el plazo de ocho días el Ministerio Fiscal se opusiere, resolverá el Juez".*

Un criterio adicional es el del artículo 4 de 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, que además de reconocer al menor los derechos del artículo. 18 CE, establece a intervención del Ministerio Fiscal, en los casos de difusión de información o la utilización de imágenes o nombre de los menores en los medios de comunicación que puedan implicar una intromisión ilegítima en su intimidad, honra o reputación, o que sea contraria a sus intereses. Asimismo, el precepto ordena a los padres o tutores y los poderes públicos respetar estos derechos y protegerlos frente a posibles ataques de terceros.

Es evidente que la realidad de las redes sociales desborda la regulación y obliga a una interpretación sistemática y adecuada del Ordenamiento. Por una parte, los menores de 14 años cuentan con medios tecnológicos suficientes para obtener, captar y reproducir información que afecta a su honor, intimidad e imagen y la de terceros, y de hecho lo hacen. Las fotografías de menores proliferan en Internet en espacios propios, en páginas familiares e incluso vinculadas a actividades escolares.

Se puede destacar que **los riesgos específicos para los menores de edad** en esta materia están directamente relacionados con:

- El acceso a contenidos publicados de carácter inapropiado para su edad.
- La posibilidad de entablar contacto online, e incluso presencialmente, con usuarios malintencionados.
- La proliferación de información personal gráfica de los menores publicada por ellos mismos o por terceros con desconocimiento de los riesgos asociados a tal hecho.

En este sentido, cabe destacar que las redes sociales y los sitios web colaborativos, en la medida en que no tienen capacidad de control sobre las publicaciones que realizan los

menores que son usuarios, ni disponen de herramientas que garanticen la identidad plena de los usuarios, provoca mayores dificultades a la hora de lograr una protección efectiva de los usuarios de la red.

Por ello, y en tanto no sean desarrolladas y debidamente implantadas las medidas que controlen la publicación de contenidos y el acceso a material no adecuado, persistirá el riesgo de que puedan ser vulnerados los derechos de los menores.

A este factor debe añadirse que, como se ha subrayado la inaplicación de la Ley Orgánica 1/1982, elaborada en un momento en la que seguramente sólo se preveían los usos mercantiles de la información y la imagen del menor, y centrada en una intervención del Ministerio Fiscal, resulta a día de hoy seguramente inviable.

El documento de ENISA "Los niños en los mundos virtuales: Lo que los padres deberían saber,"[63] publicado en septiembre de 2008 aporta una serie de recomendaciones a los padres, resaltando, entre otras recomendaciones, la necesidad de formar y educar tanto a los progenitores como a los niños.

Otros supuestos: trabajadores

Desde el **punto de vista normativo**, la protección de la intimidad de los trabajadores cuenta con protección complementaria en la medida en la que el Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del **Estatuto de los Trabajadores (ET)**, dispone en repetidas ocasiones el derecho cualificado de los trabajadores a disponer de intimidad respecto al empresario.

La citada norma dispone que *"sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará 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".*

Sin embargo, este no es en absoluto un criterio aplicable al mundo Internet y así lo ha señalado la Sentencia del Tribunal Supremo (STS) de 26 de septiembre de 2007, que indica que el empresario pueda llegar a controlar e incluso limitar el acceso, amparándose en el poder de dirección dispuesto en el art. 20.3 del Estatuto de los Trabajadores siempre que se reúnan ciertas condiciones[64].

[63] http://www.enisa.europa.eu/doc/pdf/deliverables/children_on_virtual_worlds.pdf

[64] Recurso UNIFICACIÓN DOCTRINA 966/2006, Sentencia de 26/09/2007 del Tribunal Supremo dice: "El control del uso del ordenador facilitado al trabajador por el empresario no se regula por el artículo 18 del

Por otro lado, en la actualidad, y teniendo en cuenta las posibilidades que ofrece Internet, se ha demostrado que **los procedimientos de selección son realizados no sólo utilizando la información proporcionada por el propio candidato en la entrevista de trabajo, sino también con la que éste mismo ha publicado en las redes sociales y en el resto de servicios de los que es usuario en Internet. Además, no debe subestimarse la capacidad de clasificar que ofrecen los resultados de los buscadores.**

Sin duda alguna, esta situación puede suponer un riesgo para la protección de la intimidad de los trabajadores, por lo que de nuevo se hace necesario que los usuarios recurran a limitar, en sus perfiles, las posibilidades de acceso a su información personal y privada.

3.1.5 Medidas empleadas para proteger el derecho al honor, a la intimidad y a la propia imagen de los usuarios

Las redes sociales y las plataformas colaborativas son los principales interesados en proteger a sus usuarios respecto a la utilización no autorizada de su información. Este hecho les ha llevado a establecer los siguientes tipos de medidas:

- **Métodos de denuncia** ante situaciones en las que los usuarios detecten una posible vulneración de sus derechos dentro de la plataforma.
    - *Sistemas de denuncia internas*: Las principales redes sociales y sitios web colaborativos analizados cuentan con este tipo de medidas que permiten a cualquier usuario notificar al administrador de la red social la publicación de una fotografía en la que se utilice su imagen sin su consentimiento así como solicitar la retirada de un determinado comentario, vídeo o imagen que atente contra su derecho a la intimidad, honor y propia imagen.

Estatuto de los Trabajadores, sino por el artículo 20.3 del Estatuto de los Trabajadores y a este precepto hay que estar con las matizaciones que a continuación han de realizarse. La primera se refiere a los límites de ese control y en esta materia el precepto citado remite a un ejercicio de las facultades de vigilancia y control que guarde "en su adopción y aplicación la consideración debida" a la dignidad del trabajador, lo que también remite al respeto a la intimidad en los términos a los que ya se ha hecho referencia al examinar las sentencias del Tribunal Constitucional 98 y 186/2000. (…) lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va a existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.

La segunda precisión o matización se refiere al alcance de la protección de la intimidad, que es compatible, con el control lícito al que se ha hecho referencia. Es claro que las comunicaciones telefónicas y el correo electrónico están incluidos en este ámbito con la protección adicional que deriva de la garantía constitucional del secreto de las comunicaciones."

Esta denuncia genera la cancelación del contenido denunciado y la notificación al usuario denunciado de su falta de autorización para publicar más contenidos respecto al usuario denunciante (ejemplo: no se le permitirá etiquetar de nuevo al usuario en fotografías). Normalmente, en el caso de que el usuario denunciado continúe publicando contenidos en los que aparezca el usuario denunciante, se procede además a la cancelación de su cuenta por parte del administrador de la red social. En este sentido, se presentan deficiencias en los sistemas de denuncias[65].

- *Autorización expresa del usuario*: Está relacionada con la medida anterior. Se requiere que el usuario relacionado con un contenido mediante etiquetas, imágenes o comentarios tenga que autorizar expresamente la publicación de este, pudiendo incluso *denunciar* el contenido al administrador de la plataforma. Sin embargo, este sistema está establecido mediante un "*opt out*", es decir, el usuario puede eliminar a posteriori su foto. En el caso de usuarios no registrados y que sean etiquetados, puede conllevar un mayor riesgo ya que, si bien, en unas plataformas no es posible etiquetarlos, en otras es suficiente con incluir una dirección de correo.

Debe tenerse en cuenta, sin embargo, que el ordenamiento jurídico debe aplicarse de modo integrado y sistemático. En este sentido, no puede desconocerse que las redes sociales, y los servicios de la Web 2.0, -como los blogs-, ofrecen al usuario un espacio para el ejercicio de derechos fundamentales como el derecho a la información y la libertad de expresión.

El ejercicio del derecho a la información, si bien resulta particularmente cualificado cuando se ejerce por los profesionales del periodismo, también puede ejercerse por cualquier ciudadano. Para ser legítimo requerirá que se trate de información sobre hechos noticiables, esto es de interés público ya sea en razón de la noticia o de las personas concernidas, y basado en hechos veraces en cuanto que son contrastados.

Por tanto, de tratarse de un ejercicio legítimo de los derechos del artículo 20 CE, la retirada de determinados contenidos puede en la práctica suponer para quien lo solicita un ejercicio del derecho de rectificación y afectar a los derechos del autor. Estos últimos, podrían lesionarse si la retirada es automática y preventiva. Por lo tanto, parece necesario definir estos procedimientos como procedimientos contradictorios en aquellos casos en los que la lesión a los derechos no sea evidente o en los que quepa inferir un ejercicio legítimo de derechos por quién publicó la información.

[65] Por ejemplo, en Facebook. Algunos proveedores de redes sociales en la opción de "reportar una foto" ofrecen varias opciones (nudismo o pornografía, consumo de drogas, violencia, ataques a una persona o grupo). No da la opción de retirar la foto por falta de consentimiento para que esta aparezca. Asimismo, según reza el propio mensaje "NO eliminaremos fotografías sólo porque no te favorezcan"

- **Métodos de protección técnicos y humanos**:

  - *Procedimientos de información*: Varias de las redes sociales analizadas cuentan con sistemas que preavisan a los usuarios cuando alojan contenidos respecto a las implicaciones que puede conllevar, tanto para sí mismo, como para los terceros implicados. Este tipo de avisos son mostrados frecuentemente cuando los usuarios alojan contenidos multimedia, como fotografías y/o vídeos.

  - *Vigilancia voluntaria de contenidos*: Varias de las redes sociales entrevistadas cuentan con grupos de usuarios voluntarios que se ocupan de vigilar la idoneidad de los contenidos. Estos grupos vigilan tanto los contenidos *publicados* por los usuarios de la red, como aquellos que aun estando enlazados desde la plataforma, se alojan físicamente fuera de esta.

  - *Aplicaciones software de identificación de la edad*: Algunas redes sociales han implementado, con el fin de proteger a los menores, programas que detectan la edad aproximada del usuario. La técnica empleada tiene como base el testeo de las expresiones vertidas por los usuarios en sus mensajes (empleo del lenguaje, expresiones, estilo de redacción, etc.). El objetivo de la medida se centra en:

    - Detectar la presencia y participación de menores en redes sociales destinadas únicamente para adultos.

    - Identificar a usuarios adultos que estén intentando suplantar o contactar con usuarios menores de edad.

No obstante, como se ha señalado anteriormente, actualmente esta medida no alcanza el grado de efectividad deseado.

- **Formación y concienciación de los usuarios**

  - *Información sobre los deberes de los usuarios:* El alta en las redes sociales suele venir acompañada de prolijos contratos de adhesión. En ellos las *obligaciones* de los usuarios se diluyen en una maraña de cláusulas contractuales. Deberían adoptarse estrategias informativas específicas que obliguen a una lectura de las obligaciones de los usuarios y que se encuentren siempre disponibles.

  - *Elaboración y publicación de códigos éticos:* La existencia de reglas éticas de actuación no es desconocida en el mundo Internet. Los ISP deberían definir el estándar razonable de conducta en sus entornos, más allá de la

aplicación de lo dispuesto en las normas. El fomento de códigos de autorregulación de las comunidades de una red social puede contribuir significativamente a la formación y concienciación de los usuarios.

3.2 Protección de Datos de Carácter Personal

El funcionamiento de las redes sociales y sitios web colaborativos se fundamenta principalmente, como ya se ha comentado, en la publicación, por parte de los usuarios, de información y datos personales, lo que conlleva diferentes implicaciones jurídicas.

3.2.1 Definición del derecho

El constituyente español, al igual que previamente había ocurrido en la Constitución de Portugal, sentó en el artículo 18.4 CE las bases de un nuevo derecho fundamental. Dicho derecho fue definido en su día como “Habeas Data”, aunque resulta mucho más precisa y adecuada la denominación de derecho a la protección de datos. Se trata de un derecho de configuración jurisprudencial a través de un conjunto de sentencias que arrancan con la STC 254/1993 y culminan con la STC 292/2000, cuyo fundamento jurídico quinto define un nuevo derecho fundamental dotándolo de plena autonomía respecto del derecho a la intimidad:

“La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

Este **derecho fundamental a la protección de datos**, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran”.

Según el Tribunal Constitucional el objeto del derecho a la protección de datos alcanza:

"a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo".

A efectos normativos, se entiende que un dato de carácter personal es *"cualquier información concerniente a personas físicas identificadas o identificables",* lo que convierte en dato de carácter personal la mayor parte de la información sobre personas físicas, en la medida en que a través de escasos datos o informaciones sobre éstas y mediante la correcta aplicación de herramientas informáticas, es relativamente sencillo **identificar a la persona concreta que se encuentra detrás de los datos de que se dispone. Entre los datos personales que en el contexto de las redes sociales pueden llegar a identificar a las personas, se encuentra, entre otros, la dirección IP, tal y como ha sido definida por la Agencia Española de Protección de Datos[66] y por el Grupo de Trabajo del Artículo 29 en su "Dictamen sobre el concepto de datos personales"[67].**

Dada la gran cantidad de datos personales que los usuarios publican en sus perfiles, éstos se convierten en auténticas "**identidades digitales**" que facilitan un rápido conocimiento de datos de contacto, preferencias y hábitos del usuario. Además debe considerarse que durante la prestación de estos servicios se recopilan datos como la dirección IP, que se utilizan para segmentar la publicidad que se dirige a los distintos tipos de usuarios, así como aumentar el grado de contacto entre los usuarios registrados.

[66] Informe de la Agencia Española de Protección de Datos 327/2003 https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf

[67] Dictamen sobre el concepto de datos personales. El Grupo de trabajo considera las direcciones IP como datos sobre una persona identificable. En ese sentido ha declarado que «*los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el* sentido de la letra a) del artículo 2 de la Directiva (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_es.pdf.

De esta forma, y teniendo en cuenta los principios básicos dispuestos en la normativa vigente, la protección de datos personales debe ser especialmente atendida por parte de todo proyecto relacionado con el mundo de las redes sociales y sitios web colaborativos, donde el funcionamiento y tratamiento de información personal es el elemento clave para su funcionamiento.

3.2.2 Marco jurídico aplicable: normativa y evolución legislativa

El marco legal en materia de protección de datos responde a la necesidad de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, evitándose así que los datos sean utilizados de forma inadecuada o fraudulenta, o sean tratados o cedidos a terceros sin consentimiento inequívoco del titular.

Normativa internacional

Actualmente existen leyes reguladoras de la protección de datos de carácter personal en, al menos, 46 Estados. Este dato, unido al hecho de que la mayor parte de las normas publicadas son recientes y ya prevén aspectos específicos derivados de la Sociedad de la Información, hacen de la protección de datos de carácter personal uno de los aspectos más y mejor tratados desde el punto de vista legislativo.

Todo ello, unido a la existencia de varias directrices realizadas por la OCDE[68] y la ONU[69] o el Marco de Privacidad de APEC,[70] hacen que los principios básicos que rigen las normativas sean semejantes o aproximados en cada uno de los Estados, sin que ello suponga que se encuentren exentas de diferencias.

Normativa europea

Del mismo modo que ocurriera con el desarrollo del derecho a la vida privada, el Consejo de Europa en el **Convenio núm. 108**[71] define el contexto de protección de la privacidad en relación con las tecnologías de la información y las comunicaciones. Por otra parte, las sentencias emanadas del Tribunal Europeo de Derechos Humanos producen efectos

[68] Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, de 23 de septiembre de 1980.
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

[69] Directrices para la regulación de los archivos de datos personales informatizados, Adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990.

[70] Asia-Pacific Economic Cooperation Privacy Framework
http://www.apec.org/apec/news___media/fact_sheets/apec_privacy_framework.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1

[71] Convenio del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado el 27 de enero de 1984 (B.O.E. de 15 de noviembre de 1985).

jurídicos en el ordenamiento interno y han venido inspirando la labor del Tribunal Constitucional en la interpretación de los derechos fundamentales.

El Convenio núm. 108 surgió de la necesidad de profundizar en la protección de los derechos de los individuos en relación con el uso de la informática, en especial en lo relativo a la vida privada, protegida por el artículo 8.1 del Convenio Europeo de Derechos Humanos. Además, se debía hacer compatible esta tutela jurídica con la libertad de circulación de la información, y, por último, se consideraba necesario establecer un mínimo denominador común entre las legislaciones de los futuros Estados signatarios que permitiese facilitar el flujo internacional de datos.

El Convenio estuvo precedido por dos Resoluciones del Comité de Ministros, la R (73) 22[72] y la R (74) 29,[73] referidas a la protección de datos en los sectores privado y público respectivamente, que adelantaban algunos de los principios básicos que posteriormente inspirarían la redacción del Convenio de 1981. Atendiendo al Convenio, hay que señalar que éste posee *tres partes claramente diferenciadas por su Memoria explicativa*: las disposiciones de Derecho sustantivo, en forma de principios básicos; las reglas especiales referentes a los flujos internacionales de datos; y unos mecanismos de auxilio mutuo y consulta de las Partes. El Convenio ha sido completado por un conjunto de Recomendaciones dirigidas a orientar las decisiones normativas nacionales en sectores específicos:

El Convenio además define *aspectos básicos* como el concepto de dato de carácter personal, fichero automatizado, tratamiento automatizado o la autoridad «controladora del fichero», que hoy se define como responsable.

Asimismo, el Convenio *fija los principios básicos para la protección de datos*, como el de calidad o el de seguridad; los derechos de acceso, rectificación y cancelación; la protección de los datos que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual; o la fijación de procedimientos de salvaguarda.

Por otra parte la jurisprudencia del Tribunal Europeo de Derechos Humanos ha extendido la aplicación del artículo 8 CEDH con una concepción muy amplia de la vida privada y familiar que alcanza al reconocimiento del derecho a la protección de datos en los términos del Convenio núm. 108.

[72] Resolución (73) 22 relativa a la protección de la vida privada de la personas físicas respecto de los bancos de datos electrónicos en el sector privado, acordada por el Comité de Ministros el 26 de septiembre de 1973.

[73] Resolución (74) 29 relativa a la protección de la vida privada de la personas físicas respecto de los bancos de datos electrónicos en el sector público, adoptada por el Comité de Ministros el 20 de septiembre de 1974.

En el marco de la Unión Europea el **artículo 8 de la Carta Europea de Derechos Fundamentales** reconoce de modo específico el derecho a la protección de datos como un derecho autónomo del derecho a la vida privada, que comprende tanto el derecho a consentir, como el deber de tratar los datos lealmente y de satisfacer los derechos de los afectados y encomienda su tutela a autoridades independientes. Este principio que también se recoge en el artículo 286 del Tratado de la Comunidad Europea.

La Unión Europea publicó en el año 1995 la **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 éstos datos**,[74] con la finalidad de que los Estados miembros armonizasen y adaptasen sus legislaciones internas en materia de protección de datos de carácter personal.

Este texto constituye un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE).

Los aspectos clave de la normativa comunitaria en materia de protección de datos son:

- El establecimiento del principio de calidad de los datos, de tal forma que los datos personales deben ser adecuados, pertinentes y no excesivos, conforme a la finalidad para la que serán tratados.

- Se impone como principio básico y esencial para el tratamiento de datos personales, la existencia del consentimiento previo del titular de los datos.

- Se requiere a los Estados que establezcan la obligación de conciliar el derecho a la intimidad en el tratamiento de los datos personales con el derecho a la libertad de expresión.

- Se establecen como principios básicos de los ciudadanos los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) en relación a sus datos personales.

- Se incorpora como principio básico la garantía de confidencialidad, así como la obligación de implantar las medidas de seguridad oportunas que garanticen que el acceso a la información se encuentra limitado y controlado.

- Se enuncian los principios básicos para la creación de las Autoridades Nacionales de Protección de Datos.

[74] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML

- Se fijan las bases de las transferencias internacionales de datos personales.

- Se promueve la elaboración de códigos de conducta sectoriales, destinados a contribuir a la correcta aplicación de las disposiciones nacionales en materia de protección de datos personales.

- Se crea el Grupo de Trabajo del Artículo 29 institución de referencia en esta materia[75].

Debe destacarse además la importante tarea desarrollada por el Tribunal de Justicia de las Comunidades cuyas sentencias han precisado distintos aspectos en esta materia[76].

Es importante resaltar la reciente reunión que han mantenido en Estrasburgo las autoridades encargadas de velar por la protección de datos personales en Europa, para abordar la importancia de la seguridad de los datos en este tipo de servicios -blogs, redes

[75] Órgano creado en virtud del artículo 29 de la Directiva 95/46/CE e integrado por representantes de las autoridades de protección de datos de los Estados Miembros. Se trata del órgano consultivo independiente de la UE sobre protección de los datos y la vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

Investiga, analiza y aúna las iniciativas a nivel comunitario en materia de protección de datos de carácter personal. Su actividad se ha visto ligada en los últimos tiempos al análisis de los servicios de la Sociedad de la Información y a los problemas derivados para la protección de datos y la seguridad.

El conjunto de directivas dictadas en esta materia es particularmente extenso:

- 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.
- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
- Directiva 2000/31/CE, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, y en particular el comercio electrónico en el mercado interior.
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones.
- Directiva 2006/24/CE, de 21 de febrero de 2006, del Parlamento Europeo y del Consejo 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 por la que se modifica la Directiva 2002/58/CE.
- Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales por las Instituciones y los Organismos Comunitarios y a la Libre Circulación de estos Datos.

Más información en: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

[76] Un ejemplo claro es el caso de la sentencia dictada en el caso de la Sra. Lindqvist, acusada de haber infringido la normativa sueca relativa a la protección de datos personales al publicar en su sitio Internet diversos datos de carácter personal sobre varias personas que, como ella, colaboraban voluntariamente con una parroquia de la Iglesia protestante de Suecia. Esta señora habiendo aprendido rudimentos de informática y diseño web mantenía una página de información parroquial en la que llegó a informar sobre el estado de salud de un miembro de la comunidad. Respondiendo a las cuestiones planteadas el TJCE identificó la presencia de un tratamiento de datos de carácter personal sujeto a la Directiva.

sociales, y otros servicios avanzados de Internet- y la necesidad de establecer soluciones normativas y tecnológicas de ámbito internacional capaces de garantizar la correcta protección de los derechos de los usuarios.

En este sentido, las autoridades allí reunidas han manifestado públicamente su decisión de abordar el fenómeno de las redes sociales y servicios análogos, emplazándose a realizar en noviembre del año 2009 una Conferencia en Madrid (España) en la que se aborde la posible redacción de un **Tratado Internacional de Protección de Datos Personales**,[77] que permita disponer de una regulación extraterritorial que se adecue a las características propias de este tipo de servicios.

En este sentido, la intervención del Director en la Conferencia de Primavera de autoridades europeas de protección de datos (Roma, 2008) puso de manifiesto algunos extremos relevantes desde el punto de vista de este estudio.

Por una parte, es evidente, que aunque los ciudadanos no sepan definir con precisión el alcance y naturaleza del derecho fundamental a la protección de datos lo intuyen, reconocen e identifican en cuanto éste es amenazado y puesto en riesgo, y les preocupa la seguridad de los datos personales en la Red.

Por otra, si bien los dicen conocer la existencia de las políticas de privacidad en Internet, la práctica ofrece una conclusión bien contraria. El número de accesos a las páginas de las políticas de privacidad es muy bajo, prácticamente marginal. Las políticas de privacidad ocupan espacios residuales en los websites y resultan ininteligibles. Por tanto, es evidente que el ciudadano desconoce el contenido real y las consecuencias de estas políticas de privacidad. En Internet no puede hablarse de un consentimiento basado en información fiable o confiable. Otro tanto sucede con los rastros en la navegación, las cookies, la indiferencia frente a estos tratamientos desaparece cuando existe una conciencia clara de riesgo.

Estamos ante un gravísimo problema de desconocimiento e ignorancia en el uso de estas tecnologías de Internet. Y la “letra pequeña” de las ilegibles cláusulas generales de contratación para la instalación de software contribuye significativamente a este problema.

Este estado de cosas obliga a proponer de estándares internacionales compartidos que garanticen una eficaz protección universal de los derechos de los usuarios.

Aunque no posee valor normativo, mención especial requiere la ***Comunicación sobre el fomento de la protección de datos mediante las tecnologías de protección del***

[77] Para más información acceda a la Agencia Española de Protección de Datos.

derecho a la intimidad (PET) de 2 de mayo de 2007[78] que realizó la Comisión del Parlamento Europeo, introduciendo un claro ejemplo de la protección de los derechos de protección de datos e intimidad de los usuarios, mediante herramientas tecnológicas denominadas *"PET".*

Las ***"Tecnologías de protección del derecho a la intimidad" (PET)*** son sistemas tecnológicos destinados a reducir y, en su caso, suprimir el impacto de las nuevas tecnologías de la información sobre los derechos de protección de datos e intimidad de los usuarios, sin que ello suponga menoscabo alguno respecto a las funcionalidades de los sistemas tecnológicos. Algunos ejemplos de PET son:

- *La disociación (anonimización o mantenimiento anónimo) automática de los datos. Los datos deben ser almacenados en un formato que permita identificar al interesado únicamente durante el tiempo necesario para la consecución de las finalidades para las que fueron obtenidos inicialmente. Así, una vez que los usuarios no se encuentren activos, será, por tanto, necesario disociar los datos de aquellos*

- *El uso de instrumentos de cifrado que impidan el acceso no autorizado a la información transmitida a través de Internet, evitando así el tratamiento no autorizado e ilícito de los datos personales publicados en Internet.*

- *El uso de anuladores de "cookies", que impiden que el sitio web pueda instalar en los equipos de los usuarios ficheros que, de forma automática y sin que el usuario lo conozca, recopile toda la información estadística y relativa a los accesos que el usuario lleva a cabo durante su navegación.*

- *La Plataforma de Preferencias de Privacidad (P3P), que permite a los usuarios analizar y comparar las políticas de privacidad de los sitios web que visita, otorgándole un informe sobre la adecuación de éstas a la normativa aplicable.*

- *Los sistemas de gestión de identidad, que permiten el control por parte de los usuarios de los datos que revelan sobre sí mismos en cada transacción, como los promovidos por el proyecto PRIME (Privacy and Identity Management for Europe).*

Tal como se menciona en la Comunicación de la Comisión sobre el papel de la administración electrónica en el futuro de Europa, la administración electrónica debe emplear PET para generar la confianza necesaria y prestar un servicio satisfactorio.

Estados Unidos

[78] Documento disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:ES:PDF

En el caso de EE.UU. la primera norma relativa a la protección de la privacidad de los usuarios en Internet, fue la ***"Electronic Communications Privacy Act (ECPA)"*** vigente desde 1986, en la que se establecen las bases normativas en lo que respecta a la regulación de la privacidad de las comunicaciones electrónicas de los usuarios, así como los límites específicos respecto a las posibilidades de acceso por parte de los organismos públicos a las comunicaciones electrónicas de los usuarios.

En el año 1994 se publica ***"The Computer Fraud and Abuse Act"***, modificando la anteriormente citada, definiendo y regulando en mayor medida los diferentes aspectos relacionados con la seguridad de la información respecto a virus, spyware y las diferentes modalidades de software maligno que circulan por la Red y que potencialmente pueden poner en peligro la integridad de la privacidad e intimidad de los usuarios de servicios online.

En el año 1998, el gobierno federal publica la norma ***"Children's Online Privacy Protection Act (COPPA)"***, en la que se regula en mayor medida y de forma claramente proteccionista la privacidad de los usuarios de servicios online menores de edad, estableciendo que todos los prestadores de servicios de la sociedad de la información que cuenten con contenidos que vayan dirigidos expresamente a menores de 13 años, serán responsables de la adecuación de los mismos a estas edades.

Del mismo modo, se dispone que, en caso de que los menores tengan que facilitar datos personales a través del sitio web, deberá informarse de forma clara y comprensible respecto a cuáles son las finalidades para las que son solicitados, así como la puesta a disposición, de los tutores de los menores, de procedimientos sencillos y gratuitos que permitan conocer el tipo de datos facilitados por el menor y dar de baja o actualizar dichos datos.

A partir del año 2001, a raíz de los atentados del 11 de septiembre, el gobierno federal publicó la ***"USA Patriot Act (UPA)"***, vigente desde el 24 de octubre de 2001 y la *"**Cyber Security Enhancement Act (CSEA)"***, mediante las que se autoriza la intervención, por parte del gobierno, de cualquier comunicación electrónica (con independencia del formato en que se encuentre), telefónica, las búsquedas realizadas en los buscadores de Internet, los históricos de visitas de páginas web, etc., sin que para ello sea necesario contar con autorización judicial previa, lo que ha supuesto un claro retroceso de los derechos civiles y políticos en favor de la seguridad de los ciudadanos.

Además, cabe resaltar la publicación de la ***"Controlling Assault of Non-Solicited Pornography and Marketing"***, vigente desde el 17 de mayo del 2002 y que recientemente ha sido modificada y completada en cierta medida por la ***"Keeping the Internet Devoid of Sexual Predators"***, presentada a firma por el presidente de los Estados Unidos el día 3 de octubre de 2008. Esta norma tiene como objetivo permitir al

Abogado General acudir al registro de agresores sexuales para buscar coincidencias con casos de intentos de abuso en las propias redes sociales y en cualquier herramienta online semejante, lo que ha provocado una reacción inmediata de las diferentes redes sociales que operan en Estados Unidos, manifestando su disposición y colaboración plena con las fuerzas y cuerpos de seguridad en la búsqueda y eliminación de aquellos perfiles de personas presuntamente peligrosas para los menores[79].

Por último, se debe señalar la norma **"Can Spam Act"** Uno de los objetivos prioritarios de la promulgación de ésta ley ha sido la homogenización de la legislación en materia de *spam* dentro de los Estados Unidos, donde ya empezaban a proliferar leyes estatales con diferentes acercamientos al problema, todas ellas abolidas con la entrada en vigor de la "CAN SPAM Act". Esta ley establece una serie de garantías que básicamente son:

- Obligatoriedad de etiquetar los mensajes en caso de contenido publicitario o de carácter pornográfico.
- Prohibición de la falsificación de las cabeceras de los mensajes, donde se identifica el emisor del mismo, así como la cumplimentación engañosa del campo "asunto".
- Prohibición de la utilización encubierta del ordenador personal de otro para el envío de comunicaciones comerciales electrónicas.
- Prohibición de la recolecta de direcciones de correo electrónico sin consentimiento del afectado, así como la utilización de "técnicas de diccionario" (formación de direcciones de los destinatarios mediante diccionarios de nombres).

Normativa Nacional

En España, la regulación sobre protección de datos de carácter personal se centra en dos normas principalmente:

- **La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).**
- **Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RDLOPD).**

Además existen normas sectoriales en ámbitos como la sanidad, las telecomunicaciones o las finanzas. No obstante dos normas se proyectan de modo muy particular sobre las redes sociales:

[79] Para más información puede leer el comunicado hecho público por Facebook.; http://blog.facebook.com/blog.php?post=34342042130

- **Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI-CE).**

- **Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.**

- **Ley 25/2007, de 18 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.**

- **Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.**

De conformidad con lo dispuesto en la **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal** (**LOPD**), el objeto de la norma es *"…garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar."*

Todo tratamiento de datos de carácter personal debe atender a una serie de principios básicos:

- **Calidad de los datos:** es esencial que los datos personales tratados sean adecuados, pertinentes y no excesivos, en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, no pudiendo usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recabados. Los datos deberán responder con veracidad a la situación actual del afectado debiendo rectificarlos si se constatan errores. Sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento, prohibiéndose la recogida de datos por medios fraudulentos, desleales o ilícitos. Por otra parte, el responsable debe conservar los datos personales mientras subsista la finalidad y cancelarlos cuando esta cese.

- **Información en la recogida de datos**, el afectado será informado, en el momento en el que se recaben sus datos, del alcance del tratamiento que se va a realizar. El art. 5 LOPD establece que "*los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*

  a) *De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*

  b) *Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*

c) *De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*

d) *De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*

e) *De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".*

- **Consentimiento del afectado** o manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de sus datos personales.

- **Datos especialmente protegidos**, este principio hace referencia a datos de carácter personal que revelan la ideología, afiliación sindical, religión, creencias, -caso para el que el consentimiento debe ser expreso y por escrito-, origen racial, salud y vida, sexual, -para cuyo tratamiento se requiere consentimiento expreso-, y los relativos a la comisión de infracciones penales o administrativa.

- **Seguridad de los datos**, todas las empresas, organizaciones, asociaciones e Instituciones, públicas y privadas, que almacenen, traten y accedan a ficheros de datos de carácter personal, deben aplicar medidas de seguridad técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información.

- **Deber de secreto**, este principio recoge las obligaciones de secreto, confidencialidad y custodia que incumben a aquellas personas que traten los datos; y, de manera particular, a aquellos que en el desarrollo de sus funciones accedan a ficheros que contienen datos personales.

- **Comunicación de datos**, es "toda revelación de datos realizada a una persona distinta del afectado o interesado". Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero, para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

- **Acceso a los datos por cuenta de terceros**, supone la prestación de un servicio al responsable del fichero por parte de una tercera empresa denominada Encargado del Tratamiento, que accede a los datos del fichero para el cumplimiento de la prestación contratada; actuando en nombre, por cuenta y de acuerdo a las instrucciones establecidas y dadas por el Responsable del Fichero.

Antes de realizar el análisis completo respecto a la aplicación de las normas, se ha de tener en cuenta el **aspecto extraterritorial de los servicios de la Sociedad de la Información.**

Dado que la gran mayoría de los proveedores de este tipo de servicios operan desde fuera de la UE (principalmente desde los EEUU), se ha de analizar en qué medida es posible exigir a las plataformas el cumplimiento de la normativa comunitaria. En este sentido, la normativa dispone que ésta será de aplicación en los siguientes casos:

- Cuando el tratamiento de datos se realice en España a través de un establecimiento del responsable del tratamiento.

- En el caso de que el responsable del tratamiento no se encuentre en territorio español, pero le sea de aplicación directa la normativa española mediante acuerdos internacionales.

- Cuando el responsable del tratamiento no este establecido en territorio de la Unión Europea y utilice en el tratamiento de datos, medios o elementos situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

Debe considerarse que en España la normativa específica respecto a los prestadores de servicios de la sociedad de la información, previa fundamentación jurídica y práctica, admite la posibilidad de que las autoridades de protección de datos nacional apliquen dicha normativa a los prestadores, con independencia del lugar desde el que se opere.

Por un lado, la **Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal**, establece que existen dos casos en los que se aplica a los responsables establecidos fuera de la UE/EEE: En primer lugar, cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento ubicados en territorio español y, en segundo lugar, cuando utilice medios situados en dicho territorio.

En este sentido, el Grupo de Trabajo del Artículo 29 se ha pronunciado en su **"Dictamen sobre cuestiones de protección de datos en relación con buscadores"**[80]. Este dictamen contiene una serie de criterios para definir cuando se considera que existe un establecimiento del responsable:

"La existencia de un "establecimiento" implica el ejercicio real y efectivo de actividades a través de gestiones estables. La forma jurídica del establecimiento (una oficina local, una filial con personalidad jurídica o una representación mediante terceros) no resulta

80 https://www.agpd.es/portalweb/canaldocumentacion/internacional/common/pdf/WP_148_Dictamen_Buscadores_es.pdf

determinante. Sin embargo, otro requisito consiste en que la operación de tratamiento se realice "en el marco de las actividades" del establecimiento. Esto significa que el establecimiento también debe desempeñar un papel importante en la operación de tratamiento concreta. Éste es claramente el caso cuando:

- *un establecimiento es responsable de las relaciones con los usuarios del buscador en una jurisdicción concreta;*
- *un proveedor de buscadores establece una oficina en un Estado miembro (EEE) implicada en la venta de anuncios dirigidos a los habitantes de dicho estado;*
- *el establecimiento de un proveedor de buscadores cumple los autos judiciales y/ o solicitudes de cumplimiento de la ley por parte de las autoridades competentes de un Estado miembro en relación con los datos de los usuarios"*

Por otro lado, en lo que respecta a la prestación de servicios por parte de proveedores fuera de la UE utilizando medios situados en dicho territorio, el documento recoge una serie de criterios. Tal y como establece el documento, *"los centros de datos situados en el territorio de un Estado miembro pueden utilizarse para el almacenamiento y el tratamiento a distancia de datos personales. Otros tipos de medios podrían ser la utilización de ordenadores personales, terminales y servidores. La utilización de cookies y dispositivos de software similares por parte de un proveedor de servicios online también puede considerarse como recurso a medios en el territorio del Estado miembro.*

Asimismo, en el año 2002 el citado Grupo de Trabajo adoptó un **"Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE" (WP 56)"**[81]. Dada la gran complejidad de este ámbito y el dinamismo del entorno Internet, este documento constituye una herramienta y punto de referencia para los responsables del tratamiento en el examen de los casos que implican el tratamiento de datos de carácter personal en Internet por sitios web establecidos fuera de la Unión Europea.

De la misma manera, la **LSSI-CE** contempla su aplicación a "los prestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo". Así, su artículo 4 dispone que *a estos prestadores les será de aplicación los artículos sobre la libre prestación de los servicios y sobre colaboración de los prestadores de servicios de intermediación para interrumpir el servicio o retirar determinados contenidos cuando lo haya declarado un órgano español competente sobre la licitud de los mismos.*

[81] WP 56, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf

Y también, establece su aplicación cuando dirijan sus servicios específicamente al territorio español siempre que ello no sea contrario a los convenios internacionales aplicables.

A los efectos de determinar si los prestadores de servicios dirigen sus servicios específicamente al territorio español, ha de atenderse a **varios elementos indiciarios**:

- Si disponen de la extensión de nombre de dominio .es registrada ante Nic.es u operan a través de nombres de dominio *"es.redsocial.com"* o *"redsocial.com/es"*
- Si el sitio web se encuentra en castellano.
- Si tiene política de privacidad específica.
- Si el sitio web, por su apariencia y contenido, pudiera llegar a dar a entender que se dirige al territorio de España.
- Si la publicidad realizada es de productos y servicios distribuidos desde España.
- Si el número de usuarios españoles es elevado respecto a la muestra estadística.
- Si disponen de oficinas o agentes comerciales que traten datos personales en territorio nacional.
- Si para la prestación del servicio emplean servidores alojados en España.

En este marco, la Agencia Española de Protección de Datos ha afirmado su competencia para aplicar esta normativa a prestadores de servicios establecidos fuera del EEE respecto de la prestación del servicio del correo electrónico gratuito[82].

3.2.3 Posibles riesgos de las redes sociales. ¿Cómo pueden verse afectados los datos personales de los usuarios?

El conjunto de riesgos que se identifican a continuación no comporta necesariamente la comisión de ilícitos por el proveedor de servicios sin perjuicio de que los hechos demuestren que generalmente la configuración por defecto de sus servicios suele ofrecer una estándar bajo de privacidad.

El consentimiento que presta el usuario es válido en el momento en que decide aceptar, la política de privacidad y condiciones de uso de la plataforma que constan en el formulario de registro. Por ello, debe estar muy atento a su contenido y consecuencias. Evidentemente, esto no obsta a que resulte exigible que las políticas de privacidad deban ser transparentes, accesibles y claras. La AEPD ha insistido sobre el particular en su

[82] Expediente E/01544/2007.

"Declaración sobre buscadores", así como en la "Resolución sobre correo electrónico gratuito".

Del mismo modo, los usuarios deben valorar siempre, qué tipo de datos proporcionan a la plataforma y publican en su perfil, ya que no tiene la misma trascendencia el tratamiento por parte de la plataforma de los datos de carácter personal de nivel básico (nombre, dirección, teléfono, etc.), que otras información de contenido más sensible (nivel de renta, solvencia, recibos, afiliación sindical o política, salud, vida sexual, etc.), donde el nivel de protección y concienciación por parte del usuario deberá ser mucho mayor, dado que se trata de derechos pertenecientes a la esfera más íntima de su vida.

Por ello, a pesar de que la información contenida en los perfiles de los usuarios es alimentada directamente por éstos, es necesario tener en cuenta cuáles son los principales riesgos que se pueden derivar del uso de este tipo de plataformas para la protección de los datos de carácter personal.

Tras el análisis individual y pormenorizado de las redes sociales referenciadas en el Anexo I del Estudio, y como criterio general, cabe destacar que todas las redes sociales y plataformas colaborativas disponen de avisos legales, condiciones de uso y políticas de privacidad **redactadas en un lenguaje de difícil comprensión para el usuario medio.** De esta forma, y a pesar de encontrarse recogidas en el sitio web, **no alcanzan su finalidad última: que el usuario comprenda el objeto, la finalidad y el plazo para el que son recabados y tratados sus datos personales.**

Así, **el primer momento crítico para la protección de datos personales** se encuentra en la fase inicial de registro del usuario, cuando este proporciona la información personal necesaria para poder operar en la red social. En este momento, los datos se pueden ver sometidos a varios riesgos:

- **Que el tipo de datos solicitados en el formulario de registro,** aunque no obligatorios, **sean excesivos.** En este sentido, debe tenerse en cuenta que, con frecuencia, las redes sociales solicitan a los nuevos usuarios datos relativos a su ideología política, orientación sexual y preferencia religiosa. Si bien es cierto que estos datos tienen carácter voluntario y todo usuario es libre de publicar el contenido que deseé respecto a sí mismo, debe considerar las implicaciones que ello puede conllevar para su vida y las personas de su entorno, ya que estos datos serán visibles por todos sus contactos y, dependiendo de la configuración del perfil, por todos los usuarios de la red. Es por ello que los usuarios y los responsables de las redes deben limitar y controlar en todo momento que el grado y la trascendencia de los datos publicados no sea extrema. Debe tenerse en cuenta que el artículo 7 LOPD obliga a contar con un consentimiento expreso y por escrito en lo que se refiere a datos

relativos a ideología, religión o creencias, y expreso en el ámbito de la salud, origen racial y vida sexual.

- **Que el grado de publicidad del perfil de usuario sea demasiado elevado.** Es en el momento inicial del registro como usuario cuando éste debe configurar debidamente el grado de publicidad de su perfil, de tal forma que determine desde el comienzo quiénes podrán tener acceso a toda la información que el usuario publique. Todas las redes analizadas muestran, activado por defecto, el mayor grado de publicidad, resultando el perfil de acceso completamente público lo que supone un grave riesgo para la seguridad de los datos personales de los usuarios, en la medida en que éstos serán accesibles por parte de cualquier usuario de la plataforma.

- **Que la finalidad de los datos no esté correctamente determinada.** Con frecuencia las políticas de privacidad recogidas en este tipo de plataformas, determinan las finalidades para las que se recaban y tratan los datos personales, pero de forma generalista y sin aclarar completamente para qué pueden o no tratar los datos personales, lo que supone un grave riesgo para el tratamiento de los datos de los usuarios.

- **Transferencia internacional de datos.** Como se ha señalado, es frecuente que este tipo de plataformas se encuentren ubicadas fuera del territorio europeo, principalmente en EE.UU., lo que supone que en el momento de registro del usuario, los datos son trasladados a los servidores y oficinas ubicados en este país. Por ello, resulta fundamental que las políticas de privacidad del proveedor garanticen un estándar adecuado de protección. Junto a este hecho cabe la posibilidad de que las plataformas cedan sus bases de datos a terceras organizaciones, para que lleven a cabo campañas de envío de comunicaciones comerciales no autorizadas (*spam*) o realicen otro tipo de tratamiento que goce de menor protección en el país en el que se tratan los datos. Y ello debería ser tenido en cuenta por el usuario como criterio de elección de una determinada red.

El segundo momento considerado crítico para la protección de datos personales se sitúa en la fase intermedia, es decir, en la que el usuario desarrolla su actividad en la plataforma y utiliza los servicios y herramientas que ésta le ofrece. En este momento los aspectos que pueden poner en riesgo la seguridad y protección de datos personales de los usuarios son:

- **La publicación excesiva de información personal (propia o de terceros).** En esta fase se mantiene el posible riesgo que conlleva la publicación excesiva de información personal por parte de los usuarios.

Además se debe tener en cuenta que existe la posibilidad de que los usuarios publiquen también datos respecto de terceros, lo que puede conllevar el tratamiento y la cesión pública de datos de personas que no han prestado el consentimiento para ello.

La AEPD ha sancionado la captación y publicación de imágenes de terceros en plataformas colaborativas sin consentimiento de las personas afectadas[83].

De la misma forma, la AEPD ha reconocido el derecho frente al responsable del sitio web a cancelar los datos publicados que habían sido facilitados por terceros en entornos online[84].

- **La instalación y uso de "*cookies*" sin conocimiento del usuario.** Con frecuencia las redes sociales y plataformas análogas utilizan este tipo ficheros que tienen la posibilidad de almacenar determinada información sobre el usuario y su tipo de navegación a través de un sitio web.

  Estos ficheros se instalan en los equipos de los usuarios, de forma que resulta posible detectar el lugar desde el que accede el usuario, el tipo de dispositivo empleado (móvil o fijo) para el acceso, el tipo de contenidos accedidos, los lugares más visitados y las acciones habituales realizadas durante la navegación, así como el tiempo empleado en cada una de las páginas, entre otras muchas funcionalidades.

  Este modo de recabar los datos funciona de forma automática, al contrario que en el caso de los formularios.

  Dado que la dirección IP[85] desde la que se conecta a Internet el usuario es considerada por la Agencia Española de Protección de Datos un dato de carácter personal, en la medida que puede asociarse a una persona identificable, se debe entender que por ende, a través de aquella cabe la posibilidad de obtener información relacionada con los usos y hábitos de navegación de los usuarios del sitio web, lo que proporciona una herramienta muy valiosa desde el punto de vista del marketing y la publicidad.

[83] Resolución de la Agencia Española de Protección de Datos PS/00117/2008

[84] Procedimiento TD/00266/2007.

[85] La dirección IP está formada por una serie numérica de cuatro grupos entre 0 y 255 separados por puntos y que identifica un ordenador conectado a Internet. Obviamente, este sistema no se utiliza para la navegación por las dificultades que supondría recordar esta serie de memoria. En su lugar, el DNS (Domain Name System o Sistema de Nombres de Dominio) traduce esos números a direcciones web, tal y como normalmente las utilizamos en los navegadores, que son fáciles de reconocer y recordar.

- **Uso de Web *"Beacons"* [86].** Son imágenes electrónicas que permiten al sitio web conocer quién y qué contenido online ha sido visitado. Normalmente estas imágenes son incluidas en correos electrónicos, anuncios, etc. Dependiendo del tipo de acceso, esta información podría incluir los siguientes datos:

    - Dirección IP de origen de la conexión.
    - Programa gestor de correo electrónico que se utiliza.
    - Sistema operativo empleado.
    - Momento de la conexión o visualización de la página o mensaje.
    - Información sobre direcciones de correo electrónico válidas.

  Estas y otras informaciones obtenidas pueden utilizarse con diferentes fines, incluso como ataques al usuario (abusando de vulnerabilidades conocidas de los programas que utiliza), confirmación de direcciones electrónicas (para envío masivo de correo electrónico no deseado o para comercialización de bases de direcciones confirmadas), etc.

- **Que el perfil de usuario sea indexado automáticamente por los buscadores de Internet.** La mayor parte de las plataformas analizadas para la elaboración del informe, y salvo algunas concretas que así lo han trasladado en las entrevistas mantenidas, permiten que los motores de búsqueda de los principales buscadores de Internet puedan indexar los perfiles de los usuarios de forma pública en la Red.

  En algunos casos dicha indexación incluye el nombre del usuario registrado, su fotografía del perfil y el nombre y fotografías del perfil de los amigos o contactos con los que cuenta en la red social, así como una invitación general a entrar a formar parte de la plataforma.

  Este hecho supone una amenaza para la protección de datos personales de los usuarios, en la medida en que sus datos básicos y principales contactos se exponen públicamente en la Red, accesibles por parte de cualquier usuario, pudiendo llegar a ser empleadas esas informaciones de forma descontrolada por terceros, sin que éstos queden en el "circulo cerrado" de la red social.

  Además se debe considerar que la Agencia Española de Protección de Datos ha tutelado el derecho a oponerse a la indexación del nombre o de otro tipo de datos de

[86] Un web bug o web beacon es una diminuta imagen en una página web o en un mensaje de correo electrónico que se diseña para controlar quién lee el mensaje. Su tamaño es inapreciable, pudiendo ser un píxel en formato GIF y transparente. Se representan como etiquetas HTML. Un web bug permite tener cierta información sobre el usuario (visitante de página web ó lector de mensaje de correo electrónico).

carácter personal en los buscadores ya que supone un tratamiento automatizado de datos, que debe ajustarse a todas las obligaciones dispuestas en la normativa vigente[87].

- **La recepción de publicidad hipercontextualizada.** La publicidad online es el modelo de explotación comercial más utilizado actualmente por parte de las redes sociales. Estas pueden determinar un grado de exactitud casi absoluto respecto del tipo de productos y servicios que el usuario va a demandar gracias a la cantidad de información que tratan respecto a cada uno de sus miembros; aunque de forma automatizada y mediante la aplicación de algoritmos de indexación basados en lógica *"booleana"*[88].

- **La recepción de comunicaciones comerciales electrónicas no solicitadas (*spam*).** Cada vez más, las redes sociales están siendo empleadas por *spammers* como fuentes para recabar información y datos personales a los que posteriormente se dirigirán comunicaciones comerciales no deseadas. Caben varios tipos de *spam* dentro de las redes sociales:

  En primer lugar, **cuando el usuario empieza a operar en la plataforma** y se da de alta en varias aplicaciones o grupos y, posteriormente, **decide enviar una invitación a todos sus contactos** sobre el registro en dichas herramientas.

  El usuario está remitiendo a sus contactos una serie de comunicaciones, que aunque en principio no parezcan contar con un carácter eminentemente comercial, reportan importantes cantidades económicas para las plataformas y desarrolladores de este tipo de aplicaciones, cuyo valor aumenta en la medida en que existan más o menos usuarios registrados en las mismas.

  El segundo supuesto consiste en que **el usuario permite que la aplicación o red en concreto acceda a su libreta de direcciones de correo electrónico para remitir a todos sus contactos un correo electrónico comercial animando a que se registren en la red.**

  La Agencia Española de Protección de Datos ha señalado en los casos en que la comunicación tiene formato y contenido eminentemente comercial, que si la dirección IP desde donde se remite es de la propia plataforma y si los que la reciben, a pesar

[87] Procedimiento TD/00463/2007

[88] Se trata de un sistema algebraico definido en un conjunto B, el cual contiene dos o más elementos y entre los cuales se definen dos operaciones denominadas "suma u operación OR" (+) y "producto o multiplicación u operación AND" (+).

de ser por mediación de un usuario, no han prestado su consentimiento expreso para ello, se estaría ante un caso de comunicación electrónica no deseada o *spam*[89].

Por otra parte, cuando el usuario admite que se envíen invitaciones a usuarios no registrados en la plataforma para convertirse en nuevos miembros, esta actuación podría llegar a ser interpretada como una forma de comunicación comercial electrónica no deseada, aunque habría que atender a las circunstancias concretas de cada caso.

- **La suplantación de identidad de los usuarios de la red social.** El concepto de "***suplantación de identidad***" recogido como delito en nuestra normativa penal, adopta una nueva trascendencia en el mundo online, dado que cualquier usuario puede contar en Internet – y normalmente así sucede- con varias ***"identidades digitales"***.

  Desde luego que no se trata de un comportamiento negativo, sin embargo la posibilidad de que la identidad de una persona sea registrada por otra persona ajena aumenta considerablemente. En este sentido existen medidas –analizadas en el capítulo de recomendaciones del Estudio- para conseguir que la red social en la que se esté produciendo esta situación, lleve a cabo la baja de los *usuarios ficticios*, previa autenticación de la verdadera identidad del usuario suplantado.

Así, **el tercer momento crítico para la protección de datos personales** se sitúa en la fase en la que el usuario pretende darse de baja del servicio. En este momento, deben tenerse en cuenta los siguientes aspectos que pueden poner en riesgo la seguridad y protección de datos personales de los usuarios:

- **La imposibilidad de realizar la baja efectiva del servicio.** Comprobados los procesos de alta, utilización y baja en las redes sociales analizadas, se ha detectado como en algunos casos, a pesar de solicitar la baja del servicio conforme a las políticas de privacidad recogidas en algunas plataformas, la baja del servicio no se ha llevado a cabo de manera efectiva, manteniéndose los datos personales de los usuarios a disposición de los responsables de la red social.

  Es frecuente que el usuario que intenta darse de baja del servicio, se encuentre con procedimientos complejos que nada tienen que ver con el procedimiento

[89] En este caso se debe considerar la reciente Resolución de la Agencia Española de Protección de Datos. La clave de la resolución se encuentra en el siguiente párrafo *"El envío publicitario que el denunciante manifiesta haber recibido, corresponde a una campaña continua de captación de clientes que promueve el demandado. Dicha campaña consiste en ofrecer a los clientes registrados la posibilidad de recomendar a sus familiares y amigos los servicios de Iniciativas Virtuales a través de la página web, para lo cual existe en dicha página web una facilidad que permite remitir a una dirección de correo electrónico un mensaje informativo invitando al destinatario a registrarse en ella. El mensaje que recibe el destinatario incluye un botón que enlaza directamente con la página de inscripción de clientes."*

automatizado y electrónico de alta en la plataforma. Este hecho implica un riesgo para la seguridad y protección de datos personales de los usuarios.

- **La conservación de datos y el cumplimiento del principio de calidad de los datos.** Por último, cabe señalar el posible riesgo que supone el hecho de que **las redes sociales y otros prestadores de servicios de la sociedad de la información conserven los datos de tráfico generados por los usuarios en el sistema**, para utilizarlos posteriormente como herramientas a través de las que sectorizar y conocer las preferencias y perfiles de los usuarios para realizar publicidad contextualizada con el medio y contenido de sus comunicaciones a través de la Red, afectando de esta forma al **principio de calidad de los datos.**

  En este sentido, tanto el Grupo de Trabajo del Artículo 29 en su "Dictamen sobre cuestiones de protección de datos en relación con buscadores", como la AEPD en su "Declaración sobre Buscadores de Internet"[90], publicada el día 1 de diciembre de 2007, la cuestión de la conservación de datos personales de los usuarios. La preocupación de las autoridades de protección de datos al respecto ha provocado que durante el mes de septiembre de 2008 uno de los principales buscadores de Internet haya acordado que guardará los datos personales de los usuarios durante un plazo de 9 meses. No obstante, las redes sociales aún no se han pronunciado al respecto, manifestando únicamente en sus políticas de privacidad que los datos serán tratados mientas dure la relación entre el usuario y la plataforma, obviando por tanto la información en cuanto al periodo concreto de conservación.

  Aunque el caso particular de las redes sociales no es idéntico al de los buscadores, se puede concluir que las redes sociales, como servicios de la Sociedad de la Información, deben someterse a la aplicación de la normativa de protección de datos, debiendo atender a los principios básicos que rigen la norma, como son el **principio de calidad** de los datos en la medida en que no deben conservar los datos de forma indefinida en sus servidores, el **principio de consentimiento**, en la medida en que no pueden tratar datos de carácter personal sin que haya mediado el consentimiento por parte del titular de los datos y el **principio de información**, en la medida en que deben informar de forma clara y comprensible a todos los usuarios respecto a qué van a hacer con sus datos y del derecho a disponer respecto a los mismos en cualquier momento.

3.2.4 Colectivos especialmente vulnerables. Menores e incapaces.

Por lo que respecta a las medidas existentes en materia de protección de datos personales de especial protección para colectivos considerados especialmente

90 https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/declaracion_aepd_buscadores.pdf

vulnerables –menores e incapaces- , cabe señalar que **desde el punto de vista normativo**, tiene especial importancia la publicación del Real Decreto 1720/2007, que aprueba el nuevo Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (RDLOPD). Hasta su aprobación, no existía en España referencia expresa al tratamiento de datos de los menores.

El nuevo reglamento introduce una importante especialidad en lo que respecta a la prestación del consentimiento por parte de estos menores al disponer que **para recabar los datos de cualquier menor de 14 años es necesario contar con el consentimiento de los padres o tutores.**

La norma señala además de manera expresa que **al recabar el consentimiento del menor debe utilizarse un lenguaje sencillo y fácilmente comprensible para el y que no se podrá obtener a partir de ellos información respecto a sus familiares y allegados.**

El responsable que recaba y trata datos personales de menores de edad será el responsable de articular **los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento** prestado en su caso, por los padres, tutores o representantes legales.

Estas medidas normativas implican que las redes sociales y plataformas colaborativas tienen la obligación de disponer medios tecnológicos que garanticen la identificación de la edad de los usuarios.

Sin embargo, y a pesar de la obligación dispuesta por la norma, en la medida en que los proveedores de servicios, los fabricantes y distribuidores de soluciones de seguridad y las entidades públicas no implementen sistemas efectivos, la identificación de los menores, y por ende el tratamiento de sus datos, se encuentran ante un riesgo, en la medida en que éstos podrían estar siendo tratados bajo un consentimiento no válido.

La Agencia Española de Protección de Datos ha sancionado la falta de diligencia en la comprobación de la identificación de un menor que se registró en un sitio web, cuyos datos se utilizaron para remitirle publicidad[91].

Por lo que respecta a posibles **situaciones particulares de riesgo que pueden conllevar aspectos negativos para la seguridad y protección de datos de los menores e incapaces**, cabe señalar que realizado un grupo de trabajo específico con menores de edad de entre 14 y 16 años en la fase de investigación de este Estudio, todos coincidieron en manifestar que a pesar de su edad, son usuarios habituales de este tipo de plataformas, en las que en ocasiones publican información personal y familiar.

[91] Procedimiento PS/00281/2007

Por ello, surge la necesidad de avanzar en la investigación y desarrollo de medios de identificación de la edad para alcanzar una solución efectiva y que no suponga un freno para el desarrollo de las Sociedad de la Información entre los más jóvenes.

Sin embargo, no basta con soluciones tecnológicas. Como destacó el Director de la Agencia Española de Protección de Datos en su intervención ante la XXX Conferencia Internacional de autoridades de protección de datos[92] los riesgos para los menores en Internet parten en gran medida de un déficit educacional básico: desconoce como ejercer un verdadero control sobre su información.

La formación actual a los menores en el uso de las nuevas tecnologías, con sus riesgos y ventajas, es insuficiente. En la escuela, no se aprende a controlar la información personal ni a identificar los riesgos en la Sociedad de la Información. La formación sobre protección de datos no se ha trasladado a los programas de estudio. Por ello, resulta ineludible el compromiso real y efectivo de organismos y autoridades educativas tanto de carácter internacional como nacional.

3.2.5 Medidas empleadas para proteger los datos personales de los usuarios.

Como han declarado las redes sociales entrevistadas, para la correcta protección de los datos personales de los usuarios, es imprescindible que estos valoren el tipo de datos que publican en su perfil. Además consideran crucial, que las organizaciones públicas y privadas realicen, desde el momento en que se produce el registro y se crea el perfil de usuario, labores de información, formación y concienciación sobre los peligros de la publicación excesiva de contenidos.

A **nivel técnico**, cabe señalar las siguientes acciones:

- *Eliminar los datos obsoletos que pudieran existir en distintos servidores , así como el cifrado de aquellos que estén en uso*, minimizando así los daños que pudieran resultar de un ataque desde el exterior por parte de usuarios malintencionados

- *Establecer mecanismos de análisis respecto de la fortaleza de la contraseña* de manera que se obligue al usuario a seleccionar una que no sea fácilmente descifrable por terceros[93].

- *Disociar los datos incluidos dentro de un perfil de usuario* para que en el caso de acceso por terceros no autorizados estos no puedan acceder a los datos de los usuarios y emplearlos con fines malintencionados.

[92] 30th International Conference of Data Protection and Privacy Commissioners in Strasbourg. http://www.privacyconference2008.org/

[93] El artículo "Recomendaciones para la creación y uso de contraseñas seguras" del Observatorio de la Seguridad de la Información de INTECO ofrece información relevante para un uso adecuado de contraseñas.

- Crear categorías de perfiles para controlar el volumen de datos personales que el usuario permite que resulten visibles al resto de usuarios.

- La creación de categorías de autorizaciones por ellos mismos sobre quién puede visionar sus perfiles. En este sentido cabe destacar los siguientes elementos:

    - Limitar el grado de publicidad del perfil del usuario conforme a los criterios anteriormente expuestos.

      La posibilidad de limitar y regular el alcance de publicidad de un perfil permite al usuario modular el grado de exposición de las informaciones y datos personales que incorpora en la plataforma respecto al resto de usuarios. Esta medida otorga al usuario un control real sobre las informaciones que incorpora en la plataforma.

    - Limitar la indexación de los perfiles por parte de los principales buscadores de Internet.

      Con esta medida se protege a los usuarios de una determinada plataforma de las búsquedas indiscriminadas que en ocasiones se realizan a través de los motores de búsqueda y que en un momento dado puedan proporcionar a la persona que realiza la búsqueda, información personal del usuario de la red social.

    - Limitar la visualización del perfil de manera geográfica.

    - Limitar la cantidad de datos que los usuarios pueden introducir: así por ejemplo ciertas plataformas deciden operar con perfiles de *nickname* o seudónimo para que sean los propios usuarios los que consideren a quien mostrarse (por ejemplo *vi.vu*).

Métodos de denuncia y otras acciones:

- *Medios a través de los que denunciar situaciones que afecten a sus datos personales o intimidad en la red social*, debiendo existir un departamento en las redes sociales para que de forma automatizada en una primera fase se bloqueen dichos contenidos y en una segunda pasen a ser analizados caso por caso por persona físicas. Esta medida permite a los usuarios reclamar de forma instantánea cualquier posible vulneración de la intimidad o un uso inadecuado de los datos de carácter personal del usuario.

- A la hora de recoger datos e informaciones sobre sus usuarios, las plataformas deben guiarse por el *principio de moderación*, de tal forma que solo soliciten aquellos datos que realmente son relevantes para la finalidad de la plataforma.

- Es igualmente necesario destacar que algunas plataformas de servicios de Internet están comenzando a iniciar *programas de formación y concienciación externa* en instituciones escolares y centros educativos, con la finalidad de lograr que, tanto profesores, como alumnos conozcan completamente todos los beneficios y riesgos que puede suponer el uso de este tipo de servicios.

3.3 Protección de los Derechos de Propiedad Intelectual sobre los contenidos

La facilidad de reproducción y distribución de contenidos hacen de Internet uno de los principales medios de crecimiento para los contenidos de propiedad intelectual, al tiempo que supone uno de los principales retos en lo que respecta al control y protección de los derechos de autor, en la medida en que los contenidos se encuentran en formato digital y, por tanto, su distribución y comunicación pública es mucho más sencilla que en otro tipo de formato.

El modelo de generación de contenidos ha variado en gran medida respecto al existente antes del surgimiento de la Web 2.0, dado que hoy en día los contenidos no son generados por los propios autores en exclusiva, sino que cualquier usuario tiene la capacidad de generar y difundir sus obras de propiedad intelectual, convirtiéndose así en autor y potencial productor y distribuidor.

Las redes sociales y, en especial, las plataformas colaborativas de contenidos multimedia (Youtube, Dalealplay.com, Myspace, Google video, Redkaraoke, etc.), son el mejor ejemplo de las posibilidades que brindan este tipo de plataformas a los autores[94].

3.3.1 Definición del derecho

A la hora de analizar la protección del Derecho de propiedad intelectual en los servicios de la Sociedad de la Información, conviene tener en consideración las siguientes premisas:

- Se considera autor a la persona física o jurídica que crea una obra.

- La propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el sólo hecho de su creación.

- Los derechos de propiedad intelectual se componen tanto de derechos personales, como de los derechos de explotación sobre la obra.

[94] Extraído de "*Web 2.0, El Negocio de las Redes Sociales"*, realizado por la Fundación para la Innovación de Bankinter y la Fundación Accenture, publico en 2007.

- Son consideradas obras de propiedad intelectual las obras literarias, artísticas o científicas.

La protección se dirige, por tanto, **al derecho que el autor tiene sobre su creación literaria, artística o científica.**

La protección comprende tanto los derechos de carácter moral, como los patrimoniales, atribuyendo al autor la plena disposición y el derecho exclusivo a la explotación de sus obras.

- **Derechos morales**: son derechos inherentes a la persona física y, por tanto, irrenunciables, encontrándose entre ellos la "paternidad" de la obra, la integridad de la misma, la decisión sobre su difusión y el reconocimiento de su autoría.

- **Derechos patrimoniales**: son derechos cuantificables económicamente y que pueden ser dispuestos por los sujetos titulares (personas físicas y jurídicas). Estos derechos son los relativos a las actividades de reproducción, distribución, comunicación pública y transformación.

En este sentido, **el titular es el sujeto legitimado para autorizar la reproducción, puesta a disposición o transmisión de una obra de propiedad intelectual sobre su propiedad,**[95] quedando limitado por las posibilidades otorgadas por el derecho de cita, los trabajos de actualidad y las reproducciones provisionales o copias privadas, entre otras.

3.3.2 Marco jurídico aplicable: normativa y evolución legislativa

La legislación en materia de propiedad intelectual tiene por objeto **proteger los derechos sobre las obras artísticas, científicas o literarias de los autores y del resto de intervinientes**[96]**.**

Normativa internacional

La normativa internacional, en materia de propiedad intelectual, se encuentra en una situación claramente ventajosa respecto a otros aspectos analizados en este Estudio. Así, en el año 96 se propuso en el seno de la Organización Mundial de la Propiedad Intelectual -OMPI o WIPO- la aprobación de dos tratados para regular la materia a nivel global:

[95] Art.2 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

[96] Art.1 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

- **WIPO Copyright Treaty (Tratado de la OMPI sobre derecho de autor), que entró en vigor el 6 de marzo de 2002**. Su objeto viene definido por la protección de las obras literarias y artísticas, tales como libros, software, música, obras fotográficas, obras plásticas y obras cinematográficas.

- **WIPO Performances and Phonograms Treaty (Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas), que entró en vigor el 10 de mayo de 2002**. Destinado a proteger los derechos de los productores de fonogramas, así como los derechos de los artistas, intérpretes o ejecutantes cuando sus obras se fijan en cualquier tipo de soporte.

Estas normas suponen un gran avance en la modernización de la legislación internacional, al dotar de mayor grado de protección a los derechos de los autores, y al establecer unos criterios y estándares básicos al desarrollo e implantación de las medidas de protección de la propiedad intelectual en los servicios de la Sociedad de la Información, llegando a ser comúnmente conocidos como los *"Tratados sobre Internet".*

Ambos tratados exigen la creación de un marco de derechos básicos, que permita a los creadores ejercer un control y/o percibir una remuneración por las distintas formas en que se usan y disfrutan sus creaciones. Pero el factor más importante es la protección adecuada y eficaz que dichos tratados otorgan a los titulares de estos derechos, cuando sus obras se difunden empleando las nuevas tecnologías y sistemas de comunicación como Internet. En este sentido, los tratados establecen:

- Que el derecho de reproducción es de aplicación al entorno digital y al almacenamiento de material en formato digital en un medio electrónico.

- Que los titulares de los derechos pueden verificar si los distintos consumidores tienen acceso en línea a sus creaciones y en qué forma, por ejemplo, desde sus hogares a través de Internet.

Para mantener un equilibrio de intereses entre los titulares de los derechos y los consumidores se especifica que los Estados gozarán de flexibilidad para fijar excepciones o limitaciones a los derechos en el entorno digital, respecto de los usos considerados de interés público, para fines educativos y de investigación.

Esta normativa no regula de forma expresa los servicios de la Sociedad de la Información objeto de estudio en este informe -redes sociales y sitios web colaborativos-, ya que en el momento de aprobación de los mismos estos servicios avanzados aún no existían o se encontraban en una fase inicial o embrionaria.

En EE.UU. la norma básica en materia de protección de derechos de propiedad Intelectual es la ***Digital Millenium Copyright Act*** (en adelante, **DMCA**), de **28 de**

octubre de 1998, en la que se dispone la exoneración de responsabilidad de los prestadores de servicios de Internet o ISP respecto de la información transmitida, alojada o difundida por los usuarios a través de sus sistemas de información. Esta exención de responsabilidad, reconocida en la mayor parte de los Estados a nivel mundial, establece que será aplicable siempre que el prestador de servicios de Internet:

- No tenga conocimiento u obtenga beneficio económico de la actividad ilícita.
- Disponga de una política sobre propiedad intelectual publicada en su sitio web, que sea accesible por los usuarios.
- Y, cuente con un responsable que atienda las denuncias por infracción de derechos.

Normativa europea

A nivel europeo, dentro de las áreas legales de propiedad intelectual y nuevas tecnologías se encuentra la **Directiva 2001/29/CE, del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información**,[97] en virtud de la cual los Estados miembros establecen el derecho exclusivo a autorizar o prohibir la reproducción directa o indirecta, provisional o permanente, *por cualquier medio y en cualquier forma*, por lo que se hace extensible a las redes sociales y este tipo de plataformas.

De igual forma, se dispone que los Estados miembros establecerán, en favor de los autores, el derecho exclusivo a autorizar o prohibir cualquier comunicación pública de sus obras, mediante procedimientos alámbricos o inalámbricos, incluida la puesta a disposición del público de sus obras.

Normativa nacional

Como la gran mayoría de normas de los países de nuestro entorno, la Ley de Propiedad Intelectual concede a los autores de las obras *derechos en exclusiva* sobre éstas, lo que supone que *cualquier tratamiento, reproducción, puesta a disposición o transmisión de la obra deberá ser realizada con la autorización de los titulares de derechos*. Tanto la normativa nacional, como la comunitaria, parten de un grado elevado de restricción de los derechos de explotación, de forma que *nadie puede explotar derechos de propiedad intelectual sin autorización por parte del autor*.

Desde el punto de vista normativo, España dispone de un gran elenco de normas encaminadas a la protección de los derechos de propiedad intelectual de los autores y,

[97] Disponible el texto completo de la Directiva 2001/29/CE

más específicamente, a la protección de la propiedad intelectual en los servicios de la Sociedad de la Información:

- **Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual (LPI),** regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, modificado por la Ley 23/2006,de 7 de julio.

- **Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE).**

- **Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información (LISI).**

- **Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.**

Sin embargo, a pesar de que se trata de normas actualizadas recientemente, con el objeto de regular el uso que se realiza de los contenidos de propiedad intelectual a través de los servicios de la Sociedad de la Información, existen dificultades de aplicación a la hora de alcanzar la protección plena de los derechos de los autores, produciéndose situaciones en las que obras de propiedad intelectual son comunicadas públicamente o reproducidas sin contar con la autorización previa del autor.

Para minimizar estas situaciones, la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE) dispone que *"los prestadores de servicios de intermediación no tienen obligación de supervisar los contenidos que alojan, transmiten o clasifican en un directorio de enlaces, pero deben colaborar con las autoridades públicas, cuando se les requiera para interrumpir la prestación de un servicio de la sociedad de la información o para retirar un contenido de la Red. Pueden incurrir en responsabilidad si, conociendo la ilegalidad de un determinado material, no actúan con rapidez para retirarlo o impedir el acceso al mismo".*

Al igual que los ISP, las redes sociales como proveedores de servicios de Internet tienen la capacidad técnica de controlar los contenidos en ellas alojados. Por tanto, en principio cabe exigirles un **deber general de control y supervisión de los contenidos ajenos, a modo de diligencia u observancia debida por el servicio que prestan.**

Desde el punto de vista de la regulación penal para la protección de la propiedad intelectual, la Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, dispone tres conductas relacionadas con su protección, si bien solamente se referencian aquellas que se encuentran directamente relacionadas con los servicios objeto de estudio:

- La distribución o comunicación pública de contenidos protegibles, ya sea mediante la distribución de copias físicas, o su puesta a disposición en Internet sin la autorización del titular de los derechos.

- La importación o fabricación de software o medios que permitan vulnerar las medidas de protección técnica incluidas en las obras, es decir, cualquier sistema que permita saltarse los sistemas antipiratería o anticopia de un determinado soporte o página web.

En relación con la protección de la propiedad intelectual y las redes colaborativas, la relevancia penal que supone difundir públicamente contenidos de forma online y mediante tecnología P2P *(tecnología ampliamente utilizada en los últimos tiempos por parte de servicios de streaming de vídeo online)*, así como la posibilidad de que se creen comunidades online encaminadas a la puesta a disposición de *links* para proceder a la descarga de obras de propiedad intelectual, ha sido analizada por parte de la Fiscalía General del Estado en su Circular 1/2006 *"Sobre los Delitos contra la Propiedad Intelectual e Industrial tras la reforma de la Ley Orgánica 15/2003"* [98], donde se dispone que el intercambio de archivos a través de redes P2P no es constitutivo, en principio, de los requisitos necesarios para poder ser catalogado como un delito contra la propiedad intelectual, sin perjuicio de que pueda reunir los requisitos para ser considerado un ilícito civil.

El elemento clave para determinar la existencia de esta situación, es que en principio no exista un ánimo de lucro directamente relacionado con la actividad, requisito esencial dispuesto por la normativa vigente para poder ser considerado delito. No obstante, se establece que deberá atenderse a las circunstancias concretas de cada caso.

3.3.3 Posibles riesgos. ¿Cómo pueden verse afectados los derechos de propiedad intelectual de los usuarios en una red social?

Desde el punto de vista de los posibles riesgos que se pueden producir contra la protección de la propiedad intelectual en Internet, en general, y en los servicios de redes sociales y plataformas colaborativas, en particular, deben diferenciarse dos situaciones en origen:

- De un lado, cómo se ven afectados los contenidos que son titularidad de terceros y que el usuario decide publicar dentro de la red social sin autorización de los titulares de derechos de propiedad intelectual.

[98] Para más información puede descargar la Circular de la Fiscalía General del Estado desde el sitio web: www.fiscal.es/fiscal/public

- De otro lado, las implicaciones jurídicas sobre las obras que sean titularidad de los propios usuarios y que éstos deciden compartir o hacer públicas a través de estas redes y plataformas.

Partiendo de estas consideraciones, se analizan los posibles riesgos para la propiedad intelectual atendiendo –como se ha hecho a lo largo del Estudio- a tres momentos clave en la *vida* de cualquier usuario en una red social: fase inicial de registro, fase de participación del usuario en la red social y fase de baja del servicio.

Así, el primer momento crítico para la protección de los derechos de propiedad intelectual respecto a los contenidos y obras elaboradas se encuentra en la **fase inicial de registro del usuario**, momento en el que éste acepta las condiciones de uso que en principio regirán toda su relación con la plataforma. El usuario debe leer, comprender y aceptar expresamente las condiciones de uso de la plataforma.

Aunque pudiera parecer que este hecho no reviste especial importancia, resulta esencial, en la medida en que los usuarios aceptan con frecuencia condiciones de uso relativas a la protección en materia de propiedad intelectual, por las que ceden plenamente sus derechos de explotación a las plataformas, para que los utilicen libremente durante el plazo máximo legal de 5 años.

Si a lo anterior se añade que la mayoría de las plataformas analizadas recogen condiciones de uso confusas, con redacciones frecuentemente extensas, de difícil comprensión y que habitualmente son alojadas en lugares del sitio web de difícil acceso para el usuario, se puede concluir que el número de usuarios que leen detenidamente y comprenden dichas condiciones legales no es alto.

Por consiguiente, es frecuente, según lo anteriormente expuesto que la cesión de todos los derechos de propiedad intelectual de los contenidos creados a favor de la plataforma se realice de forma poco reflexiva con lo que existe un posible riesgo para los usuarios que publican sus obras y creaciones en estas plataformas como medio de difusión.

El segundo momento en el que se pueden producir riesgos para los derechos de propiedad intelectual es en la **fase de participación del usuario en la plataforma** en la que puede publicar contenidos -propios o ajenos- para que sean compartidos con los demás miembros usuarios de la red social. En este momento pueden plantearse varias situaciones:

- **Que el contenido original haya sido creado por el propio usuario que lo publica.** En estos casos, el usuario cede, en la mayor parte de los casos, sus derechos de explotación sobre la obra, sin apenas límite territorial, durante un plazo de 5 años -plazo legal máximo- y sin derecho a recibir ningún tipo de compensación por ello. Por

lo tanto, se recomienda que el usuario valore a priori estas actuaciones que la red social puede realizar con dichos contenidos.

- **Que los contenidos publicados sean propiedad de terceros.** Cuando un usuario decide compartir dentro de la red social, ya sea con sus contactos o con toda la red, una determinada obra con titularidad de terceros, no debe olvidar -como se ha expuesto en el apartado de normativa- que la plataforma actúa en principio como mero intermediario, por lo que la responsabilidad de la publicación de dicho contenido recae directamente sobre el propio usuario.

Las redes sociales y plataformas colaborativas tienen una gran difusión, y **para los autores esta forma de distribuir contenidos puede ser muy ventajosa**. Sin embargo, el principal problema que se puede plantear es que no hay formas efectivas de controlar y obtener una compensación directa por el trabajo realizado.

Por otro lado, y con independencia de la titularidad, existe el riesgo de **que los contenidos (propios o ajenos) publicados por los usuarios en la plataforma puedan llegar a ser indexados por los motores de búsqueda de Internet,** lo que conllevaría que la difusión fuese mayor y por tanto que el número de reproducciones aumentase de forma exponencial, incrementando, en consecuencia, de forma directa la compensación al titular de los derechos.

Por último, el tercer momento en el que los derechos de propiedad intelectual pueden verse sometidos a un posible riesgo derivado del uso realizado en este tipo de plataformas, está en la **fase de baja del servicio por parte del usuario**.

En este sentido, conviene distinguir la situación de las *redes sociales basadas en perfiles* y l*as plataformas de contenido*s, ya que en las primeras, todos los contenidos asociados al perfil del usuario: fotografías, vídeos, obras literaria, etc., serán eliminados o al menos se bloqueará el acceso a los mismos, en el momento en que el usuario solicite la baja del servicio.

Sin embargo, en el caso de las plataformas de contenidos, los miembros pueden llegar a publicar obras sin asociarse directamente a su perfil de usuario, lo que puede provocar que, a pesar de que el usuario solicite la baja del servicio, el contenido permanezca accesible públicamente. La cesión de derechos a favor de la plataforma continuaría vigente, por lo que ésta podrá seguir beneficiándose de los contenidos alojados.

3.3.4 Colectivos especialmente vulnerables. Menores e incapaces

Por lo que respecta al colectivo de **menores e incapaces**, en materia de propiedad intelectual, el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual (LPI), no establece ninguna

especialidad respecto a los menores y el derecho de autoría, pudiendo ser autor de una obra de propiedad intelectual cualquier persona, con independencia de su edad.

Sin embargo, se ha de tener en cuenta que la normativa dispone que *"Los autores menores de dieciocho años y mayores de dieciséis, que vivan de forma independiente con consentimiento de sus padres o tutores o con autorización de la persona o institución que los tengan a su cargo, tienen plena capacidad para ceder derechos de explotación."*

Será por tanto necesario que aquellas plataformas que aceptan el registro de menores de 18 años, soliciten a éstos que autentiquen su mayoría de edad o, en su caso, que viven de forma independiente conforme a los requisitos dispuestos en la legislación vigente.

Otros supuestos: Trabajadores

Por lo que respecta a los **trabajadores**, la LPI establece en sus artículos 51[99] *(respecto a las relaciones laborales)* y 97 *(programas de ordenador)* las previsiones para la realización de obras sujetas a una relación laboral y al titular legítimo al que pertenece la autoría que, salvo pacto en contrario, suele ser del empleador o persona jurídica que la publique.

Para los autores que se encuentran bajo una relación laboral, conviene señalar dos conductas de las que **pueden derivarse una serie de riesgos:**

- El primero de los supuestos a analizar incluye el caso en el que un trabajador divulga por medio de una red social que está trabajando en una determinada obra o que anticipa de forma previa su lanzamiento.

  En ambos casos, estas conductas pueden lesionar derechos de propiedad intelectual y conllevar una vulneración de las normas expresadas en el Código Penal, ya que los autores de la obra, como derecho moral, deben poder decidir si publicarla o no y en que momento, sin entrar en consideraciones de mercado y de desventaja competitiva.

  En estos casos, se llega a poner a disposición una obra que puede no estar finalizada y que, además, se ha conseguido de forma ilegal, por lo que no se puede

[99] Sentencia de la Sala de lo Civil del Tribunal Supremo de 29 de Marzo de 2001, ha sido claro cuando ha afirmado que a partir del art. 51 LPI que la creación y cesión de una obra de autor se puede llevar a cabo por medio del contrato de trabajo y con sujeción a la legislación laboral; de tal forma que cuando el resultado del trabajo es una obra de autor la cesión de éste no tiene por qué abarcar a la integridad de los derechos de propiedad intelectual, sino sólo a los principales o más relevantes que son los de explotación de las mismas en atención a su actualidad.

Precisamente en ese precepto se indica que el hecho de que el empresario no ostente tal propiedad absoluta sobre los frutos del trabajo -en este caso- de un trabajador que crea una obra original no impide que dicha relación contractual se configure como una relación laboral. Así, es clara la rúbrica del citado precepto de la LPI cuando se refiere a *"La transmisión de los derechos del autor asalariado".*

exponer la excepción por copia privada. Tal caso de revelación de contenidos supondría el despido procedente del trabajador y la posibilidad de demanda civil de los titulares de la obra divulgada.

- El caso de desarrollo de aplicaciones regirá el artículo 97 LPI, donde se dispone que en el caso en el que un trabajador asalariado cree un programa de ordenador[100] durante su jornada de trabajo y mediante los medios puestos a disposición por ésta para tal efecto, éste será de titularidad plena de la empresa.

3.3.5 Medidas empleadas para proteger los derechos de propiedad intelectual de los usuarios y de terceros

Como se ha mencionado, tanto la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE) para el caso de España como la Digital Millenium Copyright Act (DMCA) en EE.UU., emplean el ***sistema de denuncia de infracción de derechos de propiedad intelectual***, mediante el cual el usuario puede notificar internamente a los administradores de la plataforma que existe una explotación no autorizada de derechos de propiedad intelectual, para que ésta pueda comprobarlo y en su caso retirar el contenido.

En este sentido, y tal y como ha traslado alguna de las plataformas analizadas, **existen acuerdos bilaterales con asociaciones de autores y grandes organizaciones propietarias de los derechos de explotación de las obras**, mediante los cuales son los propios titulares de los derechos de explotación los que se encargan de vigilar, revisar y en su caso retirar los contenidos que vulneren sus derechos.

Esta medida dota a cada uno de los titulares de accesos privilegiados a la plataforma, así como códigos de identificación y etiquetado de sus obras, de tal forma que sean detectables de forma sencilla y se permita una actuación rápida y eficaz.

De igual forma, en los últimos tiempos se está observando como cada vez más las grandes compañías de la industria de contenidos están llegando **a acuerdos bilaterales con las plataformas de difusión y redes sociales para abrir canales en los que alojar y publicar ellos mismos sus contenidos,** como contramedida frente a la publicación indiscriminada y descontrolada de contenidos de su propiedad por parte de los usuarios. De esta forma no se evita que se publiquen en la red, pero sí se realiza el control de los contenidos publicados.

Este tipo de medidas suponen una representación clara de que el mercado está cambiando, de que los agentes intervinientes están comenzando a ver en la Sociedad de la Información una oportunidad y no un obstáculo, lo que sin duda alguna augura unos

[100] Las aplicaciones generadas para las redes sociales no dejan de ser software, la única diferencia que tiene respecto a los programas más tradicionales, es el lenguaje de programación empleado en las mismas.

buenos resultados en los próximos años, tal y como expone el informe recientemente publicado por ASIMELEC, sobre *"La Industria de los Contenidos Digitales"*[101].

Por su parte, el **Tribunal del Justicia de las Comunidades Europeas** ha afirmado que los Estados miembros al incorporar a sus sistemas legales las directivas que protegen los derechos de autor en la sociedad de la información deben garantizar un justo equilibrio entre los derechos a la protección de datos personales, a la tutela judicial y a la propiedad[102].

Recientemente, el informe del **Parlamento Europeo**, que descartaba otorgar *"poder policial"* a los operadores de Internet, ha recibido el apoyo de la Comisión Europea, indicando que las operadoras *"no pueden restringir el acceso de los internautas ni los derechos fundamentales de los ciudadanos sin una autorización judicial previa"*[103], si bien la propuesta está pendiente de aprobación definitiva.

Del mismo modo, y desde el punto de vista público, en España, el **Ministerio de Cultura,** por acuerdo del Consejo de Ministros, aprobó el **Plan integral del Gobierno para la disminución y eliminación de las actividades vulneradoras de la propiedad intelectual** publicado en el BOE de 26 de abril de 2005,[104] que se centra en la lucha contra la piratería, así por ejemplo, se están centrando en las plataformas de compartición ilegal de contenidos.

La **Industria Discográfica y Audiovisual** ha formado lo que ellos mismos han venido a denominar *"La Coalición",* formada por SGAE, Promusicae (AIE y AGEDI), Federación para la Protección de la Propiedad Intelectual, la Asociación de Distribuidores Cinematográficos (ADICAN), la Asociación de Distribuidores de Vídeos (ADIVAN) y EGEDA, cuya finalidad está en fomentar la protección de los derechos de los autores que representan, mostrando especial atención a las vulneraciones que tienen su origen en los servicios de la Sociedad de la Información.

Por su parte, la Agencia Española de Protección de Datos ha formulado unas recomendaciones sobre la necesidad de aprobar una ley que permita proteger los derechos de autor de forma compatible con el derecho a la protección de datos personales[105].

[101] Más información: Informe 2008 de la industria de contenidos digitales. ASIMELEC

[102] STJCE de 29/01/2008. Asunto C-276/06. Promusicae.

[103] Para más información, acceda a Consumer Eroski Tecnologías de la Información.

[104] Se puede acceder al Plan desde www.mcu.es

[105] Memoria AEPD 2007, recomendación normativa 2ª.

3.4 Protección de los Consumidores y Usuarios

Los avances de las redes sociales y plataformas colaborativas están modificando las prácticas comerciales, redefiniendo la forma online de ofrecer bienes y servicios mediante la publicidad hipercontextualizada, según los perfiles de usuario, diversificando el mercado y creando nuevos canales de distribución.

Estos nuevos modelos de negocio basados en el comercio electrónico pueden despertar en origen un cierto grado de incertidumbre en los consumidores, en torno a cuestiones relativas a la seguridad de las transacciones electrónicas, al perfeccionamiento y validez de los contratos, a la normativa aplicable o la jurisdicción competente en caso de litigio, entre otras cuestiones.

Los siguientes epígrafes profundizan en el análisis de este tipo de cuestiones informando acerca de los instrumentos normativos y medidas tecnológicas que existen actualmente al servicio de los usuarios/consumidores de bienes y servicios a través de Internet para garantizar un entorno de tráfico económico seguro y confiable que garantice la total legalidad y transparencia en el proceso de compra de productos a través de Internet, en general, o de cualquier red social o plataforma colaborativa, en particular, desde la que se opere.

3.4.1 Definición del derecho

Por consumidor, se entiende *"toda persona física o jurídica que interviene dentro de una actividad comercial, con el objeto de adquirir un producto o servicio a un precio determinado, bien sea a través de comercio habitual o mediante transacciones de comercio electrónico"*.

A los efectos de determinar qué se entiende por "contratos celebrados a distancia", hay que atender a la siguiente definición: *"Los contratos celebrados a distancia son aquellos celebrados con los consumidores y usuarios en el marco de una actividad empresarial, sin la presencia física simultánea de los contratantes, siempre que la oferta y aceptación se realicen de forma exclusiva a través de una* ***técnica cualquiera de comunicación a distancia*** *y dentro de un sistema de contratación a distancia organizado por el empresario"* [106].

La propia norma dispone una serie de medios a través de los que se pueden realizar prestaciones de servicios a distancia, siendo los más habituales: *"los impresos, con o sin destinatario concreto, las cartas normalizadas, la publicidad en prensa con cupón de pedido, el catálogo, el teléfono -con o sin intervención humana- la radio, el teléfono con*

[106] Concepto dispuesto por el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

imagen, el videotexto con teclado o pantalla táctil, ***el correo electrónico****, el fax y la televisión",* entre otros.

Así, los *derechos de los consumidores* y usuarios, en lo que respecta a los contratos celebrados a distancia, tal y como dispone el **Título III del Real Decreto Legislativo 1/2007**, de 16 de noviembre, por el que se aprueba el texto refundido de la **Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias**, comprenden los siguientes principios:

- Derecho de información.
- Derecho de desistimiento.
- Garantías mínimas del producto.
- Envío de comunicaciones comerciales y publicidad engañosa.

3.4.2 Marco jurídico aplicable: normativa y evolución legislativa

La normativa vigente aplicable al sector de consumidores y usuarios tiene por objeto salvaguardar los derechos de los usuarios y velar por el cumplimiento de las obligaciones impuestas entre las partes intervinientes.

Normativa internacional

A nivel internacional no se dispone de convenio expreso sobre la materia. Sin embargo, existen recomendaciones y guías de la OCDE, procedentes de las distintas reuniones entre los ministros de comercio (y cargos asimilados) de los Estados. Entre ellas destaca la OECD Consumer Protection Guidelines (OCDE Guía de Protección de Consumidores) aprobada en septiembre de 1998 con una finalidad programática en la que se establecen los principios básicos para:

- Controlar las conductas comerciales fraudulentas.
- Solventar controversias y devolver objetos.
- Asegurar la privacidad de los datos del consumidor en las transacciones electrónicas.

En EE.UU., desde el punto de vista de los servicios de Internet en materia de protección de consumidores y usuarios, el órgano competente es la Federal Communication Comission (FCC) aunque, hasta la fecha, no se dispone de una regulación, a nivel general, para la defensa de este colectivo.

Normativa europea

A nivel europeo, la legislación vigente en materia de protección de consumidores y usuarios se encuentra dispuesta en cuatro Directivas:

- **Directiva 93/13/CEE del Consejo, de 5 de abril, sobre las cláusulas abusivas en los contratos celebrados con consumidores.**

- **Directiva 99/44/CE**, **de 25 de mayo, del Parlamento Europeo y del Consejo, sobre determinados aspectos de la venta y las garantías de los bienes de consumo.**

- **Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo, relativa a la protección de los consumidores en materia de contratos a distancia**.

- **Directiva 85/577/CEE del Consejo, de 20 de diciembre, referente a la protección de los consumidores en el caso de contratos negociados fuera de los establecimientos comerciales**.

Además, es reseñable la **Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior**, objeto de transposición en España, en la actual Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE) encargada de regular la prestación de servicios de la Sociedad de la Información.

Normativa nacional

Cronológicamente se debe referenciar, la **Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista,** cuyo objeto de regulación son las ventas a distancia, estableciéndose que son aquel tipo de ventas que se realizan "*sin la presencia física simultánea*" de las partes, siempre que, acciones esenciales del contrato, como la venta y la aceptación, se realicen por cualquier modo de comunicación a distancia y llevada a cabo dentro de un sistema de contratación organizado por el vendedor.

El **Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias**, sin perjuicio de lo dispuesto por la **LSSI-CE** en lo que respecta a la contratación electrónica, dispone qué información debe figurar en las ventas a distancia de forma clara, comprensible e inequívoca, antes de iniciar el procedimiento de contratación:

- La identidad del vendedor o prestador de servicios y su dirección.

- Las características esenciales del producto o servicio.
- El precio, incluidos todos los impuestos.
- La forma de pago y modalidades de entrega o de ejecución.
- La existencia de un derecho de desistimiento o resolución y las causas del mismo.
- El coste de la utilización de la técnica de comunicación a distancia, cuando se calcule sobre una base distinta de la tarifa básica.
- El plazo de validez de la oferta y del precio.
- La duración mínima del contrato.
- En su caso, indicación de si el vendedor dispone o está adherido a algún procedimiento extrajudicial de solución de conflictos.

Cuando el usuario sea a la vez consumidor, obtendrá inmediatamente los derechos contemplados en la legislación sobre consumidores y usuarios, que serán irrenunciables y ejercidos automáticamente, aunque la legislación aplicable no sea la española. Esto ocurrirá siempre y cuando el contrato presente un vínculo estrecho con cualquier Estado miembro, pudiéndose aplicar en este momento los principios recogidos en la LSSI-CE sobre el país de destino de la prestación de los servicios.

La contratación a distancia puede realizarse incluyendo condiciones generales de la contratación, las cuales tendrán que estar incorporadas al contrato, ser aceptadas por el usuario y firmadas o aceptadas por ambos contratantes. Las condiciones generales no primarán nunca sobre las específicas, salvo que las generales sean más beneficiosas para el adherente. Las dudas sobre las condiciones generales siempre se resolverán en sentido que favorezcan al adherente. En este sentido, se ha de partir de la **Ley 7/1998, de 13 de abril, sobre Condiciones Generales de la Contratación (LCGC).**

El uso de condiciones generales de contratación es el empleado de manera frecuente en los procedimientos de contratación online. Se trata de *contratos de adhesión en los que los usuarios/consumidores no disponen de ningún tipo de capacidad de decisión y variación del clausulado*, debiendo aceptar, en todo caso, las condiciones que el empresario hubiera dispuesto. Es por esto que la normativa vigente pretende aumentar el grado de protección de los usuarios/consumidores de este tipo de procedimientos de suscripción a servicios.

No se incorporarán al contrato las cláusulas generales que el adherente no haya tenido oportunidad real de conocer plenamente en el momento de celebrar el contrato o que no

hayan sido firmadas en virtud del artículo 7 de la LCGC. Por eso, *en los contratos electrónicos, es importante remarcar su existencia y ubicación, tanto en el momento de la firma del mismo, como antes de la iniciación del proceso de firma.* Además, las cláusulas deberán ser legibles, claras, simples y comprensibles, para no correr el riesgo de nulidad recogido en el artículo 8 de la LCGC. Cuando una serie de cláusulas sean consideradas nulas, pero con las restantes y las particulares el contrato pueda seguir subsistiendo, éste no será considerado ineficaz.

Por último cabe resaltar lo dispuesto por la normativa específica para la regulación del comercio electrónico en España, concretamente en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE), en la que se dispone que "*los contratos celebrados por vía electrónica producirán todos los efectos cuando concurran el consentimiento y los demás requisitos necesarios para su validez".* Además, se regirán por el Código Civil, el Código de Comercio y las leyes referenciadas anteriormente.

3.4.3 Posibles riesgos. ¿Cómo pueden verse afectados estos derechos?

En algunos casos los posibles riesgos a los que se puede enfrentar un consumidor -como usuario de redes sociales- pueden ser asumidos por el propio usuario, ya que es él mismo quien mantiene el control de la información alojada en la plataforma o red social en la que, de forma voluntaria, se ha registrado.

En función de su actividad, todo proveedor establecido en España debe cumplir con ciertas obligaciones que la LSSI-CE establece con el fin de garantizar que su actividad se realice con total transparencia, sin vulnerar los derechos de los usuarios.

Así, el art. 10 LSSI-CE recoge una serie de obligaciones a cargo de los prestadores de servicios de la Sociedad de la Información, con el objeto de preservar el derecho de información a consumidores y usuarios respecto de los bienes o servicios que les son proporcionados. En concreto, se debe informar del:

- Nombre o denominación social, domicilio, dirección de correo electrónico y cualquier otro dato que permita establecer una comunicación directa y efectiva.
- Los datos de inscripción en el Registro Mercantil.
- Datos relativos a autorizaciones – en caso de estar sujeto a ello - .
- Si ejerce una profesión regulada deberá indicar: datos del Colegio profesional, titulación académica oficial, lugar de expedición y homologación, y si fuere el caso, sobre las normas profesionales aplicables al ejercicio de su profesión.
- El número de identificación fiscal que le corresponda.

- Información clara y exacta sobre el precio del producto o servicio, indicando si incluyen o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

- Los códigos de conducta a los que esté adherido.

Otro posible riesgo con el que se puede encontrar un consumidor en el momento de manifestar su interés por contratar un determinado servicio ofrecido a través de una plataforma colaborativa o red social, es el referido a la ***publicidad engañosa***, que consiste en aquella manifestación de publicidad ilícita, llevada a cabo en cualquier forma de publicidad que induce o puede inducir a error a sus destinatarios, pudiendo afectar a su comportamiento económico o perjudicar a los competidores del anunciante.

En este sentido, la *Ley 34/1988, de 11 de noviembre, General de Publicidad* determina todos los elementos que caracterizan la publicidad engañosa (características de los bienes, precio, condiciones de contratación y motivo de la oferta).

La *aceptación de las condiciones generales de contratación* constituye otro aspecto fundamental a tener en cuenta por el consumidor antes de formalizar la contratación del servicio ofrecido a través de una plataforma colaborativa o red social. Como se ha señalado, la propia legislación establece la obligación de informar al usuario de forma clara y precisa, sobre las condiciones a las que están sometidas las partes dentro de la relación contractual.

No obstante, la aparición de cláusulas abusivas en un contrato constituye un defecto con implicaciones jurídicas trascendentales entre las partes. La propia normativa define como cláusula abusiva la siguiente: *"Todas aquellas estipulaciones no negociadas individualmente y todas aquéllas prácticas no consentidas expresamente que, en contra de las exigencias de la buena fe, causen en perjuicio del consumidor y usuario, un desequilibrio importante de los derechos y obligaciones de las partes que se deriven del contrato"*.

En cualquier caso, toda cláusula contractual que limite los derechos básicos de los consumidores y usuarios, que sea notoriamente desproporcionada en relación con el prestador o que prive del goce de los derechos que la propia normativa le concede, tendrá el carácter de cláusula abusiva.

Por lo que respecta a la responsabilidad del respeto a estas obligaciones y a las contraídas contractualmente con los usuarios en el ámbito del comercio electrónico y prestación de servicios electrónicos, son diversos los efectos de riesgo que pueden traducirse en posibles daños en perjuicio de los consumidores y usuarios, como puede ser el caso de las medidas técnicas para proteger las comunicaciones entre los usuarios o con la propia red.

El desarrollo de las nuevas tecnologías, unido al crecimiento de la actividad comercial a través de Internet, ha dado lugar a nuevas prácticas abusivas derivadas del incumplimiento en las disposiciones legales que, en casos más extremos, derivan en la comisión de delitos sancionados por la normativa penal.

Resulta obvio manifestar que cualquier persona que suba a la Red cualquier tipo de información o archivos –fuere o no prestador de servicios- ha de ser responsable de la licitud de los mismos. No obstante, la LSSI-CE no regula la actuación derivada de los proveedores de contenidos, simplemente se somete a los principios que rigen la actuación de particulares y empresas frente a Internet.

3.4.4 Casos Especiales. Menores de edad e incapaces

Normativamente, en España, la LSSI-CE establece que, en el caso de páginas web accesibles por menores, éstas no deben integrar contenidos que atenten contra los mismos, y que además la protección de la infancia y de la juventud tiene que ser uno de los valores que rija el entendimiento de toda la norma.

Actualmente existen mecanismos -programas informáticos de filtrado y bloqueo- de especial utilidad para controlar y restringir los contenidos o materiales a los que pueden acceder los menores.

En todo caso, es conveniente acompañar a los menores en su navegación por la Red, sobre todo, en los casos en los que se disponga de suscripciones a servicios *premium* o de pago.

3.4.5 Medidas empleadas para proteger los derechos de los consumidores y usuarios

Actualmente las medidas empleadas por las plataformas online que operan como sitios de comercio electrónico o que de alguna forma pueden verse sometidos a la normativa de consumidores son las siguientes:

Los **sistemas de identificación electrónica basados en certificados de firma electrónica reconocida**, están comenzando a ser utilizados por las plataformas de comercio electrónico como medio para garantizar las transacciones comerciales que los consumidores realizan.

La implementación y uso de este tipo de sistemas, permiten tanto al consumidor, como a la tienda de comercio electrónico garantizar:

- La identidad de la persona que compra y la que vende.
- La integridad del consentimiento prestado.

- El “no repudio” de la transacción.

De esta forma, cualquier usuario/consumidor que compre a través del sitio web:

- Tiene plena seguridad de que el titular del nombre de dominio y de la tienda online es la compañía que realmente vende los productos o presta los servicios.

- Puede demostrar que un día concreto, a una hora específica prestó su consentimiento y abonó una cantidad determinada a cambio del envío de un producto.

Por otro lado, el vendedor cuenta con:

- La capacidad tecnológica de acreditar la fecha y hora del consentimiento prestado electrónicamente por parte del usuario.

- La aceptación por parte del usuario/consumidor de las condiciones generales de contratación expuestas en el sitio web.

- En el caso de que el usuario niegue que fue él quien prestó el consentimiento requerido será carga suya el demostrarlo, reflejándose así el “no repudio” anteriormente mencionado.

En este sentido, es esencial tener en cuenta que la implantación plena de este tipo de sistemas de identificación electrónica se encontrará totalmente aplicada en el momento en el que el **DNI electrónico** alcance una penetración global para ciudadanos nacionales y europeos, momento en el que el desarrollo de la Sociedad de la Información se sustentará en principios más sólidos –que los actuales- de seguridad, identidad e integridad.

Del mismo modo, la gran mayoría de las plataformas analizadas que cuentan con procedimientos de compra electrónica recurren a la **instalación en sus servidores de un protocolo de puerto seguro, *(Secure Socket Layer o SSL)*** que garantiza a todos sus usuarios que las comunicaciones, solicitudes e informaciones transmitidas entre el sitio web y el usuario no son accesibles por parte de terceros no autorizados.

De igual forma, todas las plataformas que integran comercio electrónico, disponen de una **Terminal Punto de Venta –TPV- de pago electrónico proporcionada por una entidad financiera**, que somete todo el procedimiento de pago electrónico a un protocolo de seguridad debidamente certificado y que garantiza que el establecimiento no tiene acceso, ni conserva, ni trata los datos de tarjeta de los usuarios.

Por otro lado, se ha detectado la evolución clara por parte de las plataformas en relación al empleo de **medios de pago alternativos** que garanticen plenamente la seguridad de

las transacciones y **que prevean seguros de responsabilidad** para el caso de que el producto no se reciba o la transacción sufra algún tipo de error.

En este sentido, cabe destacar servicios como Paypal, pertenecientes al grupo de empresas de Ebay Inc, que ponen a disposición de consumidores y empresarios un medio de pago seguro, basado en direcciones de correo electrónico y tarjetas de crédito, que garantiza a los usuarios un seguro económico para todas y cada una de las transacciones que lleven a cabo a través de este sistema de pago.

Del mismo modo, supone una garantía para el usuario/consumidor de bienes y servicios de una red social, la **puesta a su disposición de las condiciones generales de contratación**, donde se disponen todas las cláusulas relativas a las garantías, plazos de devolución, precios, transportes, entre otras. No obstante, actualmente esta garantía no se encuentra totalmente implementada como se ha constatado por el análisis llevado a cabo respecto de las plataformas analizadas para la elaboración de este Estudio, al no disponer de documentos legales que cumplan de forma estricta con las obligaciones dispuestas en el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

4 PROPUESTAS Y RECOMENDACIONES DE ACTUACIÓN DIRIGIDAS A LOS AGENTES INTERVINIENTES EN LAS REDES SOCIALES

Si bien es cierto que las redes sociales y sitios web colaborativos han supuesto una auténtica revolución en Internet, poniendo a disposición de los usuarios innumerables beneficios, es necesario que todos los agentes de la cadena de valor tengan en cuenta determinados aspectos relativos a la seguridad y protección de los usuarios, para procurar que la utilización de este tipo de servicios reporte beneficios y experiencias positivas para todos ellos.

Por ello, y para la correcta protección de los usuarios finales, es esencial que los principales sujetos de la cadena de valor dispongan y consideren la aplicación de una serie de recomendaciones de forma personalizada: *las redes sociales y plataformas colaborativas* (respecto de las necesidades jurídico–tecnológicas), los *servicios ISP o proveedores de acceso a Internet* (respecto de los aspectos tecnológicos y de seguridad), los *fabricantes y proveedores de servicios de seguridad informática* (respecto de las herramientas necesarias para fomentar la seguridad de los usuarios), las *Administraciones e Instituciones Públicas* (respecto de las medidas normativas, de concienciación y formación de los usuarios y agentes del mercado) y los *usuarios* (respecto del uso que deben hacer de este tipo de plataformas).

En este sentido, se hará especial hincapié en los siguientes aspectos:

- El conocimiento y valoración del grado de **cumplimiento** por parte de las redes sociales y plataformas colaborativas de la **normativa vigente** en España y en la Unión Europea.

- El conocimiento y valoración de los **sistemas de seguridad** instalados por las redes sociales y plataformas análogas, para lograr la protección de sus usuarios.

- El conocimiento y valoración de las **implicaciones sociológicas** que están conllevando las redes sociales y plataformas análogas en los hábitos de los usuarios.

- La obtención de datos estadísticos nacionales e internacionales sobre el **grado de uso, la situación de la seguridad jurídica y tecnológica**, así como de los **hábitos más relevantes entre los usuarios menores de las redes sociales.**

A partir de las entrevistas realizadas en el sector, así como de los grupos de trabajo realizados con especialistas en Derecho Tecnológico y en Seguridad de la Información, y usuarios mayores y menores de edad, a continuación se exponen las principales

propuestas y recomendaciones que los sujetos intervinientes en la cadena de valor han considerado.

4.1 Propuestas y recomendaciones dirigidas a la industria

4.1.1 Propuestas y recomendaciones dirigidas a las redes sociales y plataformas colaborativas

Se ha demostrado reiteradamente que aquéllas redes sociales y plataformas que **generan y mantienen el mayor grado de confianza con sus usuarios** son finalmente las que triunfan y se constituyen como las redes de referencia, tanto a nivel local como internacional.

Con las siguientes propuestas, se pretende que los proveedores de servicios de redes sociales y plataformas colaborativas dispongan de una serie de recomendaciones esenciales para que todos sus servicios se adecuen: a) a la normativa europea y nacional, b) a la protección de sus usuarios, c) a que conozcan las implicaciones jurídico tecnológicas que conlleva la realización de determinadas prácticas, d) a la identificación del tipo de herramientas tecnológicas necesarias en sus servicios, y e) a aumentar el grado de concienciación respecto de la necesidad de incrementar las medidas de seguridad y protección de los usuarios.

A continuación se exponen las recomendaciones específicas extraídas de las entrevistas y de los grupos de trabajo dirigidas a las redes sociales y plataformas colaborativas agrupadas en dos grandes bloques o niveles:

Recomendaciones tecnológicas y de seguridad

1. *Transparencia y facilidad de acceso a la información*

Tras la revisión y análisis de las plataformas con mayor número de usuarios registrados a nivel nacional e internacional, es necesario **aumentar el grado de transparencia y la facilidad de acceso a las condiciones del servicio.**

En este sentido, resulta fundamental que este tipo de plataformas exponga toda la información relativa a sus servicios de forma clara y comprensible, de manera **que el lenguaje empleado** en sus condiciones de uso y políticas de privacidad **sea absolutamente comprensible** para cualquier tipo de usuario permitiéndole conocer cuáles son sus derechos y obligaciones durante el uso del servicio.

De igual forma, es esencial que las redes sociales **destaquen dentro de sus páginas de inicio un apartado específico destinado a informar a los usuarios**, en cualquier momento de la navegación, respecto a cuáles son las condiciones del servicio y los efectos que conlleva cada una de las acciones que se realizan a través de la plataforma.

Para lograr la máxima efectividad se recomienda la **creación de *"microsites"*[107] con acceso directo desde la página principal** de la red social, **en los que se exponga información mediante "preguntas frecuentes" y contenidos multimedia** (vídeos, diapositivas online, etc.) que permitan a los usuarios conocer de forma sencilla y comprensible cuáles son las implicaciones que conlleva el uso del servicio, así como sus derechos y obligaciones.

Por último, se ha detectado que todas las redes sociales y plataformas analizadas se reservan en sus condiciones de uso y políticas de privacidad el derecho a ser modificadas en cualquier momento, sin necesidad de preaviso a los usuarios registrados que con anterioridad las hubieran aceptado.

En este sentido, es esencial **que las redes sociales mantengan su política de privacidad y condiciones de uso sin cambios importantes ni trascendentes para los usuarios** y que, en caso de ser necesarios, sean previamente comunicados, para que aquellos puedan leerlos y aceptarlos, permitiéndoles en todo caso la posibilidad de darse de baja del servicio de forma sencilla y efectiva.

2. *Garantizar a los usuarios el control absoluto del tratamiento de sus datos e información publicada en la red*

Con independencia del lugar desde el que operen las redes sociales, se recomienda la implementación de aquellas medidas que permitan cumplir con las obligaciones dispuestas en la normativa comunitaria o nacional, aumentando el bienestar y confianza de todos los usuarios y autoridades europeas.

Tal y como se ha indicado a lo largo del informe y se ha resaltado durante el estudio, las plataformas deben **garantizar a los usuarios que disponen del control absoluto de la información sobre sí mismos publicada en la red,** poniendo a su disposición el mayor número de herramientas tecnológicas, encaminadas a hacer efectivos sus derechos de forma automática, sencilla y rápida.

Es por ello esencial que todas las plataformas implementen, tal y como ya han hecho las principales redes sociales, herramientas que permitan:

- Ejercer automáticamente los derechos de acceso, rectificación, cancelación y oposición (ARCO) respecto a sus datos personales, publicados en su perfil o en el de otro usuario de la red.

- Informar siempre de forma expresa para qué se utilizan los datos personales y la información publicada en el perfil.

[107] Pequeñas páginas web, con contenidos específicos que dependen de una principal.

- Limitar la posibilidad de etiquetado de los usuarios dentro de la red, de tal forma que cualquier persona etiquetada con su nombre, reciba automáticamente una solicitud de aceptación o rechazo, impidiendo en este caso la publicación y tratamiento de datos no autorizados.

  De igual forma, esta medida deberá ir asociada a una herramienta que permita a cualquier usuario la retirada de contenidos en los que aparezca algún dato o información personal.

- Que los sistemas de denuncias implementados permitan que el usuario se dé de baja y bloquee el acceso por parte de cualquier otro usuario de la red a los contenidos denunciados, siendo éste un procedimiento completamente automático y de aplicación inmediata.

- Configurar por defecto el máximo grado de privacidad del perfil de usuario, permitiéndole que pueda graduarlo en función de sus preferencias.

Para evitar el tratamiento de datos no autorizado por parte de los buscadores de Internet, se recomienda a las plataformas la inclusión de las modificaciones pertinentes en el *código HTML* de la aplicación, impidiendo de esta forma **que los motores de búsqueda puedan indexar los perfiles de los usuarios**, debiendo ser los usuarios los que voluntariamente lo autoricen. De esta forma, se garantiza un mayor control de la información publicada en la red, y se evita que la misma sea accesible por cualquier persona que navegue por Internet.

Por último, y con el objeto de controlar el tipo de contenidos y la titularidad de los mismos, las plataformas deben tener en cuenta la importancia de la protección de los derechos de propiedad intelectual e industrial respecto a los contenidos de terceros publicados en la red. En este sentido, se recomienda a las redes sociales y plataformas análogas:

- Disponer de herramientas de denuncia interna que permitan a los propios usuarios notificar la existencia de contenidos protegidos por derechos de autor que están siendo utilizados o han sido publicados sin autorización de su autor.

- Disponer de personal interno o de herramientas automáticas que permitan revisar cada uno de los contenidos y determinen si, en efecto, se trata de un caso de vulneración de derechos o, por el contrario, se trata de contenidos libres de derechos (utilizando medidas técnicas como los DRM, marcas de agua y metadatos dentro de los propios contenidos).

- Informar debidamente a los usuarios de la naturaleza de los derechos de autor y de la importancia que tiene el respeto de los mismos para el correcto funcionamiento del servicio, a través de las condiciones generales de registro, preguntas frecuentes y

avisos espontáneos mostrados previamente al alojamiento de imágenes, vídeos y contenidos susceptibles de protección de los derechos de propiedad intelectual.

- Facilitar a los autores información relativa a las medidas tecnológicas existentes para proteger sus obras, tales como marcas de agua, sistemas DRM o semejantes.

- Establecer canales de comunicación entre las plataformas y las entidades de gestión de derechos de autor, así como con las principales editoriales y productoras, debiendo existir entre dichas entidades una colaboración constante en aras a garantizar a los autores el máximo número de compensaciones por la publicación y reproducción pública de los contenidos.

3. Garantizar la seguridad tecnológica de la plataforma

Asimismo, se ha puesto de manifiesto que todos los responsables de este tipo de plataformas deben tener en cuenta que estos servicios se basan en grandes bases de datos, con datos personales de los usuarios que las utilizan. Por ello, debe garantizarse que la red es segura frente a posibles ataques de terceros y, que impide, o al menos reduce, la posibilidad de éxito de éstos.

En este sentido, es vital la correcta elección por parte de la plataforma, de un prestador de servicios de Internet (Internet Service Provider o ISP) que cuente con un nivel de seguridad alto[108]. En este sentido, se recomienda que el ISP garantice en todo momento, al menos, los siguientes aspectos:

- Que sus **servidores de DNS[109]** sean **completamente seguros y no presenten ningún tipo de vulnerabilidad pública**, ya que la existencia de un fallo en la seguridad de los mismos puede conllevar una grave amenaza a la seguridad de la plataforma.

  Si el servidor de DNS fuera atacado, a pesar de que los usuarios visitasen el sitio web de su red social, podrían ser redirigidos a otra dirección web falsa, sin que aquellos pudiesen detectarlo, lo que supondría un grave riesgo.

- Emplear en los servidores y en la propia aplicación **herramientas especialmente destinadas a detectar, evitar y bloquear casos de *phishing* o *pharming***, advirtiendo al usuario de los grados de seguridad y confianza de cada una de las

[108] Los servicios prestados por los ISP a este tipo de plataformas se centrarán en servidores seguros, centros de respaldo, accesos seguros, etc.

[109] La dirección IP está formada por una serie numérica de cuatro grupos entre 0 y 255 separados por puntos y que identifica un ordenador conectado a Internet. Obviamente, este sistema no se utiliza para la navegación por las dificultades que supondría recordar esta serie de memoria. En su lugar, el DNS (Domain Name System o Sistema de Nombres de Dominio) traduce esos números a direcciones web, tal y como normalmente las utilizamos en los navegadores, que son fáciles de reconocer y recordar.

comunicaciones recibidas a través de la plataforma. En este sentido, se recomienda el fomento de acuerdos estratégicos con empresas de seguridad, para integrar en el propio servicio medidas que reduzcan el éxito de este tipo de ataques.

- **Emplear aplicaciones de seguridad encaminadas a garantizar, o en su caso minimizar, la posibilidad de recepción de mensajes comerciales no deseados** a través de la red social. Como se indica en el informe, la proliferación del *spam* a través de este tipo de plataformas está siendo muy alta, dado que estas plataformas cuentan con una capacidad viral muy elevada. Por ello es necesario que los responsables de los servicios adopten todas las medidas a su alcance para reducir la recepción por parte de los usuarios de comunicaciones electrónicas no deseadas.

- Dado que la normativa, en determinados Estados, exige a los prestadores de servicios de la Sociedad de la Información que controlen y limiten el acceso de menores de edad, se recomienda a los responsables de los servicios la **implementación de medidas tecnológicas que permitan conocer la edad de los usuarios**, tales como: el uso de certificados reconocidos de firma electrónica o de aplicaciones que detecten el tipo de sitio web visitado y los servicios más demandados, permitiendo así delimitar de forma aproximada su edad.

- Disponer internamente de **herramientas encaminadas a reducir los casos de suplantación de identidad por parte de usuarios** dentro de la red, permitiendo a los legítimos titulares de los servicios que puedan autenticar su verdadera identidad, para así recuperar y bloquear el acceso al usuario que ilegítimamente utilizó el perfil del otro.

- Que las plataformas integren **sistemas que detecten el nivel de seguridad de las contraseñas elegidas por los usuarios en el momento de registro**, indicándole si es o no segura e informándole de los mínimos recomendables.

  De igual forma, se recomienda a las plataformas ahondar en la posibilidad de emplear sistemas únicos para la identificación de los usuarios, con independencia del servicio al que se desee acceder y contando para ello con un mismo usuario y contraseña. De esta forma, los esfuerzos de seguridad únicamente será necesario realizarlos sobre un sistema de identificación.

- **Emplear sistemas que cifren el contenido alojado en la plataforma**, de tal forma que toda la información mostrada desde el sitio web al usuario siempre sea inaccesible por parte de cualquier tercero. Para ello se recomienda la implementación de una conexión segura mediante *Security Socket Layer (SSL),* que permita a cualquier usuario detectar mediante el candado de su navegador o el *"https"* de su dirección, que se encuentran bajo una conexión cifrada.

- **Emplear herramientas tecnológicas que impidan** que cualquier usuario pueda **descargar información publicada en los perfiles del resto de usuarios**, con independencia del tipo de contenido de que se trate. En este sentido, se recomienda limitar la descarga automatizada de los datos personales, así como las fotografías y vídeos publicados en los perfiles de usuarios, ya que de lo contrario sería posible la descarga masiva, creando bases de datos independientes de la red, con el consecuente riesgo que supone.

  No obstante, se recomienda la implantación de sistemas que no impidan absolutamente esta posibilidad, sino que trasladen al usuario la responsabilidad de decidir si acepta que otro usuario pueda descargar el contenido en cuestión.

- Se recomienda a las redes sociales y plataformas colaborativas **que permitan y fomenten entre sus usuarios el uso de seudónimos o nicks de usuario** que permitan la creación a partir de los mismos de auténticas **"identidades digitales".**

Recomendaciones en materia de formación y concienciación de los usuarios sobre la seguridad. El papel de las redes sociales

Existe la necesidad de que todas las redes sociales fomenten entre sus usuarios la formación y concienciación en materia de seguridad.

No debe olvidarse que este tipo de servicios se fundamentan en que los usuarios facilitan información propia a través de su perfil, siendo esencial que cuenten con recomendaciones en materia de seguridad que les aporte garantías de que este tipo de servicios es completamente seguro.

En este sentido, las redes sociales y plataformas colaborativas deben fomentar la concienciación y la formación de sus usuarios respecto de la protección de la privacidad, la intimidad y la protección de sus datos de carácter personal, la protección de la propiedad intelectual e industrial y, de manera especial, la protección de los menores de edad. En esta línea, resultan de especial relevancia las siguientes propuestas:

- **Desarrollo interno de espacios web dedicados a poner a disposición de los usuarios el máximo nivel de información posible** respecto al tratamiento de datos personales, los sistemas publicitarios empleados en la plataforma, las situaciones de riesgo a las que se pueden enfrentar derivadas del uso de este tipo de servicios online, así como de las implicaciones que pueden derivarse de la publicación de contenidos en la red social.

- Del mismo modo, es esencial **que las redes sociales y plataformas colaborativas pongan a disposición de los usuarios información relativa a las medidas de**

seguridad que la plataforma ha puesto a disposición de todos los usuarios para actuar en caso de que se produzca la vulneración de alguno de sus derechos.

En este sentido, se recomienda a las redes sociales y plataformas colaborativas que lleven a cabo las siguientes recomendaciones:

- Realización de **programas de formación** en los que se aborden de forma práctica aquellas situaciones conflictivas que, con mayor frecuencia, se dan durante el uso de este tipo de servicios. Se recomienda recurrir al uso de vídeos online y de material gráfico que permita a cualquier usuario la fácil comprensión de las principales ideas que se desea transmitir.

- Llegar a **acuerdos con las autoridades nacionales e internacionales competentes para el fomento de la formación y concienciación de los usuarios** respecto a la importancia de la seguridad en Internet.

Teniendo en cuenta que la mayoría de usuarios de redes sociales generalistas son menores de edad, resulta fundamental **que las redes sociales y** plataformas colaborativas, junto con las **autoridades públicas**, asociaciones y organizaciones cuya finalidad sea la protección de este tipo de colectivos, **lleven a cabo iniciativas conjuntas encaminadas a fomentar la formación entre los menores y tutores respecto a la seguridad de los usuarios**, investigando las posibilidades tecnológicas existentes para lograr la identificación de la edad de los usuarios del servicio.

Tal y como se ha indicado por parte de alguno de los proveedores, es recomendable la realización de programas de **voluntariado** dentro de la empresa para **colaborar con las instituciones escolares y centros de formación para difundir la importancia de la seguridad**, así como para informar sobre las principales recomendaciones a tener en cuenta en el uso de este tipo de servicios.

4.1.2 Propuesta de recomendaciones dirigidas a los fabricantes y proveedores de servicios de seguridad informática

El papel que juegan las empresas fabricantes y proveedoras de servicios de seguridad respecto a la protección de los usuarios es esencial, en la medida en que son éstas las encargadas de proporcionar herramientas tecnológicas capaces de evitar, y en su caso reducir, todas aquellas situaciones desfavorables que pudieran derivarse del uso de este tipo de plataformas, tales como: fraude online, *phishing*, *pharming*; suplantación de la identidad de usuarios; spam y difusión de contenidos inapropiados.

En este sentido, los fabricantes y proveedores de seguridad deben tener en cuenta dos aspectos clave para lograr el máximo nivel de seguridad:

- **Prevención del fraude online.** Se considera esencial adoptar una posición preactiva, respecto al desarrollo de aplicaciones capaces de garantizar la seguridad de los usuarios de la plataforma. Dicho esfuerzo no debe centrarse únicamente en las redes sociales, sino que deberá ser extendido al resto de agentes de la cadena de valor, para reducir al máximo posible el número de agujeros de seguridad.

- **Investigación y desarrollo en materia de seguridad tecnológica.** Se considera esencial que lleven a cabo una actividad de investigación de la seguridad online de manera constante, desarrollando a partir de la detección de nuevas situaciones de riesgo, nuevas herramientas capaces de previsualizarlas y, en su caso, controlarlas.

De esta forma, se hace esencial que todos los fabricantes de soluciones y servicios de seguridad fomenten en el sector los siguientes aspectos:

- **Que las aplicaciones** comercializadas entre las redes sociales y plataformas colaborativas, así como entre los usuarios, **hayan sido desarrolladas, revisadas y evaluadas conforme a criterios estándares de calidad, seguridad y privacidad que garanticen que su utilización es segura y respetuosa con los derechos de los usuarios**, así como que han sido sometidas previamente a un proceso de testeo que garantice el correcto funcionamiento de la aplicación.

- Las empresas de seguridad, en la medida de sus posibilidades, deben **fomentar la interoperabilidad de sus sistemas de seguridad**, promoviendo entre las redes sociales y plataformas colaborativas la implementación de sistemas y protocolos de seguridad estándares que garanticen el cumplimiento de códigos de conducta en los que se establecen mínimos exigibles.

- En este sentido, se recomienda **que colaboren directamente con las Fuerzas y Cuerpos de Seguridad del Estado en la investigación de nuevas situaciones de riesgo para los usuarios**, para lograr el desarrollo de aplicaciones capaces de detectar, actuar y contrarrestar cualquier tipo de situación desfavorable para los usuarios o la plataforma.

- Se recomienda a los fabricantes y proveedores de servicios de seguridad informática que sean proactivos en la **detección de códigos maliciosos** de programación que permitan agujeros de seguridad en las plataformas, así como la **elaboración de listados *("Black Listed"),* en los que sean incluidos todos los nombres de dominio** que cuenten con contenidos no autorizados, o en su caso, **que no superen los criterios de seguridad** previamente establecidos.

- Se recomienda **que los fabricantes desarrollen parches de seguridad y actualizaciones** que garanticen a los responsables de las diferentes plataformas, así

como a los propios usuarios, que los servicios prestados se sustentan sobre aplicaciones completamente actualizadas y seguras.

En este sentido, se recomienda a los fabricantes de soluciones de seguridad informática el desarrollo de aplicaciones que cumplan con los estándares internacionales promovidos por este tipo de iniciativas con reconocimiento mundial.

- Se recomienda el **desarrollo de aplicaciones remotas que permitan el control pleno por parte de los tutores de los contenidos y de las operaciones realizadas por los menores a través de Internet.**

  En esta línea, se recomienda el desarrollo de aplicaciones que permitan a los padres y tutores de los menores llevar a cabo las siguientes acciones: administrar y/o supervisar las listas de contactos de los menores en los servicios de mensajería instantánea, blogs, redes sociales y/o servicios de similar naturaleza; conocer los sitios web y contenidos que los menores visitan o que intentan visitar; delimitar el acceso a sitios web no adecuados para menores de edad; obtener informes respecto a toda la actividad que los menores llevan a cabo en la red y permitir diferentes grados de control y supervisión, dependiente de la edad de los menores[110].

  Mediante el uso de este tipo de aplicaciones y la promoción conjunta realizada por parte de los fabricantes y las plataformas, se puede obtener un resultado realmente efectivo en lo que respecta al control de la actividad de los menores en la red, así como a la protección de los mismos respecto a los peligros existentes en Internet.

- **Se recomienda a los fabricantes el desarrollo de aplicaciones que permitan a las plataformas controlar la edad de los usuarios que intentan acceder al servicio.**

  A pesar de que este tipo de herramientas actualmente se encuentran en estado embrionario, y dada la exigencia legal existente para que los proveedores cumplan con este tipo de requisito, es el momento clave para el desarrollo de herramientas tecnológicas capaces de garantizar la identificación de la edad de los usuarios.

- **Incluir en la descripción técnica de los productos de software destinados al tratamiento de datos personales,** la descripción técnica del **nivel de seguridad básico, medio o alto** que permitan alcanzar de acuerdo con el Reglamento de desarrollo de la LOPD.

[110] En este sentido, cabe destacar el sistema de control parental desarrollado por parte de Microsoft Inc, encaminado a que los padres y tutores cuenten con una herramienta que les permita conocer y autorizar o limitar el acceso a determinadas páginas web, así como a determinados contactos a través de redes sociales, sistemas de mensajería instantánea y cualesquiera otro servicio online. Para más información, visite el sitio web de *"Windows Live: Protección Familiar"*

- De igual forma, se recomienda **que los fabricantes de aplicaciones software de seguridad, junto con las administraciones públicas competentes, fomenten el desarrollo de herramientas encaminadas a reducir la recepción de correos electrónicos no deseados** (*spam*) a través de redes sociales y plataformas semejantes.

  En este sentido, es necesario tener en cuenta que las redes sociales se han convertido en grandes fuentes de información a través de las que generar bases de datos de potenciales receptores de comunicaciones comerciales electrónicas, gozando en este caso de un grado de viralidad máxima.

4.1.3 Propuestas y recomendaciones dirigidas a los prestadores de servicios de acceso a Internet (ISP)

A continuación se dispone una serie de recomendaciones destinadas a los Prestadores de Servicios de Internet, que se encargan del alojamiento de las redes sociales en sus servidores y proveen de conectividad a los mismos. En este sentido, y teniendo en cuenta que son parte fundamental de la cadena de valor, se recomienda:

- **La creación de plataformas de comunicación fehaciente y segura con las Fuerzas y Cuerpos de Seguridad del Estado, Ministerio Fiscal y Autoridades Judiciales.** En estos casos, se estructurarán mecanismos para que todo tipo de comunicaciones originadas por cualquiera de los sujetos intervinientes tenga la calificación de documento público y todos los efectos jurídicos de los documentos nacidos dentro de un procedimiento judicial, así se ahorrará más tiempo en la emisión y recepción que por medio de los sistemas tradicionales.

- **Apoyo y asistencia plena a las Fuerzas y Cuerpos de Seguridad del Estado** cuando realicen reclamaciones a las mismas dentro de sus labores de investigación de la posible comisión de un ilícito penal, posibilitando de esta forma la rápida incoación de un expediente que sea trasladable a la Autoridad Judicial o al Ministerio Fiscal.

- **Informar a todos los usuarios y clientes directos sobre las medidas de seguridad que mantienen respecto al servicio concreto.** En este sentido, resulta fundamental garantizar que éstas certifican la integridad de la base de datos, así como la seguridad de los servidores de DNS, que impidan o al menos reduzcan, las posibilidades de *phishing* y *pharming*.

- **Atender inmediatamente las reclamaciones de bloqueo de servicios cuando se reciban por cualquier método que deje constancia de la identidad del remitente y se identifique de forma clara y concisa el emisor del mismo**, teniendo en cuenta

el tipo de infracción. Poner en conocimiento inmediato de las Fuerzas y Cuerpos de seguridad.

4.2 Propuestas y recomendaciones dirigidas a las Administraciones e Instituciones Públicas

Las Administraciones e Instituciones Públicas, como garantes de los derechos de los ciudadanos y de millones de usuarios de Internet, cuentan con capacidad suficiente para impulsar las siguientes propuestas y recomendaciones respecto a los aspectos normativos, tecnológicos, de seguridad, así como de fomento de la concienciación y formación de los usuarios.

4.2.1 Desde el punto de vista normativo

Los especialistas consultados coinciden en resaltar que toda normativa que regule aspectos tecnológicos o íntimamente relacionados con la Sociedad de la Información debe partir de la **neutralidad tecnológica**, de tal forma que todos los aspectos regulados permitan cubrir diferentes situaciones particulares, con independencia de las características tecnológicas con las que cuente.

Del mismo modo, la **necesidad de equiparar los requisitos normativos del mundo digital con los del físico**, de tal forma que las condiciones para la prestación de servicios digitales no sean más gravosas que para su prestación en el mundo real.

No obstante, y a pesar de lo indicado, son pocos los consultados que manifiestan la necesidad de una reforma normativa completa, para adecuarla a las realidades derivadas de los servicios de la Sociedad de la Información, sino que prácticamente todos coinciden en señalar que lo que se requiere es de una mejor interpretación de la normativa con la que actualmente se cuenta.

Por todo ello, a continuación se proponen una serie de recomendaciones normativas:

Protección de Datos Personales, Intimidad, Honor y Propia Imagen

La situación normativa respecto a la protección de datos personales, intimidad, honor y propia imagen en España se encuentra actualmente en una situación muy avanzada con respecto a la existente en otros Estados del entorno. No obstante, se establecen las siguientes recomendaciones:

- Las autoridades competentes deben **promover la elaboración de informes, recomendaciones y dictámenes públicos**, en los que se analicen periódicamente los servicios de Internet más utilizados por los ciudadanos españoles, logrando así contar con un análisis actualizado del estado de la Sociedad de la Información y de los servicios de Internet.

Así, se propone que las diferentes administraciones públicas y autoridades competentes se posicionen respecto a las necesidades y deficiencias con las que cuentan este tipo de servicios, encargándose de proponer las recomendaciones pertinentes a los proveedores del servicio.

- **Que se fomente el establecimiento internacional, al menos a nivel comunitario, de los principios normativos básicos**, de obligado cumplimiento para cualquier operador, con independencia del lugar desde el que actúe, permitiendo así a las plataformas y usuarios contar con una **seguridad jurídica global**, que atienda la propia naturaleza del servicio ofrecido a través de Internet.

- Asimismo deberá garantizarse la ejecución efectiva de las sanciones para **aquellas plataformas o usuarios que compartan u obtengan información de forma ilegal.**

- Se recomienda a las autoridades trabajar en favor de **un derecho internacional homogéneo en materia de protección de datos personales, honor, intimidad y propia imagen**, que permita la correcta protección de los mismos en Internet.

Propiedad Intelectual

Tras la revisión de las condiciones de uso de las principales plataformas que operan en España, así como las consultas realizadas en propiedad intelectual y Sociedad de la Información, se ha detectado que todos los avisos legales establecen obligatoriamente la cesión de todos los derechos de propiedad intelectual a favor de la plataforma.

Por todo ello, se recomienda a las autoridades normativas que:

- **Fomenten, y en su caso dispongan como obligatorio, que este tipo de plataformas hagan públicas y destaquen con especial énfasis que dichos contenidos pasarán a ser propiedad de la plataforma**, con anterioridad a que cualquier usuario aloje cualquier contenido en la misma.

- Las redes sociales están convirtiéndose en los últimos tiempos en plataformas sobre las que los usuarios pueden publicar (*"embeber")* contenidos alojados en otras plataformas de difusión de contenidos digitales (vídeo, fotografías, etc.).

  Este hecho conlleva que, en cierta medida, las plataformas se puedan estar convirtiendo en comunicadores públicos o entidades que ponen a disposición contenidos digitales, por lo que **se recomienda que, dentro de los preceptos legales relativos a la propiedad intelectual, se amplíe su aplicación a este tipo de conductas.**

- **Se recomienda que las autoridades competentes promocionen,** desde el punto de vista normativo, **acuerdos directos entre la industria audiovisual y musical, y las grandes plataformas de difusión de contenidos**, determinando criterios objetivos, cuantificables y controlables, que permitan la comprobación y el abono económico de los derechos de explotación derivados de este tipo de actuaciones.

- **Se recomienda** que las autoridades legislativas articulen normativamente **la obligación de todo prestador de servicios de la Sociedad de la Información** a operar directamente en España, con independencia de si lo hace físicamente o no, **a que dispongan de medios automatizados, gratuitos, sencillos y eficaces para que los titulares de obras de propiedad intelectual puedan denunciar la retirada de contenidos** propios y que estuvieran siendo reproducidos sin autorización.

- La normativa de propiedad intelectual con la que se cuenta en la actualidad fundamenta sus principios básicos de protección de los derechos de propiedad intelectual de los autores en la prohibición del uso sin autorización por parte de terceros.

  Si se tiene en cuenta la práctica diaria, se puede observar cómo **el grado de eficacia de esta normativa dentro de la Sociedad de la Información es bajo**, dado que no se logra eficazmente el control de los contenidos digitales.

  Por ello, **se recomienda que la normativa de propiedad intelectual sea sometida** por parte del legislador y con la ayuda de los agentes del mercado -tanto los creadores, como los difusores de los contenidos- **a una profunda adaptación del modelo, basándose en la máxima permisividad respecto al acceso y reproducción de los contenidos.**

  No obstante, este cambio de paradigma no puede realizarse sin **que se garantice la justa remuneración de los titulares de los derechos**, de forma que éstos vean compensados todos los esfuerzos realizados para el desarrollo de sus obras.

Consumidores y Usuarios

- **Se recomienda al legislador que se delimite claramente qué autoridad es competente para atender las reclamaciones de los consumidores o usuarios** que se deriven del uso de este tipo de plataformas y, en general, del uso de Internet.

  El principal problema con el que se encuentran los usuarios a la hora de reclamar aspectos relativos a las transacciones comerciales que realizan a través de Internet, es que los costes de la reclamación, así como el tiempo que tardan en resolverse, son muy elevados. Esto, unido al hecho de que se trata de cantidades menores, desincentivan las reclamaciones por parte de los usuarios.

En ese sentido, es muy recomendable que las autoridades públicas, junto a las redes sociales y plataformas análogas, creen o fomenten la creación de algún órgano y código de conducta encargados de regular y poner a disposición de los usuarios un sistema gratuito, eficaz, válido en Derecho y rápido, que garantice a los consumidores que sus reclamaciones serán resueltas sin coste alguno.

- En relación con las redes sociales y plataformas análogas que operen para España, pero desde una localización diferente, se recomienda **disponer normativamente de mecanismos eficaces y eficientes,** tanto desde el punto de vista temporal, como económico, **respecto a la posibilidad de bloquear el acceso a la plataforma online**, en la medida en que los contenidos, procedimiento comercial y condiciones dispuestas por ésta contravengan claramente la normativa aplicable, provocando un daño real y efectivo a los usuarios.

- Se recomienda a las autoridades trabajar en favor de **un derecho internacional homogéneo en materia de consumidores y usuarios**, que permita a cualquier usuario o consumidor conocer cuáles son las condiciones mínimas exigibles a cualquier plataforma y que le permitan denunciar cualquier situación que contravenga estos derechos mínimos, con independencia del lugar en el que se encuentre el consumidor, la plataforma y/o donde se haya realizado la transacción.

  Se trata de crear reglas uniformes, que regulen el comercio electrónico a escala internacional y que permitan disponer de un cuerpo de conductas global y general, para lo que puede ser muy recomendable la adecuación del Derecho Internacional Privado a las nuevas realidades producidas en Internet, logrando así una mayor garantía a la hora de determinar la legislación y el órgano competente para la resolución del caso.

4.2.2 Desde el punto de vista ejecutivo y administrativo

A continuación, y partiendo de las recomendaciones y conclusiones obtenidas, se dispone una serie de recomendaciones destinadas a la Administración Pública con el objeto de orientar la ejecución de medidas de apoyo, fomento y actuación en materia de seguridad en los servicios de la Sociedad de la Información:

- **Formación específica en Derecho Tecnológico destinada a jueces, magistrados, forenses, fiscales y secretarios judiciales** y cualquier otro cuerpo de la Administración Pública que pudiera tener intervención en casos relacionados con los servicios de la Sociedad de la Información, permitiéndoles contar con conocimientos suficientes y previos respecto a cómo funcionan este tipo de servicios y cuáles son sus características y problemáticas principales, permitiéndoles de esta manera determinar de forma clara y ajustada cuáles son las implicaciones jurídicas que conllevan.

Por todo ello, es necesario que los Centros de Estudios Jurídicos y los programas de formación continua que se destinan a este tipo de colectivos comiencen a integrar formación específica sobre Derecho Tecnológico.

- Es esencial **dotar a las brigadas tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado**, tanto estatales y autonómicas, como internacionales, **de herramientas tecnológicas que les permitan investigar, mantener la cadena de custodia de las pruebas electrónicas y bloquear situaciones** que pudieran ser susceptibles de delitos y/o perjudiciales para los usuarios de redes sociales y plataformas colaborativas.

- **Desarrollo y articulación de procedimientos judiciales rápidos y gratuitos,** que permitan a los usuarios obtener una mejor respuesta a los casos en los que sus derechos se vean vulnerados a través de medios tecnológicos.

4.2.3 Desde el punto de vista formativo y divulgativo

Todos los aspectos relacionados con la Sociedad de la Información y la seguridad requieren un gran esfuerzo de concienciación y formación por parte de las entidades privadas implicadas, así como por parte de las Administraciones Públicas, dado que es con el trabajo conjunto como se obtendrán resultados adecuados a largo plazo.

Por ello, se formulan las siguientes recomendaciones de carácter formativo y divulgativo a las Administraciones e Instituciones Públicas:

- **Realizar campañas de concienciación sobre los riesgos de la difusión de datos personales en las redes sociales,** apoyadas por todos los sujetos intervinientes en la cadena de valor de las distintas redes.

- **Llevar a cabo jornadas de formación y programas de difusión** en los que se aborden, desde el punto de vista práctico, aspectos tecnológicos, jurídicos y sociológicos **relativos a la seguridad.**

- **Incluir en los planes oficiales de estudio el conocimiento de aspectos relacionados con la seguridad de las tecnologías de la información y la protección de datos personales** fomentando la formación específica en este campo.

- **Llevar a cabo acciones de sensibilización y fomento de la seguridad en Internet a través de los propios medios 2.0**, garantizando así un mayor grado de impacto y por tanto de efectividad de dichas campañas.

4.3 Propuestas y recomendaciones dirigidas a los usuarios y asociaciones

A continuación, se exponen varias recomendaciones destinadas a los usuarios de las redes sociales y las plataformas colaborativas, con la intención de que éstos conozcan plenamente todos y cada uno de los beneficios que pueden aportar este tipo de servicios, pero sin descuidar el conocimiento sobre la existencia de determinadas situaciones desfavorables, que sin embargo pueden ser fácilmente evitables. Por todo ello, las recomendaciones dirigidas a los usuarios y asociaciones se estructuran en la siguiente forma:

4.3.1 Protección de datos personales, honor, intimidad y propia imagen

- Todos los usuarios de servicios de redes sociales deben tener en cuenta que son ellos mismos quiénes tienen el control respecto a la información y datos personales que desean publicar, por lo que el nivel de responsabilidad respecto de la publicación excesiva de información y datos puede implicar riesgos para su intimidad.

  En este sentido, **se recomienda a los usuarios** disponer de **un perfil registrado en el que no se publique información excesiva respecto a su vida personal y familiar,** de forma que nadie que pueda tener acceso a su perfil a través de la red social obtenga información íntima.

  Por otro lado, el usuario debe conocer y considerar las implicaciones que, a nivel profesional, puede tener el hecho de *"dejar rastros"* indeseados en este tipo de plataformas, ya que cada vez más, las empresas utilizan este nuevo recurso para identificar posibles candidatos para participar en sus procesos de selección o profundizar en la información disponible en el perfil de los candidatos preseleccionados para un puesto de trabajo.

  No obstante, y dado que los usuarios son libres de hacer pública toda la información que deseen respecto a sus vidas privadas, se recomienda que dicha publicación se realice en todo caso de forma controlada y siempre que exista la posibilidad de retirar o bloquear el contenido.

- **Se recomienda a todos los usuarios recurrir al uso de seudónimos o nicks personales con los que operar a través de Internet**, permitiéndoles disponer de una auténtica "**identidad digital"**, que no ponga en entredicho la seguridad de su vida personal y profesional. De esta forma, únicamente será conocido por su círculo de contactos, que conocen el nick que emplea en Internet.

- **Se recomienda a los usuarios tener especial cuidado a la hora de publicar contenidos audiovisuales y gráficos en sus perfiles**, dado que en este caso pueden estar poniendo en riesgo la privacidad e intimidad de personas de su entorno.

Siempre que se vayan a alojar contenidos de este tipo o información relativa a terceros, se recomienda notificar previamente a ese tercero para que lo autorice o, en su caso, filtre los contenidos que desea publicar y los que no.

No obstante, todos los usuarios que detecten contenidos no autorizados o que pudieran ser dañinos para un tercero, deberán ponerlo en conocimiento del responsable de la red social, para que éste proceda a su retirada o bloqueo de forma inmediata.

- **Se recomienda revisar y leer,** tanto en el momento previo al registro de usuario, como posteriormente, **las condiciones generales de uso y la política de privacidad que la plataforma pone a su disposición en sus sitios web.**

- **Se recomienda configurar adecuadamente el grado de privacidad del perfil de usuario en la red social,** de tal forma que éste no sea completamente público, sino que únicamente tengan acceso a la información publicada en el perfil aquellas personas que hayan sido catalogadas como *"amigos"* o *"contactos directos"* previamente por el usuario.

- **Se recomienda aceptar como contacto únicamente a aquellas personas conocidas o con las que mantiene alguna relación previa**, no aceptando de forma compulsiva todas las solicitudes de contacto que recibe e investigando siempre que fuera posible y necesario, quién es la persona que solicita su contacto a través de la red social.

- **Se recomienda no publicar en el perfil de usuario información de contacto físico**, que permita a cualquier persona conocer dónde vive, dónde trabaja o estudia diariamente o los lugares de ocio que suele frecuentar.

  Es esencial que todos los usuarios tengan presente que la potencialidad de contacto y de difusión de la información publicada en Internet hace especialmente necesario tener profundo cuidado con la información personal, especialmente aquella que permite tener acceso a la vida física del usuario.

- **A los usuarios de herramientas de *microblogging*[111]** se recomienda tener especial cuidado respecto a la publicación de información relativa a los lugares en que se encuentra en todo momento. Este tipo de herramientas, utilizadas de forma compulsiva y sin limitar la información publicada, podría poner en peligro a los usuarios, dado que permite a los posibles infractores conocer en todo momento

[111] Este tipo de plataformas basan su servicio en la actualización constante de los perfiles de usuarios. Más información: Capítulo 3 de este Estudio.

donde se encuentra, qué está haciendo y hacia dónde se dirige el usuario, lo que puede suponer un grave riesgo para su integridad.

4.3.2 Propiedad intelectual

- En caso de vulneración de los derechos sobre obras y contenidos protegibles por propiedad Intelectual, **las propuestas de recomendaciones se dirigen a actuar atendiendo a los siguientes pasos:**

    - Contactar de forma inmediata con la red social, denunciando el uso no autorizado del contenido, acreditando la titularidad y solicitando expresamente la retirada del mismo. Para ello, se recomienda utilizar previamente los cauces internos de "denuncia" que las propias redes sociales ponen a disposición de los usuarios.

    - En caso de que no sean retirados, tal y como se solicita, se aconseja iniciar las acciones legales oportunas ante los juzgados o tribunales nacionales.

- Respecto al uso por parte de los usuarios de contenidos de terceros**, se recomienda utilizar y publicar únicamente contenidos respecto a los que se cuente con los derechos de propiedad intelectual suficientes**. En caso contrario, el usuario estará cometiendo un ilícito civil protegible por parte de los tribunales nacionales.

4.3.3 Tecnológicas y de seguridad

- **Se recomienda a los usuarios emplear diferentes nombres de usuario y contraseñas para entrar en las distintas redes sociales** de las que sea miembro. Esta medida procura aumentar el grado de seguridad del perfil de usuario, dado que los posibles atacantes no deberán romper la seguridad de un único sistema de acceso.

- **Se recomienda utilizar contraseñas con una extensión mínima de 8 caracteres, alfanuméricos y con uso de mayúsculas y minúsculas.** Este tipo de contraseñas certifica que el grado de seguridad del acceso es elevado, garantizando de esta forma una mayor integridad de la información publicada.

- **Se recomienda a todos los usuarios disponer en sus equipos de software antivirus instalado y debidamente actualizado,** que garantice que su equipo se encuentra libre de software maligno, así como de aplicaciones spyware que pongan en riesgo su navegación en Internet, y en peligro la información alojada en el equipo.

4.3.4 Protección de menores

Durante la realización de las entrevistas y los grupos de trabajo se ha hecho especial hincapié en determinar cuáles son las principales recomendaciones dirigidas a los

menores de edad usuarios de este tipo de servicios así como a sus tutores. A continuación se recogen las recomendaciones identificadas:

- **No se deben revelar datos personales excesivos.** Hay personas que quieren aprovecharse de los datos de los menores para acceder a un grupo de usuarios o simplemente para recolectar perfiles. **Nunca se deben suministrar los datos a desconocidos.** En caso de duda, lo más recomendable es preguntar a los padres o tutores.

- **Se debe leer toda la información concerniente a la página web.** En ella se explica quiénes son los titulares de la misma y la finalidad para la que se solicitan los datos.

- **Si el usuario es menor de catorce años, se necesita también el consentimiento de los padres o tutores.** En estos casos, siempre que se soliciten datos por parte de una red social debe preguntarse a los padres o tutores para ver si ellos aprueban la suscripción o no.

- **No deben comunicarse a terceros los nombres de usuario y contraseña, ni compartirlos entre amigos o compañeros de clase.** Estos datos son privados y no deben ser comunicados a terceros y/o desconocidos.

- **Siempre que se tenga cualquier duda respecto a alguna situación que se derive del uso de las redes sociales y herramientas colaborativas, debe preguntarse a los padres o tutores.** En caso de detectar una conducta no agradable por parte de otro usuario, lo mejor es comunicárselo a los padres o tutores y denunciar a ese usuario dentro de la propia plataforma, para que se tomen las medidas oportunas con respecto a éste a través de los medios internos con los que las propias plataformas cuentan.

  En caso de considerar tal conducta como delictiva, se debe comunicar también a las Fuerzas y Cuerpos de Seguridad del Estado, que cuentan con brigadas especializadas en este tipo de situaciones.

Respecto a las **recomendaciones especialmente dirigidas a los padres o tutores,** se establece que:

- **Se debe mantener el ordenador en una zona común de la casa**, sobre todo cuando los menores utilicen Internet. En su defecto, se recomienda utilizar herramientas de monitorización que permitan conocer las rutas de navegación de los menores y que éstos no puedan eliminar ni desbloquear dichos contenidos[112].

[112] Por ejemplo como la herramienta en versión beta de Microsoft, Windows Live Protección Infantil.

- **Se deben establecer reglas sobre el uso de Internet en casa.** En el momento en que los menores empiecen a utilizar Internet de forma independiente, se deben establecer reglas respecto al tipo de contenidos que pueden visitar, incluidas las redes sociales, así como las horas al día de utilización de las mismas.

- **Los padres deben conocer el funcionamiento y las posibilidades de este tipo de plataformas, tanto positivas como negativas.** Así, se podrán conocer las posibles implicaciones jurídicas y tecnológicas que pueden derivarse de su uso, y de otro lado, educar en su utilización de una forma más experta.

- **Activar el control parental y las herramientas de control de la plataforma, así como establecer el correo del padre o tutor como correo de contacto secundario.** Además, de esta manera, cualquier anuncio o petición proveniente de la plataforma llegará a la dirección del correo electrónico del padre o tutor, pudiendo éste conocer las actividades que realiza su hijo. Con este sistema, para la incorporación a ciertos grupos será necesaria la autorización de los padres o tutores.

- **Asegurarse de que los controles de verificación de la edad están implementados.** Asegurarse de que las páginas a las que acceden los menores disponen de sistemas de reconocimiento de edad, así como de información previa respecto al tipo de contenidos mostrados en el sitio web.

- **Asegurar la correcta instalación del bloqueador de contenidos.** El uso de este tipo de herramientas puede prevenir del acceso a contenidos no recomendables para menores, tanto desde el ordenador, como desde dispositivos móviles. Con esta herramienta, todo contenido para mayores de edad o sin clasificación de edad será bloqueado.

- **Concienciar e informar a los menores sobre aspectos relativos a la seguridad.** La educación es crucial. Hay que explicar a los menores los principios básicos para llevar a cabo una navegación segura en el entorno de estas plataformas.

- **Explicar a los menores que nunca han de quedar con personas que hayan conocido en el mundo online y que si lo hacen debe ser siempre en compañía de sus padres o tutores.** Se debe evitar que los menores acudan a citas presenciales con personas que no conocen personalmente y respecto a las que sólo cuentan con un contacto online, los padres o tutores deberán acompañarlos.

- **Asegurarse de que los menores conocen los riesgos e implicaciones de alojar contenidos como vídeos y fotografías, así como el uso de cámaras web a través de las redes sociales.** Es necesario explicar a los menores que el uso de fotografías

y vídeos puede suponer un riesgo. Por ello es necesario enseñarles cómo y cuándo utilizar este tipo de herramientas.

- **Controlar el perfil de usuario del menor.** Es recomendable revisar el tipo de información que el menor está utilizando y qué tipo de datos pone a disposición del público y del resto de usuarios de la red social. Además se recomienda realizar una revisión de las condiciones aplicadas respecto de su privacidad.

- **Asegurarse de que el menor sólo accede a las páginas recomendadas para su edad.** Así se asegurará que el resto de usuarios de la red tienen una edad semejante a la del menor, manejándose en un entorno en el que se sentirá cómodo y en el que los riesgos son menores. En caso de no conseguir encontrar la edad recomendada, la mejor solución es preguntar a la propia red social o, en su caso, bloquear el contenido.

- **Asegurarse de que los menores no utilizan su nombre completo.** De esta forma serán más difícilmente identificables por terceros malintencionados. Además, se debe potenciar el uso de pseudónimos dentro de las propias plataformas.

5 CONCLUSIONES

Actualmente, Internet se configura como un escenario de relaciones sociales sustentado en la creciente participación de los usuarios. Las redes sociales y sitios web colaborativos suponen uno de los principales medios de contacto utilizados por los usuarios de Internet, para fomentar la interacción con el resto de miembros de la red y promover la generación de nuevas relaciones y el acceso a contenidos comunes.

El método de crecimiento empleado por este tipo de plataformas basado principalmente en el "*boca a boca" (o marketing viral),* ha permitido que en poco tiempo estas redes cuenten a nivel mundial con más de 350 millones de usuarios[113].

La cifra de usuarios de redes sociales aumenta a media que se desarrolla la banda ancha. Así, en España, un 22,6% de los usuarios de Internet utilizan estas redes para relacionarse con amigos y familiares cercanos o para buscar conocidos con los que se ha perdido el contacto.

Pero el crecimiento y notoriedad de estos espacios sociales no queda exento de posibles riesgos o ataques malintencionados. Esto es debido, en parte, a que el uso de estas redes se basa en la publicación de información personal de los usuarios, hecho que puede generar situaciones que amenacen y vulneren derechos fundamentales no sólo del propio usuario, sino incluso de terceros.

Así, por ejemplo, la libre difusión de información de un usuario puede vulnerar, entre otros, los derechos de protección del honor, la intimidad, la propia imagen y los datos de carácter personal. Hay que tener en cuenta, no obstante, que en muchas ocasiones esta difusión se debe a una falta de formación y conocimiento del usuario, que realiza una mala configuración de la privacidad de su perfil.

El riesgo de vulneración aumenta cuando la información que se publica no es la de uno mismo sino la de terceros y alcanza su máximo cuando el usuario de la red social es un menor, ya que a los anteriores riesgos hay que añadir el del acceso a contenidos inapropiados y el del posible contacto con adultos malintencionados.

Las redes sociales no están estrictamente sujetas a una ubicación geográfica concreta para poder prestar sus servicios.

No obstante, debe tenerse en cuenta la existencia en España de regulación específica encargada de tratar los aspectos relacionados con los prestadores de servicios de la Sociedad de la Información[114].

[113] Datos según el Informe anual "e2008 sobre el desarrollo de la Sociedad de la Información en España", de la Fundación Orange. Disponible en www.fundacionorange.es

Por un lado, la aplicación de la Directiva 95/46/CE, teniendo en cuenta que estas actividades entran en el ámbito de aplicación de la normativa, y por otro, la Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico dispone en su artículo 5, los aspectos concretos que aplican a los *"Prestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo,"* al señalar que aquellos *"…**que dirijan sus servicios específicamente al territorio español quedarán sujetos**, ade*más**, a las obligaciones previstas en esta Ley**, siempre que ello no contravenga lo establecido en tratados o convenios internacionales que sean aplicables".*

En cualquier caso, es importante señalar que las compañías propietarias de redes sociales deben mejorar:

Desde el punto de vista jurídico:

Las redes analizadas disponen de información legal en la que existen algunas carencias entre las que destacan:

- Las condiciones de uso son alojadas habitualmente en lugares del sitio web de difícil acceso para el usuario.
- Son confusas y con redacciones frecuentemente extensas.
- Resultan de difícil comprensión para cualquier usuario medio que no disponga de conocimientos jurídicos y tecnológicos.
- Insuficiente respecto a los medios de seguridad tecnológicos existentes en la plataforma.

Desde el punto de vista tecnológico

Las plataformas entrevistadas han indicado haber implantado diferentes medidas de seguridad en colaboración con los Proveedores de Servicios de Internet (ISP), con la finalidad de reducir las posibilidades de que sus plataformas, y por tanto sus usuarios sufran casos de *phishing* o *pharming*, así como para que se reduzcan las posibilidades de suplantación de identidad.

Además, hay que destacar como la herramienta más extendida entre las redes sociales analizadas para garantizar la seguridad de los usuarios y de los contenidos que éstos alojan, está en los sistemas de denuncias internas. Todas las redes sociales

[114] Según la definición dispuesta en la Disposición Adicional Primera de la Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico, se trata de toda *"persona física o jurídica que proporciona un servicio de la sociedad de la información".*

entrevistadas coinciden en que la colaboración de los propios usuarios es esencial para lograr que la red sea un lugar seguro y con garantías suficientes.

Sin embargo, a pesar de las medidas actualmente implementadas, las redes aun deben avanzar en el uso de otras como:

- Formación a los usuarios sobre los diferentes aspectos de configuración del perfil y las ventajas de una adecuada restricción en la difusión de datos personales.
- Cambios en la configuración por defecto del nivel de privacidad (generalmente está configurado permitiendo la máxima difusión de los perfiles).
- Control de la indexación y almacenamiento de los perfiles por parte de los buscadores.
- Las redes no han implementado sistemas para *identificar la edad de los usuarios*, a pesar de que en la actualidad existen diferentes proyectos[115] con este objetivo.
- Establecer *sistemas de identificación remota de usuarios mediante sistemas de firma electrónica reconocida.* Sistemas como el *DNI electrónico* permitirían asegurar las transacciones electrónicas y supondría que todas las comunicaciones realizadas de forma online contasen con la garantía de integridad plena, detectándose cualquier tipo de variación que hubiera podido sufrir durante su envío.

[115] Cabe destacar la iniciativa propuesta por la Asociación para la protección de los menores Protégeles en su proyecto micueva.com, donde se contacta individualmente con cada usuario que solicita el registro para comprobar su edad.

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

ANEXO I

I Relación de participantes

Para la realización de este estudio se ha contado con la participación de representantes de las propias empresas prestadoras de los servicios de redes sociales, o bien de su asesoramiento jurídico, así como profesionales pertenecientes a entidades y autoridades dedicadas a la protección y salvaguarda de los derechos de los usuarios o relacionados con el derecho tecnológico. Todos ellos han aportado su conocimiento y experiencia en el ámbito de la seguridad de la información, la privacidad en Internet y la protección de datos personales.

Desde INTECO y la AEPD, queremos señalar y agradecernos el alto nivel de colaboración para la elaboración de este estudio por parte de los entes y profesionales que han participado en las entrevistas y en los grupos de trabajo organizados:

- Abraham Pasamar. Experto en Seguridad Informática y Perito Tecnológico de **Incide, Investigación Digital.**
- Alexandra Juanas Castañeda. Abogado de **Castañeda & Castañeda Abogados** (asesores jurídicos de la red social **Wamba**).
- Alonso Hurtado. Abogado de **X-NOVO Legal & Web Solutions, S.L.**
- Álvaro Cuesta. Director de **X-NOVO Legal & Web Solutions, S.L.**
- Blanca E. Sánchez Rabanal. Técnico del **Observatorio de la Seguridad de la Información de INTECO.**
- Bárbara Navarro. Responsable de Relaciones Institucionales de **Google España** (proveedor de las plataformas **OpenSocial, Orkut** y **YouTube**).
- Bárbara Olagaray. Responsable jurídico para Centro y Sur de Europa, **Microsoft España** (contacto en España de las redes sociales **MSN Live Spaces** y **Facebook**).
- Cesar Iglesias. Consultor Seguridad y Abogado LOPD de **Díaz-Bastien y Truan.**
- David Puello. Director General y Fundador de la red social **Votamicuerpo.com.**
- Enrique Dans. Profesor de Tecnologías de Información del **Instituto de Empresa.**
- Fernando Fernández. Inspector de la **Brigada de Investigación Tecnológica de la Policía Nacional.**

- Fernando Ujaldón. Responsable de Comunicación de la red social **11870.com.**
- Francesc Pla. Responsable de Seguridad de **Vesne, S.L.** (empresa dedicada al desarrollo de redes sociales, como **Moterus**).
- Iban Díez López. Abogado de **Gómez Acebo & Pombo**, (asesores jurídicos de la red social **Tuenti**).
- Ícaro Moyano. Responsable de Comunicación de la red social **Tuenti**.
- Iván García Crespo. Técnico del **Observatorio de la Seguridad de la Información de INTECO.**
- Ignacio Parada. Responsable de Seguridad de la Información de la red social **Vi.vu.**
- Jaime Esteban. Product Manager de **Microsoft España** (contacto en España de las redes sociales **MSN Live Spaces** y **Facebook**).
- Javier Cremades. Presidente de **Cremades & Calvo Sotelo.**
- Javier García. Asesor del Gabinete Técnico del **Defensor del Menor de la Comunidad de Madrid.**
- Joaquín Muñoz. Socio de **Abanlex Abogados.**
- Juan José Marín López. Socio y Catedrático de Derecho Civil de **Gómez Acebo & Pombo** (asesores jurídicos de **Tuenti**).
- Juan José Portal Svensson. Manager Seguridad de la Información de **Forbes Sinclair, S.L.** (consultora internacional en seguridad de la información y formadores del **British Standard Institute**).
- Juan Luis Alonso. Responsable de Seguridad y Contenidos de **Advernet, S.L** (proveedores de **Dalealplay.com** y que pertenece al **Grupo Vocento**).
- Juan Salom. Comandante de la **Brigada de Delitos Telemáticos de la Unidad Central Operativa de la Guardia Civil.**
- Luis Albaladejo Ufarte. Consultor Seguridad de la Información de **Forbes Sinclair, S.L.**
- Luís Cisneros. Abogado de **X-NOVO Legal & Web Solutions, S.L.**

- Luis Miguel García. Director de Estrategia de Plataforma y Responsable de Seguridad dentro del Departamento de Marketing de Windows Live, **Microsoft España** (como contacto de **MSN** y **Facebook**).
- Manuel Vázquez. Comisario Jefe de la **Brigada de Investigación Tecnológica de la Policía Nacional.**
- María González Torres. Abogada de **Gómez Acebo & Pombo** (asesores Jurídicos de **Tuenti**).
- María González. Abogado de **Google España** (proveedor de las plataformas **OpenSocial, Orkut** y **YouTube**).
- Michael Hall. Socio Fundador y auditor de seguridad de la información, CISSP, **Forbes Sinclair, S.L.**
- Miguel Ángel Díez Ferreira. Consejero Delegado de la red social **Redkaraoke.com.**
- Miguel Pérez Subías. Presidente de la **Asociación de Usuarios de Internet.**
- Mikel Lertzog. Director General de **Hi-Media España** (responsables de la red social **Fotolog España**).
- Oriol Solé. Fundador de la red social **Patatabrava.com.**
- Pablo Fernández. Socio de **Abanlex Abogados.**
- Pablo Pérez San-José. Gerente del **Observatorio de la Seguridad de la Información de INTECO** (*coordinador y director de proyecto del estudio*).
- Pedro Escribano Testaut. Magistrado del **Gabinete Técnico de la Sala III del Tribunal Supremo.**
- Pedro Jareño. Responsable de Marketing y Comunicación de la red social **Minube.com.**
- Sergio Hernando. Consultor y Auditor Seguridad de la Información e Criptografía del **Departamento de Seguridad BBVA**.
- Sylvia Alonso Salterain. Socio de **Cremades & Calvo Sotelo.**
- Tomás Serna. Abogado Especializado en Protección de Datos y Seguridad de la Información de **TFSerna Abogados**.

II Relación de redes sociales analizadas

A continuación se recoge una relación de las redes sociales y webs colaborativas analizadas para la elaboración del Estudio.

Nombre	Objetivo	Nº de usuarios	Tipo de registro
11870.com	Compartir y recomendar sitios de interés	12.269	Mayores de 14 años
43 things	Plataforma para exponer y planificar ideas y obtener colaboradores.	1.007.433	Abierto
Advogato	Compartir conocimientos informáticos	11.000	Abierto
ASmallWorld	Público adinerado	150.000	Sólo con invitación
Badoo	General	12.500.000	Mayores de 18 años
Bebo	General	40.000.000	Abierto
BlackPlanet	Público Afroamericanos	16.000.000	Abierto
Broadcaaster.com	Compartir contenidos	26.000.000	Abierto
Buzznet	Cultura y música pop	550.000	Abierto
Capazoo	General	No disponible	Abierto
CarDomain	Compartir conocimientos sobre coches	1.600.000	Abierto
Care2	Promover la ecología y movimientos sociales	8.123.058	Abierto
Classmates.com	General	40.000.000	Abierto
Cyworld	Público Afroamericanos	21.200.000	Abierto
Dalealplay.com	Compartir contenidos multimedia	No disponible	Abierto
Dandelife	General	No disponible	Abierto
Del.icio.us	Compartir enlaces en Internet	No disponible	Abierto
DontStayIn	Promover la cultura de club	330.000	Abierto
Experience Project	General	No disponible	Abierto
Facebook	General	150.000.000	Mayores de 13 años
Faceparty	General	5.900.000	Mayores de 16 años
Flickr	Compartir fotografías	4.000.000	Abierto
Flixster	Compartir vídeos	36.000.000	Abierto
Fotki	Compartir fotografías	1.000.000	Abierto
Fotolog	Blog de fotos	12.695.007	Abierto
Friendster	General	75.000.000	Abierto
Frientes Reunited	General	19.000.000	Abierto
Gaia Online	Promover la comunidad anime	9.300.000	Abierto
Gather	Compartir contenidos multimedia	450.000	Abierto
Geni.com	Conocer las familias y genealogía	750.000	Abierto
Grono.net	Promover los contactos entre polacos.	1.350.000	Sólo con invitación
GuildCafe	Comunidad de Jugadores Online	No disponible	Abierto
Hi5	General	50.000.000	Abierto
Hospitality Club	Compartir alojamientos	328.629	Abierto
Hyves	Promover los contactos entre holandeses	5.000.000	Abierto
Imeen	Compartir contenidos multimedia	16.000.000	Abierto

IRC-Galleria	Promover los contactos entre Finlandeses	400.000	Abierto
iWiW	Promover los contactos entre hungaros	3.100.000	Sólo con invitación
Jaiku	General	No disponible	Abierto
Joga Bonito	Compartir conocimientos sobre Fútbol	No disponible	Abierto
Last.fm	Compartir conocimientos sobre Música	15.000.000	Abierto
LibraryThing	Compartir conocimientos sobre Libros	214.425	Abierto
LinkedIn	Compartir conocimientos sobre Empresas	16.000.000	Abierto
LiveJournal	Compartir conocimientos Blogs	12.900.000	Abierto
LunarStorm	Promover los contactos entre Suecos	1.200.000	Abierto
Meeting	General	72.000	Abierto
Meetup.com	General	2.000.000	Abierto
MiGente.com	Promover los contactos entre el público latino	36.000.000??	Abierto
MindViz	General	145.000	Abierto
Minube.com	Compartir experiencias sobre viajes	51.353	Abierto
Mixi	Promover los contactos entre Japoneses	9.830.000	Sólo con invitación
MOG	Compartir música	No disponible	Abierto
Moterus.com	Compartir conocimientos sobre motos	4.803	Abierto
MSN - Windows Live Spaces	Agregador de Blogs	120.000.000	Abierto
Multiply	General	7.000.000	Abierto
My Opera Community	General	1.001.798	Abierto
MyChurch	Promover el contacto entre cristianos	70.306	Abierto
MySpace	General	110.000.000	Abierto
myYearbook	General	950.000	Abierto
Netlog	General	28.000.000	Abierto
Nexopia	Promover los contactos entre canadienses	1.158.531	Abierto
Okcupid	Búsqueda de contactos personales	800.000	Abierto
Orkut	General	67.000.000	Abierto
OUTeverywhere	Comunidad social Gay	No disponible	Abierto
Passado	General	4.700.000	Abierto
Passportstamp	Compartir experiencias sobre viajes	12.000	Abierto
Patatabrava.com	General	40.000	Abierto
Piczo	General	10.000.000	Abierto
Plaxo	Obtener contactos profesionales	15.000.000	Abierto
Playahead	General	530.000	Abierto
Playtxt	Red social con geolocalización de usuarios	70.000	Abierto
Pownce	Compartir contenidos multimedia	No disponible	Abierto
ProfileHeaven	General	100.000	Abierto

RatetAll	Valoración de productos y servicios	No disponible	Abierto
Redkaraoke.com	Red social de Karaoke online	100.000	Mayores de 18 años
Reunión.com	General	28.000.000	Abierto
Ryze	Compartir conocimientos sobre Empresas	250.000	Abierto
Sconex	Red social de colegios americanos	500.000	Abierto
Searchles	General	No disponible	Abierto
Sermo	Promover el contacto entre Físicos y científicos	40.000	Licenciados y doctores
Shelfari	Compartir experiencia sobre libros	Dato no disponible	Abierto
Skyrock Blog	Agregador de Blogs.	3.800.000	Abierto
Soundpedia	Compartir información sobre música	3.500.000	Abierto
Sportsvite	Fomentar los deportes recreativos	18.000	Abierto
Squidoo	General	No disponible	Abierto
StudiVZ	General	4.000.000	Abierto
Tagged.com	General	30.000.000	Abierto
TakingITGlobal	Promover la acción social	145.000	Abierto
The Student Center	General	800.000	Abierto
Threadless	Compartir diseños para camisetas	364.474	Abierto
TravBuddy.com	Compartir experiencias sobre viajes	760.000	Abierto
Travellerspoint	Compartir experiencias sobre viajes	105.000	Abierto
Tribe.net	General	602.876	Abierto
Tuenti	General	2.400.000	Mayores de 14 años
Twitter	General (microblogging)	No disponible	Abierto
Vi.vu	Realizar consultas médicas y compartir experiéncias	3.000	Abierto
Votamicuerpo.com	Contactos	300.000	Abierto
Vox	Blogs	No disponible	Abierto
Wamba	General	2.511.729	Mayores de 14 años
Wayn	Compartir experiencias sobre viajes	8.000.000	Mayores de 18 años
WebBiographies	Promocionar la genealogía	No disponible	Abierto
Woophy	Compartir experiencias sobre viajes	23.000	Abierto
Xanga	Agregador de Blogs	40.000.000	Abierto
XING	Compartir conocimientos sobre Empresas	4.000.000	Abierto
Yahoo! 360º	General	4.700.000	Mayores de 18 años
Youtube	Compartir contenidos multimedia	115.00.000	Mayores de 18 años

http://www.inteco.es

http://www.agpd.es

http://observatorio.inteco.es