© **Dereito** Vol.27, nº1:99-117 (Xaneiro-Xuño, 2018) • ISSN 1132-9947

LOS DATOS PERSONALES DE LA VÍCTIMA DE CIBERACOSO EN FACEBOOK

The personal data of the victims of ciberacoso in Facebook

DOI: http://dx.doi.org/10.15304/dereito.27.1.4229.5574

MELANIA PALOP BELLOCH
Doctora en Derecho
Universidad Jaume I de Castellón
melaniapalop@hotmail.com

Resumen
El objetivo de este artículo es evitar la vulneración de los derechos fundamentales como el honor, la intimidad, la propia imagen y la protección de los datos personales a través de la acción viral de los cibernautas en Facebook. A lo largo de este estudio se han detectado herramientas tecnológicas para paliar esta situación y proteger sus datos personales. Sin embargo, Facebook solo da recomendaciones y se escuda en la normativa vigente, alegando no tener un conocimiento efectivo. Entonces, es cuando la red social se dispone a bloquear la IP del acosador, ocultar la información nociva de la menor… mediante la orden judicial. Pero, esto ocurre con posterioridad y cuando la información nociva publicada sobre ella ha sido vista y compartida por multitud de usuarios dentro y fuera de nuestras fronteras. Por eso, se solicita una acción preventiva y no la que rige en este momento.
Palabras clave: Facebook, datos personales, big data, menores, herramientas tecnológicas.

Abstract
The objective of this article is to avoid the violation of fundamental rights such as honor, privacy, self-image and the protection of personal data through the viral action of cybernauts on Facebook. Throughout this study, technological tools have been detected to alleviate this situation and protect your personal data. However, Facebook only gives recommendations and shields itself from current regulations, claiming that it does not have an effective knowledge. Then, it is when the social network prepares to: block the IP of the harasser, hide the harmful information of the minor ... by means of the judicial order. But, this happens later and when the harmful information published about it has been seen and shared by many users inside and outside our borders. Therefore, a preventive action is requested and not the one that governs at this time.
Keywords: Facebook, personal data, big data, minor, technological tools.

SUMARIO

Recibido: 18/09/2017. Aceptado: 14/02/2018.

SUMMARY

1. LA PROTECCIÓN DE DATOS PERSONALES

La protección de datos personales se regula a través de la Ley orgánica de protección de datos 15/1999, de 13 de diciembre[1], en trámite de modificación por la nueva LOPD acorde con el futuro Reglamento 2016/679 (UE) que entrará en vigor el 18 de mayo del 2018. Además, destacar la Ley orgánica Ley 25/2007, de 18 de octubre, de conservación de datos relativa a las comunicaciones electrónicas y a las redes públicas de comunicaciones y la Ley de servicios de sociedad de la información en España.

Es necesaria esta reforma porque el problema entre los Estados de la Unión Europea radica en, por ejemplo, EEUU tiene un derecho más amplio respecto a España sobre la libertad de expresión. En EEUU determinadas conductas no serán consideradas ilícitas ni constitutivas de intromisión a la intimidad, honor o imagen de una persona. Lo contrario ocurre en España. De ahí, la dificultad de solicitar responsabilidades a prestadores de servicios o internautas residentes en este país como *Facebook*.

Por eso, la tutela de todos estos derechos en el medio virtual hace necesario un tratamiento unificador y globalizador de todos los sistemas jurídicos de todos lo países. La solución podría ser la aplicación del futuro Reglamento (UE) sobre protección de datos personales de obligado cumplimiento para todos los países miembros y no miembros de la Unión Europea.

En España, la jurisprudencia del Tribunal Constitucional en la sentencia 11/1981, de 8 de abril, en su fundamento jurídico 8ª concreta más y dice: "*El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona. Esta potestad incluye poder decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, así como permitir al individuo saber quién*

[1] En lo sucesivo LOPD

posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso"[2].

En la misma línea define la Agencia Española de Protección de Datos la protección de datos personales. Su protección constitucional reflejada en la sentencia 292/2000[3]: "*ofrece a su titular la facultad de imponer a otros la limitación del uso de la informática, (…) para impedir el tráfico ilícito y lesivo"*[4]. Sin embargo, si el afectado desconoce "*qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin"*[5]; de nada sirve la facultad otorgada constitucionalmente.

Por otra parte, el Tribunal Constitucional permite el ejercicio de este derecho: *"accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele"*[6].

La jurisprudencia del Tribunal Constitucional en la sentencia 29/2013, de 11 de febrero, fundamento jurídico 10ª, da un paso más y dice: *"Estos poderes (…) se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento (…)*[7].

Pero, la víctima de delitos informáticos no podrán ejercer este derecho de tutela sino cumple con los requisitos establecidos en el artículo 3 apartado a) de la LOPD: *"cualquier información concerniente a personas físicas identificadas e identificables"*[8].

Así lo dispone, la jurisprudencia del Tribunal Constitucional en la sentencia 292/2000, de 30 de noviembre: "*Los datos amparados son todos aquellos que identifiquen o permitan la identificación de una persona, es decir, que se puedan poner en relación con el individuo concreto, ya sea de forma directa o indirecta: pues cualquiera de estos datos puede servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier índole, o (…) para cualquier otra utilidad*

---

[2] M. HERNÁNDEZ RAMOS, "El derecho al olvido digital en la *web 2.0*", en *Cuaderno de la cátedra de seguridad salmantina*, núm. 11, 2013, pp. 20-21. Sentencia del Tribunal Constitucional, sala pleno, núm. de resolución 11/1981, 8 de abril de 1981. Sentencia del Tribunal de Justicia de la Unión Europea, gran sala, núm. de resolución 2014/85, 13 de mayo de 2014.

[3] S. Mª. SUÁREZ RUBIO, "Los menores como usuarios de redes sociales y su privacidad", en *Parlamento y Constitución*, núm. 16, 2014, p. 130. Sentencia del Tribunal Constitucional, sala pleno, núm. de resolución 292/2000, 30 de noviembre del 2000. A. RALLO LOMBARTE, *El derecho al olvido en Internet: Google versus España***,** Centro de estudios políticos y constitucionales, Madrid, 2014, p. 167.

[4] M. HERNÁNDEZ RAMOS, "El derecho al olvido digital en la web 2.0", op. cit., pp. 20-21. Sentencia del Tribunal Constitucional, sala pleno, núm. de resolución 11/1981, 8 de abril de 1981.

[5] Sentencia del Tribunal Constitucional, sala 2ª, núm. de resolución 144/1999, 22 de julio de 1999.

[6] Sentencia del Tribunal Constitucional, sala pleno, núm. de resolución 292/2000, 30 de noviembre de 2000.

[7] Sentencia del Tribunal Constitucional, sala 1ª, núm. de resolución 29/2013, 11 de febrero de 2013.

[8] Sentencia de la Audiencia Nacional, sala de lo contencioso-administrativo, sección 1ª, núm. de recurso 2/2010, 29 de septiembre del 2011.

que en determinadas circunstancias constituya una amenaza para el individuo"[9].

A tenor de lo anterior, el Tribunal Constitucional[10], y el Reglamento 2016/679 (UE)[11] definen dato personal: "*se trata de información relativa a persona identificada o identificable, careciendo de relevancia su naturaleza pública o privada*".

Esta definición es complementada por el art. 5 apartado o) y la sentencia de la Audiencia Nacional, 15 de enero, de 2011[12], referente al concepto de persona identificable: "*Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados".*

De todo lo expuesto se considera como "dato personal" al nombre y al usuario de la víctima para identificarse en la red social (*Facebook*). A su vez, también será "dato personal" el nombre y el usuario ficticio fácilmente identificativo en la víctima sin artificios técnicos desproporcionados.

De este modo, la publicación y difusión de comentarios o imágenes humillantes de la víctima en la red "supone, entre otros derechos vulnerados, un daño al honor, a la intimidad, a la propia imagen y al derecho a la protección de sus datos personales", afectando al libre desarrollo de la personalidad[13].

El derecho a la intimidad está regulado en el artículo 18.1 de la Constitución Española: "*se garantiza el derecho a la intimidad personal y familiar*". Este derecho contempla formas específicas de protección: la inviolabilidad del domicilio, el secreto de las comunicaciones y, el derecho a la intimidad personal y familiar.

ÁLVAREZ CARO dice: "El núcleo duro de este derecho comprende un "ámbito propio y reservado frente a la acción y conocimiento de los demás y necesario para mantener una calidad mínima de la vida humana"[14].

El Tribunal Supremo ha establecido la distinción entre intimidad y vida privada:"*la esfera privada(…)incluye aquel sector de circunstancias que, sin ser secretas ni de carácter íntimo, merecen sin embargo el respeto de*

---

[9] A. GARRIGA DOMÍNGUEZ, *Nuevos retos para la protección de datos personales. En la era del big data y de la computación ubicua*, op. cit., p. 95.

[10] Sentencia del Tribunal Constitucional, sala pleno, núm. de resolución 292/2000, 30 de noviembre del 2000. Sentencia del Tribunal Constitucional, sala pleno, núm. de resolución 290/2000, 30 de noviembre del 2000.

[11] J. M. MORCILLO MARTÍNEZ, "Seguridad y prevención en redes sociales. Responsabilidades legales en Internet", *Ciberacoso y violencia de género en redes sociales: Análisis y herramientas de prevención,* Universidad internacional de Andalucía Servicio de publicaciones, 2015, p. 85.

[12] Sentencia de la Audiencia Nacional, sala de lo contencioso-administrativo, sección 1ª, núm. de recurso 297/2010, 15 de enero del 2011.

[13] P. SIMÓN CASTELLANO, *El reconocimiento del derecho al olvido digital en España y en la UE: efectos tras la sentencia del TJUE de mayo de 2014*, Bosch, Barcelona, 2015, p. 184.

[14] M. ÁLVAREZ CARO, *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*, Reus, Madrid, 2015, p. 43.

todos, por ser necesarias para garantizar el normal desenvolvimiento y la tranquilidad de los titulares particulares (…)"[15]*.*

El derecho al honor está regulado en el artículo 18.1 de la Constitución Española. Este derecho se define: "La estima de cada persona en sí misma como la buena fama o estima que uno disfruta en el ambiente social"[16]. De esta definición se extrae "*la relación íntima entre el derecho al honor y el derecho a la dignidad"*[17]. Por lo tanto, el derecho al honor engloba a la dignidad y a la reputación personal en la sociedad y también en la esfera digital.

El derecho a la propia imagen está regulado en el artículo 18.1 de la Constitución Española. Este derecho configura: "*la representación gráfica de la figura mediante un procedimiento mecánico o técnico de reproducción"*[18]*.*

A su vez la Ley 1/1982 concede una doble vertiente a este derecho: *"distingue entre el contenido personalísimo del derecho a la propia imagen regulado en su art. 7.5: (captación, reproducción o publicación de la imagen de una persona o cualquier otro procedimiento) en lugares y momentos de su vida privada y fuera de ellos*[19] *y el contenido patrimonial del derecho a la propia imagen: utilización del nombre, la voz o imagen de una persona para fines comerciales".*

A su vez, FLORES FERNÁNDEZ dice: "la memoria eterna de la red o de las bases de datos de los servidores, incluyendo a los buscadores supone la acumulación de datos no pertinentes, muy antiguos, caducos e incluso inciertos, realizando una intromisión a nuestra privacidad, honor e imagen"[20]*.*

La lesión de este derecho implica la producción en internet de una primera conducta lesiva mediante la publicación sobre la víctima de sus datos privados, afectando a alguno de los derechos de su personalidad "*o a otros derechos fundamentales que estén en conflicto. La segunda se produce cuando el titular del medio, ya sea un foro, bitácora, cuenta de Facebook (…), quién no elimina la información que contiene el contenido ilícito publicado por terceros",* a sabiendas de la existencia de la

[15] Sentencia del Tribunal Supremo, sala de lo civil, núm. de resolución 1213/1989, 20 de febrero de 1989.

[16] Mª L. LOZANO, "La degradación de los derechos del art. 18 de la CE", Htp://noticiasjurídicas.com/artículos/05-Derecho-Constitucional/201403-la-degradacion-de-los-derechos-del-art-18-de-la-CE. Html (2015-1-21), p. 2.

[17] Sentencia del Tribunal Constitucional, sala 2ª, núm. de resolución 46/2002, 25 de febrero de 2002.

[18] Sentencia del Tribunal Supremo, sala de lo civil, núm. de resolución 2703/1987, 11 de abril de 1987.

[19] Sentencia del Tribunal Supremo, sala 1ª, núm. de resolución 471/2011, 15 de junio de 2011.

[20] J. FLORES FERNÁNDEZ, "Privacidad, factor de riesgo y protección en la violencia digital contra las mujeres", en I. CORREDOIRA, L. ALFONSO, Y L. COTINO HUESO, *Ciberacoso y violencia de género en redes sociales: Análisis y herramientas de prevención*, Centro de estudios Políticos y Constitucionales, Madrid, 2013, p. 319.

publicación sin el consentimiento de la víctima y, consecuentemente, la causación de un daño"[21].

2. LAS PARTICULARIDADES DE *FACEBOOK* EN EL TRATAMIENTO DE DATOS PERSONALES DE LOS DELITOS TECNOLÓGICOS

Existen multitud de prestadores de servicios de la sociedad de la información operantes en el mundo virtual como las redes sociales y buscadores. Estas empresas jurídicas ofrecen multitud de herramientas tecnológicas para compartir con otros cibernautas de todo el mundo mediante chats, foros, redes sociales, páginas *web*, etc…

Las redes sociales permiten la configuración de la privacidad en: la opción "*solo yo*" no es una opción utilizada por los usuarios. Esta modalidad ofrece al usuario ver las publicaciones consigo mismo. A modo de álbum personal. La opción "*amigos*" permitirá compartir sus publicaciones, fotos, lista de contactos y los datos personales dados serán vistos por la lista de contactos perteneciente a la carpeta "*amigos*". Lo mismo ocurre con la opción "*amigos excepto conocidos*". En la opción "*público*" el usuario compartirá toda su información con todos los usuarios de la red.

Cuando un usuario publica un comentario, foto, vídeo… será visto por la lista de contactos elegida como por ejemplo "*amigos*". Pero, esa información compartida podrá ser publicada por otro usuario perteneciente a la "*carpeta amigos*" con otra modalidad de las citadas. Por tanto, el problema surge cuando al final esa información será visionada y compartida por muchos usuarios no conocidos ni pertenecientes a la lista de contactos del editor de la publicación. En definitiva, los perfiles no son tan privados como se quiere.

Además, el usuario editor (ciberacosador) de información publicará en la modalidad "*público*" desde su muro personal porque quiere difundir la información con el mayor número de usuarios posible y en nada influye la configuración de privacidad del muro personal de la víctima.

Todas estas modalidades de configuración de la privacidad del muro generan tráfico de datos tras la información vertida en su muro. Ese tráfico de datos contiene datos personales de personas físicas. Estos datos serán almacenados mediante el tratamiento de datos por parte de los prestadores de servicios de la sociedad de la información con una finalidad determinada: publicitaria y comercial.

En una red social el individuo se identifica. Esta identificación posee un valor extraordinario porque gracias a ella la información, el mensaje o la publicidad son personalizados. Por otra parte, la viralidad de los mensajes multiplica la eficiencia y la eficacia de los tratamientos"[22].

---

[21] P. SIMÓN CASTELLANO, *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, op. cit., p. 42.

[22] A. RALLO LOMBARTE / R. MARTÍNEZ MARTÍNEZ, "Protección de datos personales y redes sociales: obligaciones para los medios de comunicación", en *Quaderns del Cac*, vol. XIV, núm. 37, 2011, p. 42.

La información recopilada por las redes sociales no se refiere solamente a los datos publicados (noticias, imágenes, videos) o datos personales facilitados para registrarse: fecha de nacimiento, sexo, aficiones, empleo, estudios, lugar de residencia, estado civil, lista de amigos… sino se almacenan otros datos: actividad en la red social, perfiles visitados, lugar de conexión, instrumento electrónico de conexión, horas de conexión, etc. Esto "ha propiciado un nivel sin precedentes de divulgación de información de carácter personal de las personas interesadas (y de terceros)"[23].

Las redes sociales utilizan la técnica del *Big Data.* El *Big Data* es el conjunto de datos masificados tratados a través de la tecnología, "empleando complejos algoritmos y estadística con la finalidad de hacer predicciones, extraer información oculta o correlativas imprevistas y, favorecer la toma de decisiones"[24].

La recolección de grandes conjuntos de datos y su posterior análisis bajo las herramientas del *Big Data* tiene un impacto directo en la preocupación por la protección de los datos personales de la víctima delitos tecnológicos, donde el Derecho debe hacer frente[25].

El tratamiento de datos personales consiste en: "recoger y almacenar, sin límite de espacio, infinidad de datos sobre un mismo individuo, realizar un auténtico catálogo de informaciones personales sobre él y además interrelacionar todos los datos existentes sobre una misma persona, con independencia de que se encuentren en archivos distintos, relativos a diferentes etapas de sus vidas, o que estos hayan sido recogidos incluso en lugares lejanos. Se puede acumular, sin límite la información y recabarla en cuestión de segundos con independencia de la distancia a la que se encuentre"[26].

El Reglamento 2016/679 (UE) contiene la definición de tratamiento de datos en su artículo 4 apartado 2º: **"***cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".*

Ante su definición me pregunto: si la incorporación de una imagen, un insulto o una burla respecto de la víctima en el muro del autor de la publicación constituyen tratamiento de datos personales.

Por consiguiente, la respuesta es afirmativa. Así pues, RALLO LOMBARTE, dice al respecto: "De ello se deriva que la conducta que consiste en hacer

[23] J. M. MARTÍNEZ OTERO, *La protección jurídica de los menores en el entorno audiovisual,* Aranzadi, Pamplona, 2013, p. 180.

[24] A. GARRIGA DOMÍNGUEZ, *Nuevos retos para la protección de datos personales. En la era del big data y de la computación ubicua*, op. cit., p. 28.

[25] A. GARRIGA DOMÍNGUEZ, *Nuevos retos para la protección de datos personales. En la era del big data y de la computación ubicua*, op. cit., p. 35.

[26] A. PLATERO ALCÓN, "El derecho al olvido en Internet. El fenómeno de los motores de búsqueda", *Opinión jurídico*, vol. 15, nº. 29, 2016, p. 245.

referencia, en una página *web*, a datos personales debe considerarse un tratamiento de esta índole"[27], ya sean identificadas "por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones"[28].

Todo tratamiento de datos se configura en ficheros para su organización. El Reglamento 2016/679 (UE) lo definen en el artículo 2 apartado c) y artículo 4 apartado 6ª): *"todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".*

Por otra parte, los prestadores de servicios de la información tienen la obligación de inscribir sus ficheros en la Agencia de Protección de Datos, determinando: el tipo de dato, la forma de su obtención, la finalidad y si se ha cedido a terceros. Pero, la Agencia Española de Protección de Datos no tiene la potestad de supervisar el contenido de los ficheros. Solamente conocerá su existencia.

Pero, existe una excepción en los ficheros de datos personales contemplada en el artículo 7 de la LOPD en su apartado 4ª: "*Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual".*

Por tanto, se necesita el consentimiento expreso e inequívoco de la víctima para gestionar en ficheros sus datos sensibles. Con el afán de subsanar este escollo la mayoría de prestadores de servicios de la información han facilitado formularios a sus usuarios para obtener su consentimiento, firmándose mediante certificado electrónico.

Con el objetivo de paliar esta exigencia legal las redes sociales lo han incluido en sus cláusulas de información en los mismos contratos, formularios, correos electrónicos donde el usuario aceptará tácitamente en el mismo acto de registro para ser miembro de la red social. Por regla general, el usuario al registrarse en una red social no lee las condiciones de uso ni de privacidad de la red social, sino las acepta con un simple "*click*".

Ante esto, cuando el acosador publique datos de la víctima, ella debería ser "informada de forma expresa, precisa e inequívoca por el responsable del fichero o su representante dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento y de la procedencia de los datos"[29]. Sin embargo, esto no ocurre. La víctima no es informada de la existencia de un fichero con sus datos ni de su contenido, si son datos sensibles o no, y si desea recibir esa información deberá solicitarla mediante "el derecho de acceso" a sus datos, ejerciendo los derechos Arco.

---

[27] A. RALLO LOMBARTE / R. MARTÍNEZ MARTÍNEZ, "Protección de datos personales y redes sociales: obligaciones para los medios de comunicación", op. cit., p. 43.

[28] A. RALLO LOMBARTE / R. MARTÍNEZ MARTÍNEZ, "Protección de datos personales y redes sociales: obligaciones para los medios de comunicación", op. cit., p. 43.

[29] J. M. BELTRÁN CASTELLANOS, "Aproximación al régimen jurídico de las redes sociales", en *Cuaderno electrónico de estudios jurídicos*, núm. 2, 2014, p. 71.

En atención a la persona física o jurídica responsable del fichero no recaerá en el acosador, puesto que la red social no le ha otorgado competencias para su gestión. Sin embargo, será responsable del tratamiento de datos de su muro, puesto que la red social le ha facilitado las herramientas necesarias para publicar datos propios o de terceros.

RALLO LOMBARTE lo ratifica, diciendo: "Se trata de un tratamiento en el que la persona usuaria que abre su cuenta carece de todo control sobre el fichero titularidad de la red social. Por ello, las obligaciones que se derivan para la organización en materia de cumplimiento de la LOPD resultan limitadas y, por ejemplo, no existe deber de inscribir un fichero ni de formalizar un contrato de acceso a datos por cuenta de terceros. Hay que partir de la base de que en este tipo de supuestos el uso se limita exclusivamente al alta en la red social y al empleo de las herramientas que en ella existen y no existe ninguna capacidad de decisión sobre la estructura, ordenación o gestión material de los datos distinta de la propia de la red social"[30].

Pero, ORTIZ LÓPEZ añade y, esta es la peculiaridad propia de las redes sociales: "los propios usuarios, que pueden ser personas físicas o jurídicas" también, forman parte del proceso. Si bien las personas suelen ser: "*afectador o interesados*, en otras ocasiones estas toman decisiones sobre la información que tratan, pudiendo llegar a ser considerados como responsables del tratamiento y asumiendo las obligaciones a las que estos están sujetos"[31].

3. CARACTERÍSTICAS DEL TRATAMIENTO DE DATOS EN LOS DELITOS TECNOLÓGICOS POR *FACEBOOK*

El tratamiento de datos debe cumplir con estos tres principios para su licitud: principio de información, principio del consentimiento del afectado y principio de calidad de los datos.

3.1. Principio de información

a) El principio de información está regulado en los artículos 13 y 14 del Reglamento 2016/679 (UE).

Este principio exige al responsable del tratamiento de datos (a la *ISP*[32] y al acosador) informar a la víctima sobre el uso, finalidad y destino de sus datos personales, así como con qué usuarios de la red se va a compartir. Sin embargo, los usuarios de las redes sociales no la informan sobre las cuestiones mencionadas sino se la etiqueta para potenciar su identificación en la red entre usuarios. Con ello, se fomenta el odio y la humillación de la víctima mediante la transmisión de sus datos sensibles.

La víctima podrá ejercer su derecho de bloqueo ante el etiquetado. Además, de solicitar su tutela mediante los otros derechos Arco. Pero,

[30] A. RALLO LOMBARTE, / R. MARTÍNEZ MARTÍNEZ, "Protección de datos personales y redes sociales: obligaciones para los medios de comunicación", op. cit., p. 46.

[31] P. ORTIZ LÓPEZ, "Redes sociales: funcionamiento y tratamiento de información personal", en A. RALLO LOMBARTE, / R. MARTÍNEZ MARTÍNEZ, *Derecho y redes sociales,* Civitas, Navarra, 2010, p. 32.

[32] Prestador de servicio de la información

estos derechos siempre se solicitan cuando la información nociva ya ha sido publicada y compartida por los usuarios de la red. Además, seguirá siendo compartida por todos los usuarios a nivel viral incluso fuera de nuestras fronteras.

3.2. Principio del consentimiento

El principio del consentimiento está regulado en el artículo 7 del Reglamento 2016/679 (UE). Se requiere un "*consentimiento inequívoco"* por parte de la víctima [33].

El consentimiento actúa como título habilitante para el tratamiento de datos personales[34] y debe reunir una serie de características para su validez[35]:

Libre: En el ámbito de las redes sociales el consentimiento libre contiene una información errónea. Al publicar un comentario o imagen se pierde el control sobre ella. La lista de contactos del titular de la publicación compartirá esa publicación con otros contactos no incluidos en lista de la víctima y sin pedirle ningún tipo de autorización. Esto ocurre con independencia del nivel de privacidad de su muro.

Informado: En las redes sociales la obligación de informar se suele realizar mediante formularios y cláusulas como ya se ha explicado.

Específico: El consentimiento debe ser para un tratamiento determinado y no generalizado.

En el ámbito de las redes sociales este tipo de consentimiento específico resulta muy complicado de aplicar. Los usuarios publican información y, posteriormente será compartida en la red por otros usuarios. Por tanto, el titular de la publicación perderá el control sobre sus datos y no sabrá el uso o destino de ellos. Este hecho hace alusión a la falta de seguridad jurídica existente en la red.

Inequívoco: Este tipo de consentimiento puede ser tácito o expreso, aunque para el tratamiento de datos sensibles no se admite la validez del consentimiento tácito. Se requiere "*un consentimiento expreso y escrito*", siendo nulo en sentido contrario.

La Agencia Española de Protección de Datos informa a través de su informe jurídico número 0342/2008: "*internet, y por ello las redes sociales, no son fuentes accesibles al público*" sobre el contexto del consentimiento inequívoco en una red social. Este se produce cuando se solicita: "*hacerse amigo de*" o cuando se "*acepta una invitación*". En estos casos se debe tener en cuenta:

---

[33] F. J. DURÁN RUIZ, "La necesaria intervención de las administraciones públicas para la preservación del derecho fundamental a la protección de datos de los menores de edad", op. cit., p. 140.

[34] J. L. PIÑAR MAÑAS, "El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales", en J. L. PIÑAR MAÑAS / S. RODOTA / P. L. MURILLO DE LA CUEVA / K. BENYEKHLEF / C. G. DE GREGORIO / P. FLEISHER, *Redes sociales y privacidad del menor*, Reus, Madrid, 2011, pp. 77-78.

[35] M. ARENAS RAMIRO, "El consentimiento en las redes sociales *on line*", en A. RALLO LOMBARTE, / R. MARTÍNEZ MARTÍNEZ, *Derecho y redes sociales*, Civitas, Navarra, 2010, pp. 122-123.

El consentimiento únicamente afecta a los datos de la persona agregada, nunca a su lista de contactos. Esta regla operará en los perfiles encontrados "abiertos" sin aplicar ningún tipo de privacidad en la red social.

Al mismo tiempo, el responsable del tratamiento de los datos debe ofrecer a la persona usuaria la posibilidad de retrotraerse en su decisión mediante la revocación de su consentimiento de autorización del tratamiento de sus datos personales. Por tanto, ese consentimiento válido otorgado en un principio puede ser revocable y constituirse en un consentimiento nulo porque el acosador no ha informado a la víctima sobre estos aspectos.

Así, lo determina la jurisprudencia del Tribunal Constitucional en la sentencia 117/1994[36]: "*Estos derechos, por tanto, son irrenunciables en su núcleo esencial y por ello, aunque se permita autorizar su intromisión o divulgación, será siempre con carácter revocable*".

En la misma línea, la Agencia Española de Protección de Datos dice: "los derechos fundamentales, y más si cabe los derechos de la personalidad, son irrenunciables, inalienables e imprescriptibles"[37].

3.3. Principio de calidad de los datos

En cuanto al principio de calidad de los datos personales está regulado en el artículo 5 del Reglamento (UE).

Estas disposiciones normativas se refieren a los principios de finalidad, pertinencia o proporcionalidad y veracidad informadores de todo tratamiento de datos de carácter personal.

El principio de finalidad exige a cualquier tratamiento de datos su justificación con el cumplimiento de un fin concreto, expreso y legal. Los datos personales derivados de delitos tecnológicos jamás se debieron someter a un tratamiento de datos por resultar desde un principio carentes de toda finalidad.

El principio de proporcionalidad requiere el tratamiento de los datos personales de forma adecuada, necesaria, no excesivo[38] y pertinente para alcanzar una concreta finalidad. Serán cancelados los datos personales cuyo tratamiento no cumpla con este objetivo.

El principio de veracidad requiere la veracidad de la información publicada de la víctima identificada e identificable en esos datos personales. Los datos publicados y tratados sin ser veraces se procederán a su cancelación o rectificación.

Entre estas medidas se incluye la elaboración de un Documento de seguridad contenido en el artículo 88 del Reglamento de la LOPD. En él se detallarán los datos almacenados, las medidas de seguridad adoptadas, la identificación de las personas con acceso a esos datos; garantizando la

[36] Sentencia del Tribunal Constitucional, sala 2ª, núm. de resolución 117/1994, 25 de abril de 1994.
[37] M. HERNÁNDEZ RAMOS, "El derecho al olvido digital en la web 2.0", op. cit., p. 14.
[38] J. L. PIÑAR MAÑAS, "El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales", *Redes sociales y privacidad del menor*, op. cit., p. 77.

confidencialidad, la seudonimización y el cifrado de los datos. En él se establecen tres niveles de seguridad de forma acumulativa en sus artículos 80 y 81:

- "Nivel medio = nivel básico + nivel medio. Serán adoptadas para ficheros que contengan datos: relativos a la comisión de infracciones administrativas o penales, sobre Hacienda pública, sobre servicios financieros, sobre solvencia patrimonial y un conjunto de datos suficientes, permitiendo identificar un perfil del afectado.
- Nivel alto = nivel medio + nivel alto. Aquellos que contengan datos de ideología, religión, creencias, origen racial, salud y vida sexual.
- Nivel Básico: Para todos los ficheros de datos de carácter personal.

Los datos personales de la víctima de delitos tecnológicos se encontrarían en un nivel de protección alto al ser datos sensibles. Se requiere auditar esas medidas de seguridad por parte de la red social cada dos años para salvaguardar su seguridad[39]. El incumplimiento de estos puntos producirá la nulidad del consentimiento obtenido y la ilicitud de los tratamientos a realizar o realizados.

4. HERRAMIENTAS DE PROTECCIÓN DE DATOS PERSONALES EN LOS DELITOS TECNOLÓGICOS

Por otro lado, España implementó la Directiva 2006/24 mediante la Ley 25/2007[40]. Según esta Ley cualquier red social no podrá en ningún caso revelar datos almacenados en su servidor sin autorización judicial previa. Por tanto, obliga a los servicios de telecomunicación a conservar los datos de sus usuarios durante un año y permite el acceso por parte de las autoridades policiales siempre y cuando sea durante la investigación de un delito grave.

Facebook cuenta con políticas de privacidad y servicio de ayuda ante los casos de vulneración de derechos fundamentales por el uso de las herramientas tecnológicas puestas a disposición de sus usuarios como es el caso de la divulgación y publicación de comentarios, imágenes o vídeos sobre una víctima de delitos tecnológicos.

Además, *Facebook* permite denunciar una conducta abusiva mediante el enlace "*denunciar*" situado junto a la mayoría de los contenidos publicados en *Facebook*. También, permite eliminar el "*etiquetado*" de una foto propia. De esta forma, se eliminarán los datos personales asociados a la imagen como nombre y apellidos, etc. Pero, el problema no se soluciona. La imagen de la víctima sigue siendo visionada por multitud de internautas.

También, tiene la opción "*reportar la publicación*" con diversos ítems asociados a esta opción: "*Es molesto o no es interesante, creo que no debería estar en Facebook, es spam, es pornografía, va en contra de mis ideas, fomenta la violencia o daños a una persona o un animal, es una*

[39] http://www.lant-abogados.com/proteccio-datos

[40] Ley 25/2007, de 18 de octubre, de conservación de datos relativa a las comunicaciones electrónicas y a las redes públicas de comunicaciones. BOE núm. 251.

noticia falsa, perjudica o humilla por raza, sexo, orientación o discapacidad…."

Además, aconseja a la víctima el "*bloqueo"* de la información y del usuario. Esta opción permite a la víctima no poder visualizar la información nociva sobre ella pero seguirá estando en *Facebook* y seguirá siendo compartida por los usuarios de esta red.

Por último, da la opción a la víctima de ponerse en contacto con el editor de la publicación, requiriéndole: el eliminado voluntario de su publicación, ocultado del muro toda información o bloquee esta información. Se solicita la voluntariedad al ciberacosador porque *Facebook* considera a los datos publicados en un muro propiedad de su usuario y no del titular de los datos personales publicados en el mismo. Esto agrava aún más la situación.

En sí misma, esta opción es muy costosa para la víctima. La víctima deberá investigar los perfiles personales de usuarios donde se han publicado sus datos y solicitarles su borrado voluntario. La difusión de la información es rápida, instantánea y automática. En pocos segundos la información ha podido llegar a millones de usuarios de la red. Este hecho y la voluntariedad de la acción de borrado resulta ser poco efectiva.

A su vez, aconseja hacer "*captaciones de pantalla*". Sin embargo, esto de nada servirá como prueba en un juicio sino se realiza mediante la oportuna orden judicial de registro y captura de pruebas por parte de los cuerpos de seguridad tecnológica de la policía nacional o de la guardia civil[41].

Asimismo, *Facebook* no se responsabiliza de los datos personales producidos en su plataforma virtual tal y como manifiesta en las condiciones de privacidad en su página oficial[42] donde la víctima ha prestado su consentimiento de forma tácita. No establece ninguna medida para evitar el problema sino solamente da recomendaciones cívicas a sus usuarios.

Sin embargo, los prestadores de servicios de la información establecerán otras medidas provisionales por infracciones graves o muy graves en aras a proteger a la víctima de delitos tecnológicos regulado en el artículo 41 de la LSSICE[43]:

1. Orden de cancelación de un perfil en una red social en internet.
2. Advertencia al público de "*la existencia de posibles conductas infractoras y la incoación del expediente sancionador de que se trate, así como las medidas adoptadas para el cese de dichas conductas".*
3. "*Precinto, depósito o incautación de registros, soportes informáticos y archivos informáticos y documentos*" para evitar la apertura de otra página *web* con el mismo contenido atentatorio contra los derechos fundamentales de la víctima.

[41] Resultado de la entrevista realizada a la jueza y juez de menores de valencia el 20 de abril del 2017.

[42] Ver: Política de condiciones y privacidad de *Facebook.*

[43] J. M. MARTÍNEZ OTERO, *La protección jurídica de los menores en el entorno audiovisual,* op. cit., pp. 247-248. Ley de servicios de la sociedad de la información.

4. Los responsables de la red social analizarán el hecho y eliminarán el resultado lesivo tras su denuncia.

Estas obligaciones constituyen un deber tal y como establece el Auto del Juzgado de lo Mercantil de Madrid, de 3 de noviembre, de 2004: "*de evitar el resultado lesivo*" mediante el cese o suspensión la prestación del servicio[44].

El artículo 16 de la LSSICE contiene la responsabilidad de los operadores de redes y dispone:

"Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

Por otra parte, se solicitó implantar las medidas tecnológicas adecuadas y posibles conforme al estado de la tecnología para impedir la indexación de la página por los Motores de Búsqueda de los datos personales del demandante, y, por ende, la eliminación de la noticia al considerarla atentatoria de sus derechos fundamentales.

En consecuencia, el apartado 38 de la sentencia lo justifica : *"en la medida en que la actividad de un motor de búsqueda puede afectar, significativamente y de modo adicional a la de los editores de sitios de Internet, a los derechos fundamentales de la vida privada y de la protección de datos personales, el gestor de este motor, como persona*

[44] Los apartados tercero y cuarto del artículo 11 de la LSSI dice: 3) "*En la adopción y cumplimiento de las medidas a que se refieren los apartados anteriores, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados"*. 4) *"En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales de forma excluyente para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo. En particular, la autorización del secuestro de páginas de internet o de su restricción cuando ésta afecte a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrá ser decidida por los órganos jurisdiccionales competentes".*

que determina los fines y los medios de esta actividad, debe garantizar, en el marco de sus responsabilidades, de su competencia y de sus posibilidades, (…) pueda llevarse a cabo una protección eficaz y completa de los interesados, en particular, de su derecho al respecto de la vida privada (38)"[45].

Ante esto, los prestadores de servicio de la información han adoptado una actitud preventiva para paliar esta responsabilidad, "fijando políticas de comportamiento para los participantes del foro y, asignando consecuencias a su incumplimiento tales como retirar el mensaje por solicitud de un usuario e incluso bloquear la *IP* de la que proviene el comentario".

Pero, esta actitud preventiva sobre los datos personales publicados en la plataforma virtual se realiza *a posteriori* de su publicación y visionado entre los internautas, y este hecho no garantiza la protección de los derechos personales de la víctima.

Por otra parte, esperar a que un órgano jurisdiccional informe sobre la existencia de vulneración de datos personales y otros derechos fundamentales provoca su rápida difusión a todos los usuarios de la red. Lo cual resulta ser un desastre para la víctima. Por tanto, las redes sociales *Facebook*, y *Google* deben poner al servicio del usuario medidas tecnológicas adecuadas para facilitar la seguridad en sus plataformas virtuales a todos los usuarios.

Por eso, es necesario aplicar normas de privacidad de diseño y por defecto. Una vez la información está en las redes sociales es muy difícil su eliminación o rectificación. La difusión y la pérdida de control son los principales problemas. Las redes sociales han impuesto en sus políticas de usos "la prohibición de generar contenido atentatorio o humillante entre los usuarios", sin embargo, sigue ocurriendo. Esta recomendación tiene un carácter preceptivo, es decir, no es vinculante y resulta ineficaz[46].

Lo que ocurre en la esfera virtual es un reflejo del problema existente en la esfera física. Pero, en el medio virtual todo se magnifica debido al poder de difusión exponencial que tiene y a la memoria perpetúa de la red, siendo difícil su eliminación por completo.

5. CONCLUSIÓN

Considero que el usuario de una red social no puede beneficiarse de las herramientas tecnológicas de la red para lesionar derechos fundamentales al compartir datos privativos.

La protección de los datos personales legitima a la víctima a tener el poder de disposición y control respecto a la publicación de sus datos y conocer dónde están almacenados, qué datos se tienen, quién los tiene,

[45] P. LÓPEZ ZAMORA, "¿Por qué Google?: Análisis de la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C131/12, sobre el llamado "derecho al olvido", *Nuevos retos y amenazas a la protección de los derechos humanos en la era de la globalización,* op. cit., p. 131.

[46] G. BUTTARELLI, "Los menores y las nuevas tecnologías", en J. L. PIÑAR MAÑAS / S. RODOTA / P. L. DE LA CUEVA / K. BENYEKHLEF / C. G. DE GREGORIO / P. FLEISHER, *Redes sociales y privacidad del menor*, Reus, Madrid, 2011, pp. 157-162.

quién los publicó con el fin de salvaguardar su reputación y evitar la intromisión ilegítima a su persona.

Así, pues, para la protección de los datos personales se requiere la identificación de la víctima en ellos de forma fácil y sin procedimientos complejos. De lo contrario, no se necesitaría solicitar su protección.

A su vez, se establecen una serie de obligaciones a las empresas tecnológicas para poder comercializar con esos datos, destacando la solicitud del consentimiento expreso e inequívoco a la víctima antes de publicar o almacenar sus datos personales y, más tratándose de datos calificados de sensibles, por su vinculación a su vida privada y personal. Sin embargo, esto no se produce en las redes sociales ni *Google*.

Es más, el tratamiento de datos personales de la víctima no cumple ninguno de los principios de información, consentimiento ni veracidad puesto que los datos son desproporcionados, es decir, no tienen una finalidad legítima y no son de interés público ni ciertos. Los datos personales que vulneran derechos fundamentales no pueden ser nunca "pertinentes, adecuados y no excesivos sino devienen lo contrario. Tampoco, tiene sentido la exactitud de estos datos y menos su actualización al ser falsos.

El agresor realiza una conducta totalmente ilegítima y *contra legem*. Por tanto, hace falta establecer los medios necesarios para concienciar al acosador de su aparente impunidad en la red y su correspondiente sanción ante la conducta lesiva producida.

El acosador será responsable ante la justicia de las publicaciones nocivas realizadas sobre la víctima puesto que la red social le está otorgando las herramientas necesarias para ello. Además, está realizando tratamiento de datos personales en su muro a modo de fichero personal y, aunque no tenga las mismas obligaciones que el prestador de servicios, debería informar y solicitar el consentimiento expreso e inequívoco a la víctima antes de publicar sobre ella. Pero, si *Facebook* no lo hace, tampoco el usuario.

Por el contrario, *Facebook* y el resto de operadores de internet escudan su responsabilidad en el "conocimiento efectivo", que según la Ley, lo tienen a través del comunicado u oficio por parte del juzgado. Antes de esto, *Facebook* solo da recomendaciones cívicas a la víctima y al resto de usuarios, no poniendo en marcha las herramientas para bloquear la información nociva publicada sobre la menor para evitar su efecto viral.

Y, todo esto, a pesar de estar obligados a proteger los datos para evitar: *su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natura*l.

Además, *Facebook* no cumple la Ley en cuanto a su funcionamiento, puesto que la víctima no tiene privacidad con independencia de la configuración de su muro: cualquiera puede publicar datos sobre ella sin que nadie lo impida en un primer momento. *Facebook* no informa a sus usuarios sobre el almacenamiento de sus datos en ficheros, obligación determinada por la Ley en un plazo de tres meses. Además, no puede

almacenar ficheros cuya finalidad sean datos sensibles y muchos datos contenidos en los muros de sus usuarios responden a datos sensibles.

Ante el etiquetado de la víctima en las redes sociales su alternativa para defenderse de esta agresión es desetiquetarse, consiguiendo eliminar los datos personales, normalmente nombre y apellidos, asociados a la imagen. Pero, el problema no se soluciona porque su imagen sigue estando en el muro de otros usuarios, pudiendo ser vista y compartida por multitud de internautas.

Ante esto, las redes sociales deberían utilizar herramientas tecnológicas para identificar una imagen con una persona concreta y, así evitar su publicación por terceras personas si estas no solicitan el previo consentimiento expreso e inequívoco del titular del dato personal a publicar.

Pero, se agrava más la situación de la víctima al considerar *Facebook* los datos publicados sobre ella de propiedad del usuario del muro, eximiéndose, *Facebook,* de nuevo su responsabilidad. Por eso, le recomienda a la víctima que solicite a los usuarios de los muros dónde aparece su información nociva su retirada voluntaria. Pero, dada la viralidad de la web la víctima no dispone de las herramientas necesarias para rastrear y buscar su información en cada unos de los perfiles contenidos en *Facebook*.

El consentimiento tácito otorgado por la víctima y resto de usuarios de *Facebook* al aceptar las políticas y uso de esta red social no cumple con los principios del tratamiento de datos, cuya exigencia es un consentimiento expreso e inequívoco. Tampoco la aceptación tácita en la negación de responsabilidad por parte de *Facebook*. Pero, las Leyes todavía no le exigen un comportamiento más eficiente a *Facebook*.

Por otra parte la víctima está totalmente indefensa ante las herramientas aplicadas por *Facebook* ante el oficio judicial o ante el contenido de un fichero puesto que no hay ningún cuerpo de inspectores que corroboren e investiguen sobre la aplicación y cumplimiento de lo ordenado.

También, *Facebook* aconseja a la víctima que denuncie estos hechos. Al mismo tiempo, el responsable del tratamiento de los datos debe ofrecer a la persona usuaria la posibilidad de retrotraerse en su decisión mediante la revocación de su consentimiento de autorización del tratamiento de sus datos personales. Por lo tanto, ese consentimiento válido otorgado en un principio puede ser revocable y constituirse en un consentimiento nulo porque el acosador y el prestador de servicio no han informado a la víctima sobre estos aspectos. Ante esto, la víctima solo puede revocar un consentimiento no prestado o prestado tácitamente, generando inseguridad jurídica.

Por otro lado, se requiere impedir la difusión viral realizada sin el consentimiento de su titular puesto que se están vulnerando sus derechos fundamentales. Pero, los mecanismos para impedirlos actúan una vez se ha producido el daño. Por lo tanto, teniendo en cuenta las características del medio como su inmediatez, rapidez y viralidad, esta opción no es aceptable.

Creo que se debería solicitar el consentimiento expreso e inequívoco de la persona cuyos datos de su titularidad se vayan a solicitar antes de su publicación. De este modo, la persona podrá controlar: quién publica, qué publica, dónde se almacena, en qué muros está y tendrá la disposición de sus datos personales en cualquier momento tal y como dispone la legislación estudiada.

De nuevo, se insiste en crear una eficaz regulación jurídica para dotar de seguridad a los usuarios de las redes sociales frente a la política de uso, de privacidad y ante el uso nocivo de la red por parte de algunos usuarios.

6. BIBLIOGRAFÍA

A. AGUSTINOY GUILAYN, y J. MONCLÚS RUIZ, *Aspectos legales de las redes sociales,* Bosch, Barcelona, 2016.

M. ÁLVAREZ CARO, *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*, Reus, Madrid, 2015.

M. ARENAS RAMIRO, "El consentimiento en las redes sociales *on line*", en A. RALLO LOMBARTE / R. MARTÍNEZ MARTÍNEZ, *Derecho y redes sociales*, Civitas, Navarra, 2010.

J. M. BELTRÁN CASTELLANOS, "Aproximación al régimen jurídico de las redes sociales", en *Cuaderno electrónico de estudios jurídicos*, núm. 2, 2014.

G., BUTTARELLI, "Los menores y las nuevas tecnologías", en J. L. PIÑAR MAÑAS / S. RODOTA / P. L. MURILLO DE LA CUEVA / K. BENYEKHLEF / C. G. DE GREGORIO / P. FLEISHER, *Redes sociales y privacidad del menor,* Reus, Madrid, 2011.

F. J. DURÁN RUIZ, "La necesaria intervención de las administraciones públicas para la preservación del derecho fundamental a la protección de datos de los menores de edad", *I Congreso internacional sobre retos sociales y jurídicos para los menores y jóvenes del siglo XXI*, Comares, Granada, 2013.

J. FLORES FERNÁNDEZ, "Privacidad, factor de riesgo y protección en la violencia digital contra las mujeres", en I. CORREDOIRA / L. ALFONSO / L. COTINO HUESO, *Ciberacoso y violencia de género en redes sociales: Análisis y herramientas de prevención,* Centro de estudios Políticos y Constitucionales, Madrid,2013.

A. GARRIGA DOMÍNGUEZ, *Nuevos retos para la protección de datos personales. En la era del big data y de la computación ubicua*, Dykinson, Madrid, 2015.

M. HERNÁNDEZ RAMOS, "El derecho al olvido digital en la *web 2.0*", en *Cuaderno de la cátedra de seguridad salmantina*, núm. 11, 2013.

P. LÓPEZ ZAMORA, "¿Por qué Google?: Análisis de la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C131/12, sobre el llamado derecho al olvido", en A. G. LÓPEZ MARTÍN / J. CHINCHÓN ÁLVAREZ, *Nuevos retos y amenazas a la protección de los derechos humanos en la era de la globalización*, Tirant lo Blanch, Valencia, 2016.

Mª L. LOZANO, "La degradación de los derechos del art. 18 de la CE", Htp://noticiasjurídicas.com/artículos/05-Derecho-Constitucional/201403-la-degradacion-de-los-derechos-del-art-18-de-la-CE. Html (2015-1-21).

J. M. MARTÍNEZ OTERO, *La protección jurídica de los menores en el entorno audiovisual,* Aranzadi, Pamplona, 2013.

J Mª. MARTÍNEZ OTERO, "Vulneración del honor y la propia imagen de una persona con discapacidad, con nulidad del consentimiento otorgado para aparecer en un programa televisivo de carácter humorístico. Comentario a la Sentencia del Tribunal Constitucional 208/2013, 16 de diciembre", *Revista boliviana de derecho,* nº. 18, 2014.

J. M. MORCILLO MARTÍNEZ, "Seguridad y prevención en redes sociales. Responsabilidades legales en Internet", en I. CORREDOIRA / L. ALFONSO / L. COTINO HUESO, *Ciberacoso y violencia de género en redes sociales: Análisis y herramientas de prevención,* Universidad internacional de Andalucía Servicio de publicaciones, 2015.

P. ORTIZ LÓPEZ, "Redes sociales: funcionamiento y tratamiento de información personal", en A. RALLO LOMBARTE / R. MARTÍNEZ MARTÍNEZ, *Derecho y redes sociales*, Civitas, Navarra, 2010.

A. PLATERO ALCÓN, "El derecho al olvido en Internet. El fenómeno de los motores de búsqueda", *Opinión jurídico*, vol. 15, núm. 29, 2016.

J. L. PIÑAR MAÑAS, "El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales", EN J. L. PIÑAR MAÑAS, S. RODOTA / P. L. MURILLO DE LA CUEVA / K. BENYEKHLEF / C. G. DE GREGORIO / P. FLEISHER, *Redes sociales y privacidad del menor*, Reus, Madrid, 2011.

A. RALLO LOMBARTE / R. MARTÍNEZ MARTÍNEZ, "Protección de datos personales y redes sociales: obligaciones para los medios de comunicación", en *Quaderns del Cac*, vol. XIV, núm. 37, 2011.

A. RALLO LOMBARTE, *El derecho al olvido en Internet: Google versus España*, Centro de estudios políticos y constitucionales, Madrid, 2014.

P. SIMÓN CASTELLANO, *El reconocimiento del derecho al olvido digital en España y en la UE: efectos tras la sentencia del TJUE de mayo de 2014*, Bosch, Barcelona, 2015.

S. Mª. SUÁREZ RUBIO, "Los menores como usuarios de redes sociales y su privacidad", en *Parlamento y Constitución*, núm. 16, 2014.

C. ZOCO ZABALA, *Nuevas tecnologías y control de las comunicaciones: LO 13/2015, de 5 de octubre, de modificación de la ley de enjuiciamiento criminal par el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica,* Civitas, Navarra, 2015.