Boletín Mexicano de Derecho Comparado
ISSN: 0041-8633
bmdc@comunidad.unam.mx
Universidad Nacional Autónoma de México
México

PLATERO ALCÓN, Alejandro
LA RESPONSABILIDAD DE LAS REDES SOCIALES: EL CASO DE ASHLEY MADISON
Boletín Mexicano de Derecho Comparado, núm. 150, septiembre-diciembre, 2017, pp. 1259-1288
Universidad Nacional Autónoma de México
Distrito Federal, México

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

LA RESPONSABILIDAD DE LAS REDES SOCIALES: EL CASO DE *ASHLEY MADISON*

THE RESPONSIBILITY OF SOCIAL NETWORKS: THE CASE OF ASHLEY MADISON

Alejandro PLATERO ALCÓN*

RESUMEN: El presente trabajo tiene por objeto analizar el tratamiento de datos personales efectuado por las redes sociales. Las redes sociales permiten a los usuarios realizar un nivel de interacción con otros usuarios, usuarios que pueden encontrarse en cualquier lugar del mundo; pero no todos los aspectos de las redes sociales son positivos, sino que al realizar una actividad jurídica, deben adaptarse a la normativa de protección de datos europea, y a la de los diferentes países en los que operen. Se analizará, a través del ejemplo de la red social *Ashley Madison*, si es posible aplicar la legislación nacional de protección de datos personales para exigir una responsabilidad a la misma, fundamentalmente civil, por inadecuado tratamiento de datos personales, siendo necesario exponer también el régimen de competencia judicial internacional aplicable.

Palabras clave: redes sociales, *Ashley Madison*, responsabilidad civil, competencia internacional.

ABSTRACT: This paper aims to analyze the processing of personal data by social networks. Social networks allow users to perform a level of interaction with other users, users can be found anywhere in the world. But not all aspects of social networks are positive, but when performing a legal activity, must adapt to the rules of European data protection, and the different countries in which they operate. It will be analyzed through the example of the social network Ashley Madison, *if possible apply national legislation on protection of personal data, to demand a responsibility to it, by improper processing of personal data, being necessary to expose also the regime international jurisdiction applicable.*

***Keywords**: Social networking,* Ashley Madison, *liability, international competition.*

* Becario de investigación en el área de Derecho Civil de la Universidad de Extremadura, España, correo: *alejandroplateroal@gmail.com.*

Boletín Mexicano de Derecho Comparado, nueva serie, año XLIX, núm. 150, septiembre-diciembre de 2017, pp. 1259-1288

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

SUMARIO: I. *Introducción.* II. *Las redes sociales en la era digital.* III. *La responsabilidad jurídica de las redes sociales: el caso de* Ashley Madison. IV. *Conclusiones.* V. *Bibliografía.*

I. INTRODUCCIÓN

La sociedad evoluciona y cada paso que afronta es originado por una revolución distinta. En la actualidad, la revolución que impera es la revolución tecnológica. Es inimaginable pensar en cualquier adulto que no tenga un *smartphone* con el que pueda disfrutar de las aplicaciones de moda, chatear con sus contactos, o simplemente leer las versiones digitales de los diarios. Pero esta revolución, al igual que todas las anteriores, no sólo ha proporcionado riquezas y avances, sino también controversias que el mundo del derecho debe solucionar.

Normalmente, una de las aplicaciones a las que tendrá acceso el ciudadano del siglo XXI será una red social,[1] a través de la cual se contactará con conocidos que se encuentren lejos, por ejemplo, y como no, poder subir fotos y videos de su vida. Lo que no muchos de estos ciudadanos conoce, son que cuando acceden a una red social, y rellenan sus datos, están suministrando datos personales suyos, a una compañía que normalmente opera en todo el mundo y que se lucrará económicamente a través de los datos de dichos ciudadanos. Es necesario analizar la actividad jurídica que desarrollan las redes sociales, la actividad concerniente al tratamiento de datos personales de sus usuarios, los cuales, en ocasiones son verdaderos consumidores.

La relación entre los usuarios de las redes sociales y las mismas difícilmente será gratuita, cuestión que también desconocen la mayoría de sus usuarios. Simplemente la cesión de un dato referido a la edad, o al lugar de nacimiento de cualquier usuario, ya reporta un beneficio económico a la red social. Es siempre una relación sinalagmática, ya que la red social ofrece servicios de interacción, pero a cambio de la cesión de datos personales, que como se verá en el presente trabajo, son objeto de cuantifi-

[1] El *Diccionario* de la Real Academia Española de la Lengua define en la 10a. acepción del vocablo "red" al "conjunto de computadoras o de equipos informáticos conectados entre sí y que pueden intercambiar información", y, más precisamente, red social como "plataforma digital de comunicación global que pone en contacto a gran número de usuarios".

Boletín Mexicano de Derecho Comparado, núm. 150, pp. 1259-1288

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

cación económica. Además, es preciso destacar que existen otro tipo de redes sociales, donde para acceder sí hay que abonar una determinada cantidad económica, por ejemplo, de *Ashley Madison.*

Las redes sociales en el marco de su actuación conviven con una serie de normas jurídicas de protección de datos personales, normas que en la mayoría de casos les son desconocidas, debido a que fundamentalmente las principales redes sociales tienen su base en países extracomunitarios, y poseen una normativa bastante distinta a la de protección de datos personales que lleva la comunidad europea desde 1990. Dicha cuestión no es baladí, sino que afecta a millones de usuarios, que observan cómo las redes sociales no cumplen con la normativa de protección de datos vigentes, y en ocasiones puede ocurrir que incluso sus datos personales salgan a la luz y se filtren, como ocurrió en el caso de la red social de encuentros: *Ashley Madison*. Es necesario analizar en el presente trabajo, el régimen de aplicación de la normativa comunitaria de protección de datos a las redes sociales.

II. Las redes sociales en la era digital

1. *Concepto y actividad de las redes sociales*

Internet es utilizado diariamente por más de 3,000 millones de personas, es decir, más del 40% de la población total del mundo.[2] Una de las grandes atracciones de Internet es, sin lugar a dudas, el fenómeno de las redes sociales. Actualmente, es muy difícil encontrar a alguna persona que declare no utilizar algunas de las más famosas como Facebook o Twitter.

Para poder realizar una correcta definición de las redes sociales en el mundo del derecho actual se debe, en primer lugar, poner de manifiesto la realidad de la sociedad de la información. La ley 34/2002, del 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI) define a los servicios de la sociedad de la información, como "todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario".[3]

[2] Disponible en: *http://www.20minutos.es/noticia/2130398/0/internet/usuarios/mundo*.

[3] Anexo letra A, de la Ley 34/2002, del 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, *BOE* núm. 166, del 12 de julio de 2002.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

Este concepto engloba "las actividades típicas de los prestadores de servicios de Internet y de los suministradores de servicios y contenidos en línea, incluida la actividad de los prestadores de servicios de redes sociales y la organización de subastas".[4] Así lo establece también el artículo 4o., LSSI, cuando dicta que los prestadores que dirijan sus servicios específicamente al territorio español "quedarán sujetos a las obligaciones previstas en esta Ley, siempre que ellos no contravengan lo establecido en tratados o convenios internacionales que sean aplicables".

En virtud de lo anterior, no cabe duda que las redes sociales se enmarcan dentro de los servicios de la información. Las redes sociales online pueden ser definidas como "servicios que se prestan a través de Internet y que posibilitan a los usuarios crear un perfil púbico, donde plasman datos personales e información, contando con herramientas que permiten interactuar con el resto de usuarios, sean afines o no al perfil".[5]

Tradicionalmente, las redes sociales se han enmarcado dentro del concepto de web 2.0, concepto que es definido como

> ...una nueva tendencia en el uso de las páginas webs, en la cual el usuario es el centro de la información y se convierte en generador de contenidos. Supone un cambio en la filosofía, una actitud, una forma de hacer las cosas que identifica el uso actual de Internet que hacen tanto los internautas como las empresas, pasando de ser meros consumidores a productores y creadores de contenido.[6]

Otros autores centran sus esfuerzos en diferenciar esta nueva etapa tecnológica de la anterior, definiéndola de la siguiente manera:

> ...en los medios tradicionales y en la web 1.0 los dueños de las webs tienen pleno control sobre ellas, tanto sobre la información que exponen como sobre el acceso y nivel de interactividad que quieren fomentar. Sin embargo, en

[4] Miguel Asensio, P., *Derecho privado en Internet*, *estudios y comentarios legislativos*, Madrid, Aranzadi, 2015, pp. 1-6.

[5] Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales *online*. Elaborado por el Instituto Nacional de Tecnologías de la Comunicación, 2009, p. 36.

[6] Heredero Campo, M., "Web 2.0: afectación de derechos en los nuevos desarrollos de la web corporativa", *Cuadernos Red de Cátedras Telefónica*, núm. 6, mayo de 2012, pp. 1-40.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

> la web 2.0 el control pasa directamente a todos los usuarios en igualdad de condiciones. El control está en los propios usuarios de la red social.[7]

En la actualidad, este concepto de web 2.0 ha quedado obsoleto. En efecto, el concepto predominante debe ser el de web 3.0, o *semantic web*.[8] Debe entenderse esta acepción de web semántica como aquella que contiene un nivel de organización de ideas y contenidos que ofrece una respuesta rápida a la demanda de información necesitada por el individual. Como se desprende de lo anterior, el desarrollo tecnológico es imparable, pero

> ...si bien el creciente desarrollo tecnológico representa grandes beneficios para las personas en términos de acceso al conocimiento y a la información, trae aparejado riesgos significativos para el titular de los datos personales, que circulan sin mayor control en la red, lo cual merma de manera importante la protección de su esfera privada y determinación informativa.[9]

Internet, sin lugar a dudas, ha incrementado el auge de derechos, como la libertad de información y la libertad de expresión; sin embargo, al mismo tiempo ha creado de una manera demoledora riesgos para derechos fundamentales tan importantes como el de la protección de datos o el derecho a la intimidad, entre otros. La población vive actualmente con una demanda de información constante y con una necesidad, a veces incomprensible, de narrar sus acontecimientos vitales a través de las redes sociales, de suerte tal que existen autores que relacionan las redes sociales con el ego, así: "el ego mueve el mundo y, sin duda, mueve las redes sociales, y en esta expresión continua de nuestro yo dejamos al pairo su parte más íntima, sin ser conscientes, mientras lo hacemos, de cuánto de nosotros exponemos ni del peso que esa exposición tendrá en el futuro".[10]

Las redes sociales son armas de doble filo, ya que, por una parte, el funcionamiento intrínseco de las mismas posibilita al ciudadano elec-

---

7 Cebrián Herreros, M., "La web 2.0 como red social de comunicación e información", *Estudios sobre el Mensaje Periodístico*, vol. 14, 2008, pp. 345-361.

8 Martínez López, F. *et al.*, *Evolution of the Web*, Suiza, Springer, 2016, p. 5.

9 Muñoz Massouh, A., "Eliminación de datos personales en Internet: el reconocimiento del derecho al olvido", *Revista Chilena de Derecho y Tecnología*, vol. 4, núm. 2, 2015, pp. 215-261.

10 Llaneza, P., "Derechos fundamentales e Internet", *TELOS, Cuadernos de Comunicación e Innovación*, octubre-diciembre de 2010, pp. 56-59.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

trónico poder comunicarse con amigos o personas que viven a una distancia que no permite su contacto directo, o permiten observar las fotos o videos que sus "amigos" deciden compartir, material que, en ocasiones, se sube de forma inconsciente. ¿Qué ocurre si alguien decide utilizar esas fotos para publicarlas con alguna información que puede ser dañina, o si decide utilizar los comentarios vertidos en redes sociales con el mismo fin? La respuesta a la cuestión anterior es muy importante, ya que el daño producido puede ser irreversible y además, en ocasiones, las fotos subidas, los comentarios expuestos y el estilo de vida que una persona ha querido describir a través de estas redes sociales puede ser contraproducente en un futuro. De esta manera, como publicó el *Huffington Post* en el proceso de contratación americano, más del 35% de las empresas no contrataban a empleados por aspectos que habían descubierto (investigando su pasado en redes sociales).[11] Éste fue el caso de Stacy Snyder, quien no fue acreditada para dar clases como profesora por la Conestoga Valley High School por subir a una red social una foto de ella tomando bebidas alcohólicas.[12]

Las redes sociales realizan una actividad jurídica, como es la correspondiente al tratamiento de datos personales, datos que las personas deciden normalmente colgar voluntariamente en las mismas. El derecho a la protección de datos es un derecho fundamental del individuo, consagrado en la normativa comunitaria, concretamente en la Carta de los Derechos Fundamentales de la Unión Europea del 18 de diciembre de 2000. Es el artículo 8o. de la Carta el que establece que

> ...toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente.[13]

[11] Adsuar Prieto, Y., "La elección de ser olvidado en la red: derecho o privilegio", *Actualidad Jurídica Aranzadi,* Pamplona, núm. 864, 2013, pp. 1-3.

[12] *Caso Drunken Pirate*, disponible en: *http://abcnews.go.com/TheLaw/story?id=4791295*.

[13] Artículo 8o. de la Carta de Derechos Fundamentales de la Unión Europea, *DOUE* núm. 83, del 30 de marzo de 2010.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

La regulación instrumental de este derecho fundamental se encuentra recogida a nivel comunitario en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 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. Así, el artículo 1o. de la Directiva 95/46 regula el objeto de la misma, siendo: "la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales".[14]

Pero la Directiva de 1995 ha quedado obsoleta, ya que en 1995 no se podría tener en la mente los avances que la revolución informática está produciendo en el mundo.[15] Por eso, la Comisión Europea aprobó el 25 de enero de 2012 una propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de datos, propuesta que ha sido modificada en números ocasiones, y cuyo último texto disponible se encuentra fechado en junio de 2015.[16] El texto fue presentado para su adopción como posición del Consejo en primera lectura, y ésta se remitió al Parlamento para su aprobación. El Reglamento entró en vigor el 24 de mayo de 2016 y será aplicable a partir de la primavera de 2018, por lo tanto será de aplicación el régimen jurídico europeo determinado anteriormente.[17]

---

[14] Artículo 1o. de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 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, *DOUE* núm. 281, del 23 de noviembre de 1995.

[15] Batuecas Caletrío, A., "El control de los padres sobre el uso que sus hijos hacen de las redes sociales", en Aparicio Vaquero, Juan Pablo y Batuecas Caletrío, Alfredo (coords.), *En torno a la privacidad y la protección de datos en la sociedad de información*, Granada, Comares, 2015, p. 137.

[16] Disponible en: *http://data.consilium.europa.eu/doc/document/ST95652015INIT/es/pdf*. Respecto a los principales cambios que se introducirán en el nuevo reglamento, véase, por ejemplo, Hert, P. y Papakonstantinou, V., "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?", *Computer Law and Security Review*, núm. 32, 2016, pp. 179-194.

[17] Véase*: http://www.consilium.europa.eu/es/policies/data-protection-reform/data-protection-regulation/*.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

En todos los países europeos, la protección de datos personales se encuentra establecida directamente en sus Constituciones, debido a la influencia de la normativa europea. Así, en el caso de España, el derecho fundamental a la protección de datos aparece consagrado en el artículo 18.4 de la Constitución española. Dicho precepto dicta: "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".[18] La regulación instrumental del derecho fundamental a la protección de datos se encuentra en el ordenamiento jurídico español en la Ley Orgánica 15/1999, del 13 de diciembre, De protección de datos (LOPD); ley que fue dictada como consecuencia de la necesidad de trasponer la Directiva 95/46 aludida anteriormente y su Reglamento de desarrollo aprobado por el Real Decreto 1720/2007, del 21 de diciembre.

Distinta al caso de los países europeos es la regulación del derecho a la protección de datos en los países de Latinoamérica. En efecto, dependiendo del país que se analice, puede ser que la protección de datos personales se encuentre protegida expresamente en la Constitución de un país, como ocurre en Colombia, Ecuador y Perú, o no, como es el caso de Costa Rica o el de México, pero entre este grupo de Estados destaca el paradigmático caso de Chile, ya que éste fue el primer país de Iberoamérica que aprobó una ley de protección a la privacidad, la Ley 19628, sobre protección de la vida privada, que contiene los principios fundamentales de la protección de datos personales.[19]

2. *Los principios del tratamiento de datos personales*

Después de hacer mención al marco jurídico existente tanto a nivel europeo como a nivel nacional del derecho fundamental a la protección de datos personales, es menester desarrollar los principios de un adecuado tratamiento de datos personales. Para ello, toca hacer mención a diferentes artículos de la LOPD, Ley que tiene por objeto "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades

[18] Artículo 18.4 de la Constitución española, *BOE* núm. 311, del 29 de diciembre de 1978.

[19] Chen Mok, S., "Privacidad y protección de datos: un análisis de legislación comparada", *Diálogos, Revista Electrónica de Historia*, vol. 11, núm. 1, 2010, p. 128.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".[20] El propio texto legal establece en su artículo 3o. una definición de tratamiento de datos personales, considerando que existe tratamiento cuando se produzcan operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Principio de calidad de los datos. El artículo 5o. de la LOPD regula este principio y establece que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Los datos de carácter personal, objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Principio del consentimiento del afectado. Regulado en el artículo 6o. de la LOPD, establece que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa, consentimiento que podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. En relación con la posibilidad de revocación, algunos autores consideran que "teniendo en cuenta la trascendencia del consentimiento, que la disponibilidad de los datos que, en su caso, lo fundamenta afecta a derechos fundamentales de la persona y que la directiva no dice nada en relación con la revocación, solo cabe concluir que, en principio, la revocación del consentimiento ha de ser tan libre como la emisión".[21] Además, se establece una excepción a la necesidad de prestar consentimiento, como ocurre en el caso de que los datos de carácter personal se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias.

[20] Artículo 1o. de la Ley Orgánica 15/1999, de 13 de diciembre, De protección de datos de carácter personal, *BOE* núm. 298, del 14 de diciembre de 1999.

[21] Palacios González, M., "El poder de autodeterminación de los datos personales en Internet", *Revista de Internet, Derecho y Política*, núm. 14, mayo de 2012, p. 66.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

Principio de seguridad de los datos personales. El artículo 9o. de la LOPD regula una de las salvaguardas más importantes del derecho fundamental a la protección de datos personales. En efecto, este precepto establece el deber que el responsable del tratamiento deberá adoptar, como las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten 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 natural.

Principio del deber de secreto. En este caso, es el artículo 10 de la LOPD el que lo establece, utilizando los siguientes términos:

> ...el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Una vez expuestos los anteriores principios y salvaguardas de un adecuado tratamiento de datos personales, es preciso mencionar la posibilidad de exigir el cumplimiento tanto en vía administrativa como en judicial de los mismos. En efecto, el artículo 18 de la LOPD establece que las actuaciones contrarias a lo dispuesto en su articulado pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos.[22] Y contra las resoluciones que ésta emita procederá recurso contencioso-administrativo.

Puede ocurrir que de un inadecuado tratamiento de datos personales pueda surgir para el usuario una lesión de otro derecho (piénsese, por ejemplo, en una posible filtración de los mensajes privados en una determinada red social, de la que puede derivarse una violación del derecho al honor o a la intimidad personal del usuario). En estos casos, la normativa, objeto de análisis, establece que los interesados que como consecuencia

[22] Artículo 35, LOPD: "La Agencia 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. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno".

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

del incumplimiento de las salvaguardas previstas, debido a la incorrecta actuación del responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos, tendrán derecho a ser indemnizados. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las administraciones públicas, pero en el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria. En relación con este derecho a obtener una indemnización, existen opiniones que consideran que "la formulación de la Ley es excesivamente genérica y resulta insuficiente al no concretar con cierto rigor los requisitos que han de cumplirse para reclamar la indemnización".[23]

III. La responsabilidad jurídica de las redes sociales: el caso de *Ashley Madison*

1. *Análisis de los términos y condiciones de uso de* Ashley Madison

El objetivo del presente apartado es asociar la realidad práctica del tratamiento de datos personales realizado por parte de una red social, a la normativa vigente de protección de datos descrita con anterioridad. Para ello, en primer lugar, es menester recordar que cuando una persona accede a una red social y rellena un cuestionario con sus datos, está otorgando su consentimiento para que sus datos personales sean tratados, aunque ésta desconozca que esté autorizando dicha cesión. Así lo establece R. Martínez Martínez:

> ...la mayor parte de nuestra sociedad carece de una cultura de protección de datos y ello se manifiesta de modo contundente en los procesos de captación de datos personales. Basta con comprobar hasta qué punto, ya sea en Internet o en soporte físico convencional, se tiende a actuar de modo que la prestación del consentimiento se plantee como un trámite tedioso más que el titular de los datos personales debe cumplimentar cuanto antes para llegar a

[23] Aberasturi Gorriño, U., "El derecho a la indemnización del artículo 19 de la Ley Orgánica de Protección de Datos de Carácter Personal", *Revista Aragonesa de Administración Pública*, núm. 41-42, 2013, p. 175.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

> su objetivo de comprar un bien o recibir un servicio. Tanto más tediosa será la técnica empleada cuanta mayor información se desee obtener.[24]

Realizada la anterior precisión, es el momento de hacer mención a la red social *Ashley Madison* ¿Qué ocurre si una persona se registra en una web de infidelidades, depositando todos sus datos personales, y éstos son objeto de una publicación posterior? En ocasiones, la realidad supera a la ficción, y el ejemplo anterior ha ocurrido en la praxis, ya que se han filtrado los datos de los usuarios registrados en la página de citas *Ashley Madison.*[25] En agosto de 2015 se publicaron los datos de casi 39 millones de personas que formaban parte de este portal web, personas que han visto cómo su intimidad ha sido violada a través de Internet. La empresa española Tecnilógica elaboró un mapa donde se mostraban el punto exacto de localización de estos usuarios,[26] y a modo de curiosidad establecieron que São Paulo y Nueva York encabezan el *ranking* con el mayor número de ciudadanos registrados, 374,554 y 268,247, respectivamente.

Entre las cuestiones que los usuarios tendrán que desmontar de dicha red social para poder exigir una indemnización a la misma destaca fundamentalmente la respuesta a dos en concreto, ¿queda sujeta esta red social con sede en Chipre a la normativa europea, y por ello, a la española, de protección de datos personales?, ¿puede un usuario de esta red social con domicilio en España, acudir a los tribunales españoles para pedir esta indemnización?

Para responder a las dos cuestiones se debe partir, en primer lugar, de la exposición de las condiciones de términos y servicios que establece *Ashley Madison* en el proceso de registro en la misma. Sobre esta última cuestión destaca especialmente la siguiente información obtenida de su propia página web:

> ...si bien hacemos todo lo posible por mantener la seguridad necesaria para proteger sus datos personales, *no podemos garantizar la seguridad o la privacidad de la información* que usted proporciona a través de Internet o de sus mensajes de

[24] Martínez Martínez, R., "El derecho fundamental a la protección de datos: perspectivas", *Revista de Internet, Derecho y Política*, núm. 5, 2007, p. 56.

[25] Web de Ashley Madison: *https://www.ashleymadison.com/?c=11*.

[26] Véase: *https://tecnilogica.cartodb.com/viz/56e702fe469311e58f790e853d047bba/public_map*.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

> correo electrónico. Nuestra Política de Privacidad queda incorporada a los Términos mediante esta referencia. Acepta eximirnos de responsabilidad, tanto a nosotros como a nuestra casa matriz… reconoce y entiende que, debido a la incerteza implícita en el uso de los sistemas de información e internet y a los potenciales ataques malintencionados por parte de entidades externas, no podemos garantizar que el uso de nuestros sistemas, sitios web y aplicaciones sea totalmente seguro.[27]

En vista de la anterior afirmación, el usuario que se registra, si realiza una lectura comprensiva del texto, observará cómo la propia empresa no asegura una privacidad de su información privada, siendo esto una razón de peso para no proceder a registrarse en el portal web. En este sentido, se debe recordar el principio de seguridad de los datos personales que se encuentra en el artículo 9o. de la LOPD que, como se estableció con anterioridad, obliga al encargado del tratamiento a adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten 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, provengan de la acción humana o del medio físico o natural.

La cláusula sexta de los términos y condiciones de uso también merece ser destacada, estableciendo la misma que

> ...al enviar contenidos (como, entre otros, su foto o información de su perfil o de otro tipo) a nuestro Sitio, usted declara que renuncia absolutamente a todos los derechos morales de ser identificado como autor del contenido, incluso su fotografía y perfil, y derechos similares en cualquier jurisdicción del mundo. Al enviar contenidos (incluso, entre otros, su fotografía y perfil) usted automáticamente otorga, y declara un derecho ilimitado, perpetuo, mundial, no exclusivo, libre de regalías, irrevocable y transferible y una licencia para usar, reproducir, exhibir, transmitir. No tenemos ninguna obligación de eliminar su perfil, fotografía e información de nuestro Servicio, incluso después de haber cancelado su membrecía [*sic*].[28]

---

[27] Apartado 4. I de los términos y condiciones de registro en *Ashley Madison*, disponible en: *https://www.ashleymadison.com/app/public/tandc*

[28] Cláusula sexta apartado *a* de los términos y condiciones de registro en *Ashley Madison*, *https://www.ashleymadison.com/app/public/tandc*.p.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

De lo anterior se extrae que el usuario que quiera formar parte de la red social objeto de estudio debe aceptar renunciar a reclamar cualquier derecho moral respecto a su posible identificación como miembro de la red social en todas las jurisdicciones. En un sentido similar al anterior, la cláusula decimoquinta establece que

> ...usted acepta que no seremos responsables de ningún daño, incluso daños directos, indirectos, incidentales, punitorios, especiales, emergentes o ejemplares (aunque hayamos sido informados de la posibilidad de que ocurran tales daños), que se relacionen con lo siguiente: (c) divulgación o alteración de su contenido, o acceso no autorizado a este [*sic*].[29]

Realmente, esta cláusula debe considerarse nula de acuerdo con la legislación española, ya que el Código Civil en sede contractual establece en el artículo 1256 que la validez y el cumplimiento de los contratos no pueden dejarse al arbitrio de uno de los contratantes, y en el artículo 1102, que la responsabilidad procedente del dolo es exigible en todas las obligaciones, siendo la renuncia de la acción para hacerla efectiva nula. También debería hacerse mención en este momento a la normativa de protección a los consumidores y usuarios, pero la misma se efectuará cuando se responda a la segunda cuestión planteada anteriormente, ya que la posible consideración de la relación entre una red social y sus usuarios como de consumo, altera el régimen de competencia judicial internacional aplicable.

En la cláusula decimonovena se puede encontrar una sumisión obligatoria a resolver todas las controversias jurídicas que se planteen contra *Ashley Madison,* mediante un proceso arbitral en Chipre, que además se desarrollará conforme a la Ley de Arbitraje de Chipre. Se establece además que la decisión del árbitro será definitiva y vinculante; no obstante, el juicio del árbitro podrá ser presentado en cualquier tribunal que tenga jurisdicción y ejecución posterior u otro proceso legal puede ser emitido al respecto. La responsabilidad de ambas partes se limita a la suma de 5,000 dólares por daños. Las partes renuncian a recibir daños indirectos, emergentes, especiales, punitorios o ejemplificatorios, o daños o reparaciones que excedan el monto permitido por este Acuerdo, y el árbitro no tendrá facultades para otorgar estos daños.

[29] *Ibidem*, cláusula decimoquinta.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

En último lugar se debe hacer mención a la cláusula vigesimosegunda, donde se establece que el usuario debe aceptar que la red social sólo tiene su base en Chipre y cualquier conflicto se debe resolver aplicando su legislación. Así:

> ...usted acepta que: (i) se entenderá que el Servicio tiene su base únicamente en la República de Chipre; (ii) el Servicio se considerará un servicio pasivo que no hace lugar a jurisdicciones en razón de la persona sobre *Ashley Madison*, sean estas específicas o generales, en jurisdicciones distintas de la República de Chipre; y (iii) los Términos, y su relación con *Ashley Madison* conforme a estos Términos, estarán regidos por las leyes substantivas internas de la República de Chipre, independientemente de sus principios de conflictos entre leyes. Estos Términos serán interpretados de acuerdo con la ley de la República de Chipre, sin hacer referencia a los principios de conflictos entre leyes.[30]

Para responder a las dos cuestiones enunciadas con anterioridad, aparte de hacer mención a los términos y condiciones de uso, se debe analizar el apartado que lleva por rúbrica "política de privacidad". En efecto, *Ashley Madison* establece en el mismo, cuestiones muy importantes dentro del derecho fundamental a la protección datos, como el tipo de datos que almacena:

> ...recopilamos datos personales de usted utilizando diversos medios, incluido cuando se registra con nosotros en la página Web. Asignamos categorías a los datos personales en dos tipos de información: información que identifica a la persona ("IIP") e información que no identifica a la persona ("INIP"); a esta última también se la denomina datos agregados y anónimos. Algunos de los datos recopilados pueden estar relacionados con la salud, el origen étnico, la vida sexual u otra información que puede considerarse confidencial.[31]

Respecto a los datos referentes al origen étnico, la salud o la vida sexual, se debe establecer que la normativa española de protección de datos, en su artículo 7o. constituye la obligación de que sólo pueden ser recabados, tratados y cedidos cuando sea de interés general, cuando así lo disponga una

[30] Cláusula vigesimosegunda de los términos y condiciones de registro en *Ashley Madison*, *https://www.ashleymadison.com/app/public/tandc*

[31] Punto primero de la Declaración de Privacidad de *Ashley Madison*, *https://www.ashleymadison.com/app/public/privacy.p*.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

ley o el afectado consienta expresamente. Realmente, es discutible que en el caso en concreto, la aceptación general de las condiciones de términos y servicios haciendo *click* en el apartado "Aceptar" sea suficiente para que medie un consentimiento expreso por parte de los usuarios acerca del tratamiento de datos personales especialmente protegidos.[32]

En la declaración de privacidad se establece cómo el usuario autoriza a la red social para compartir o vender todos los datos personales que recopile, incluso algunos tan trascendentes como los de origen étnico o la vida sexual con terceros, o también se reservan el derecho de compartir la información financiera de los clientes, ya que esta red social es de pago. En último lugar, se debe destacar que *Ashley Madison* se reserva el derecho de alterar su política de privacidad sin necesidad de pedir el consentimiento a sus usuarios sobre la misma, ya que consideran que el simple uso de la red social provocaría un consentimiento tácito al cambio realizado por parte de los usuarios, aunque se establecen dos excepciones donde si preguntaran a los usuarios si aceptan o no dicha política de privacidad: Suecia y España. En el caso de España, se establece expresamente que

> ...podemos realizar cambios en esta Declaración de privacidad en cualquier momento y siempre se los notificaremos antes de que tales cambios materiales entren en vigor. Si las correcciones afectan al procesamiento de sus datos personales, le solicitaremos su consentimiento expreso a la Declaración de privacidad revisada.[33]

2. *Análisis de la aplicación de la normativa europea y española de protección de datos*

Una vez analizadas las políticas de privacidad y sus términos y condiciones de servicios, es necesario dar respuesta a las dos cuestiones enunciadas, empezando por la relativa al derecho aplicable; por tanto, ¿queda sujeta esta red social con sede en Chipre a la normativa europea, y por ello a la española de protección de datos personales?

---

[32] Sanjuro Rebollo, B., *Manual de Internet y redes sociales*, Madrid, Dykinson, 2015, pp. 106-112, donde se establecen los diferentes niveles de protección de los datos personales, distinguiendo tres tipos: básico, medio y alto.

[33] Punto decimoprimero de la Declaración de Privacidad de *Ashley Madison*, *https://www.ashleymadison.com/app/public/privacy.p*.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

Para responder a esta cuestión se debe en primer lugar partir de lo previsto en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 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, anteriormente citada. Concretamente, en su artículo 4o. establece que los Estados miembros aplicarán las disposiciones nacionales que hayan aprobado para la transposición de la Directiva, en el caso de España, la LOPD, en una serie de supuestos:

a) El tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros, deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el derecho nacional aplicable.
b) El responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del derecho internacional público.
c) El responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.

En el caso objeto de estudio, parece que el primer apartado de los descritos anteriormente es el que resulta de aplicación, ya que *Ashley Madison* opera en varios Estados distintos, debiendo, según lo establecido en el apartado 4.1 a), adoptar las medidas necesarias para garantizar que cada uno de dichos *establecimientos* cumpla las obligaciones previstas por el derecho nacional aplicable; sin embargo, la cuestión queda lejos de resolverse tan simplemente. En efecto, como se instituyó en el análisis de las condiciones de términos y servicios de la red social, la cláusula vigesimosegunda establece que el usuario debe aceptar que la red social sólo tiene su base en Chipre, y cualquier conflicto sólo se debe resolver aplicando su legislación, de suerte tal que si efectivamente, independientemente de la

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

validez o no de esa cláusula, *Ashley Madison* sólo posee un establecimiento en Chipre y no en ningún otro país, lo cual resulta complicado aplicar literalmente la normativa comunitaria que menciona expresamente el término "establecimiento".

Además, la propia Ley Orgánica de Protección de Datos española dispone en su artículo 2o. que se regirá por la misma, todo tratamiento de datos de carácter personal cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento, cuestión que no ocurre en el presente caso, y cuando al responsable del tratamiento no establecido en territorio español le sea de aplicación la legislación española de acuerdo con normas de derecho internacional público. Este segundo supuesto sí se encuentra en conexión con lo establecido en la normativa europea, pero aun así, con base en lo previsto en ambas normativas, resulta difícil determinar si efectivamente *Ashley Madison* ha actuado de forma incorrecta y los usuarios españoles podrían tener derecho a una indemnización en vía civil[34] debido a un inadecuado tratamiento de datos personales,[35] en virtud de lo previsto en el artículo 19 de la LOPD.

La respuesta a la pregunta necesita alguna precisión más, y la misma al no encontrarse en los textos legales, debe venir suministrada por los tribunales de justicia. En efecto, el Tribunal de Justicia de la Unión Europea se ha pronunciado en dos ocasiones acerca de la aplicación de una normativa nacional de un país miembro sobre protección de datos personales hacia una compañía que no tenía su establecimiento *de facto* en el

[34] Este resarcimiento en vía civil de los daños causados por prestadores de servicios *online* ha sido estudiado, entre otros, por Rubí Puig, A., "Derecho al honor *online* y responsabilidad civil de ISPs. El requisito del conocimiento efectivo en la SSTS, Sala Primera, del 9 de diciembre de 2009 y 18 de mayo de 2010", *InDret, Revista para el Análisis del Derecho*, núm. 4, 2010, pp. 1-20. Véase también Soler Presas, A., "Am I in Facebook?", *InDret, Revista para el Análisis del Derecho,* núm. 3, julio de 2011, pp. 1-44.

[35] El derecho fundamental de protección de datos personales se encuentra en conexión con los derechos al honor, a la intimidad y a la propia imagen, ya que todos forman los denominados derechos de la personalidad. Por tanto, es probable que cuando se produzca un inadecuado tratamiento de datos personales, se produzca también una posible violación de los restantes derechos. Véase, por ejemplo, la obra de Escribano Tortajada, P., "Algunas cuestiones sobre la problemática jurídica sobre el derecho al honor, a la intimidad y a la propia imagen en Internet y las redes sociales", en Fayós Gardó, Antonio (coord.), *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Madrid, Dykinson, 2014, pp. 61-85.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

país en cuestión. El primer pronunciamiento se produjo con la sentencia TJUE (Gran Sala) del 13 de mayo de 2014, más conocida como sentencia *Google*,[36] sentencia que ha venido a consagrar la existencia de un auténtico derecho al olvido[37] de los ciudadanos contra la actividad de los motores de búsqueda. El pronunciamiento del TJUE tiene su origen en una cuestión prejudicial planteada por la Audiencia Nacional Española, a través de su auto del 27 de febrero de 2012, donde decidió plantear al Tribunal de Justicia de la Unión una cuestión prejudicial de interpretación al amparo del artículo 267 del Tratado de Funcionamiento de la Unión Europea.

El asunto consistía, entre otras cuestiones, en determinar si *Google*, compañía americana, debía respetar su actuación en España, la normativa europea y española de protección de datos. De lo enunciado hasta el momento, parece que el caso se asemeja al objeto del presente estudio, ya que se pretende aplicar la normativa europea y española a una compañía que no tiene su sede en el Estado miembro en cuestión, siendo determinante para ello, como se estableció anteriormente en la exposición del artículo 4o. de la Directiva de protección de datos comunitaria, la existencia de un establecimiento en el país en cuestión para poder aplicar la normativa propia del mismo. Pues bien, el TJUE en su sentencia del 13 de mayo de 2014 estableció el criterio interpretador del término "establecimiento", considerando que dicha interpretación debe realizarse de forma flexible.

Google siempre mantuvo en el proceso la inaplicabilidad de la Directiva, debido a que las funciones de buscador las realiza *Google Search*, compañía con sede en Estados Unidos de América, mientras que en España el único establecimiento con el que contaba era *Google Spain*, empresa que

[36] Esta compañía ha provocado numerosos problemas relacionados con las normativas de privacidad y protección de datos en todo el mundo. Véase una obra donde se analizan de manera individual los problemas de privacidad de dicha compañía, Schinasi, J., "Practicing Privacy Online: Examining Data Protection Regulations Through Google's Global Expansion", *Columbia Journal of Transnational Law*, vol. 52, núm. 2, 2014, pp. 569-616.

[37] El derecho al olvido es la capacidad para ejercer los derechos de rectificación y cancelación de datos por parte de un ciudadano, que encuentran como en la red aparece información suya difamatoria, falsa, o incluso siendo verdadera, puede encontrarse obsoleta la misma. Sobre esta figura véase, entre otros, Martínez Otero, J., "El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google *vs*. AEPD y Mario Costeja", *Revista de Derecho Político*, núm. 93, mayo-agosto de 2015, pp. 103-142; Bartolini, C. y Siry, L., "The Right to be Forgotten in the Light of the Consent of the Data Subject", *Computer Law and Security Review*, núm. 32, 2016, pp. 218-237.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

se dedicaba a gestionar los ingresos publicitarios, "lo cual permite que el servicio del motor de búsqueda resulte rentable y, al mismo tiempo, se constituya en el medio que permite realizar esas actividades".[38] El Tribunal en el análisis de esta cuestión llega a la conclusión de que la actividad desarrollada por *Google Spain* se enmarca dentro del término establecimiento utilizado por la Directiva, ayudado en este razonamiento por lo establecido en el considerando 19 de la Directiva, que añade dos requisitos para catalogar una actividad desarrollada por una organización como un establecimiento, que son, en primer lugar, el ejercicio efectivo y real de una actividad mediante una instalación estable, y en segundo lugar, la no importancia de la forma jurídica del establecimiento en cuestión.[39] Para llegar a esta conclusión, el TJUE además "consideró que la protección eficaz y completa perseguida por la Directiva 95/46 obliga a prescindir de una interpretación restrictiva del término marco de actividades reducida a que el tratamiento deba realizarse por el establecimiento".[40]

De lo anterior, se puede extraer que para el TJUE en el marco del tratamiento de datos personales, el término "establecimiento" como criterio para aplicar la normativa comunitaria y la nacional de un país debe considerarse de manera flexible; pero para poder responder a la cuestión planteada acerca de la aplicabilidad de la normativa comunitaria y española a la red social *Ashley Madison* todavía debe destacarse el contenido de la sentencia del TJUE del 1 de octubre de 2015, más conocida con el nombre de *Weltimmo*.[41] Dicho proceso versaba en la controversia existente entre una empresa que se dedicaba a vender pisos por Internet en diferentes países, y con domicilio establecido en un país miembro de la Unión, como es Eslovaquia, y la agencia de protección de datos de Hungría. En síntesis, se juzgaba si la agencia húngara podría aplicar sus normas de protección

[38] Maqueo Ramírez, M., "Análisis comparativo de las resoluciones emitidas por el tribunal de justicia de la Unión Europea y el Instituto Federal de Acceso y Protección de Datos respecto del motor de búsqueda gestionado por Google y la protección de datos personales", *Boletín Mexicano de Derecho Comparado*, núm. 145, enero-abril de 2016, p. 6.

[39] Sentencia del TJUE (Gran Sala) del 13 de mayo de 2014, apartado 46.

[40] Rallo Lombarte, A., *El derecho al olvido en internet. Google versus España*, Madrid, Centro de Estudios Políticos y Constitucionales, 2014, p. 274.

[41] Miguel Asensio, P., "Aspectos internacionales de la protección de datos: las sentencias *Schrems* y *Weltimmo* del Tribunal de Justicia", *La Ley Unión Europea*, núm. 31, noviembre de 2015, pp. 1-10.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

de datos personales propias para sancionar las conductas inadecuadas cometidas por la empresa con domicilio en Eslovaquia, siendo éste un caso bastante similar al estudiado en el presente trabajo.

El TJUE resuelve esta cuestión en los apartados 24 a 41 de su sentencia, partiendo en primer lugar de la interpretación del ámbito territorial de aplicación de la Directiva Europea de Protección de datos establecido en la sentencia del caso *Google*. Así, vuelve a interpretar de manera flexible el término establecimiento, considerando que

> ...es preciso considerar, habida cuenta del objetivo de garantizar una protección eficaz y completa del derecho a la intimidad y evitar que eluda la normativa aplicable que persigue la Directiva, que la presencia de un único representante puede bastar, en determinadas circunstancias, para constituir una instalación estable si actúa con un grado de estabilidad suficiente a través de los medios necesarios para la prestación se los servicios concretos de los que se trate en el Estado miembro en cuestión.[42]

Una vez puntualizada dicha interpretación de la normativa, el TJUE analiza el supuesto fáctico. Concretamente, el Tribunal considera que "la actividad ejercida por Weltimmo consiste, como mínimo, en la gestión de uno o varios sitios de Internet de anuncios de inmuebles situados en Hungría, que están redactados en Húngaro y que pasan a ser de pago transcurridos el primer mes. Por lo tanto, procede señalar que dicha sociedad ejerce una actividad real y efectiva en Hungría".[43] Añade el Tribunal que la sociedad contaba con un representante en Hungría que se menciona en el registro de sociedades de Eslovaquia. Como se puede observar, la mera existencia de un representante de una sociedad que presta servicios en Internet es suficiente para considerar que existe un establecimiento en otro Estado miembro.

En vista de la anterior argumentación, el Tribunal concluye permitiendo la aplicación del derecho de protección de datos nacional de un Estado miembro sobre una empresa de prestación de servicios en Internet, con sede principal en otro Estado miembro. En efecto:

[42] Sentencia del TJUE (Gran Sala) del 1 de octubre de 2016, apartado 30.
[43] *Ibidem*, apartado 32.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

> ...el artículo 4, apartado 1, letra a) de la Directiva 95/46 debe interpretarse en el sentido de que permite aplicar la legislación relativa a la protección de datos personales de un Estado miembro distinto de aquel en el que está registrado el responsable del tratamiento de esos datos, siempre que esta ejerza, mediante una instalación estable en el territorio de dicho estado miembro, una actividad efectiva y real, aun mínima, en cuyo marco se realice el referido tratamiento.[44]

Ahora sí, es momento de poder responder a la primera cuestión planteada. En el caso en cuestión, y en vista de los argumentos jurisprudenciales emitidos por el TJUE, ampliando de manera muy flexible el ámbito de aplicación territorial de la Directiva Comunitaria, y por ello, extendiendo de facto el poder de las diferentes normativas nacionales, considerando, que Ashley Madison ofrece un servicio en España; realizando indudablemente un tratamiento de datos personales de personas con residencia en España, y siendo razonable pensar que al menos dispondrá de algún representante legal que gestione sus intereses en el citado país, se debe considerar que *Ashley Madison* debe responder por infringir el principio de seguridad de los datos, al no adoptar todas las medidas necesarias para salvaguardar los mismos, y podrá ser demandado en vía civil por los afectados en las filtraciones de sus datos personales. En el mismo sentido, aunque en referencia a las redes sociales en general, se manifiesta Aparicio Vaquero al considerar que

> ...es difícil pensar en supuestos den los que no resulte de aplicación la legislación española de protección de datos a proveedores de SRS cuando estos prestan sus servicios a usuarios que físicamente se encuentren en territorio español, con todo lo que ello conlleva en orden al cumplimiento de la misma, las responsabilidades que se deriven y la sujeción a la autoridad de control nacional.[45]

[44] Sentencia del TJUE (Gran Sala) del 1 de octubre de 2016, apartado 41.

[45] Aparicio Vaquero, J., "Cuestiones de derecho aplicable y responsabilidad de los prestadores se servicios de red social y de sus usuarios", en Aparicio Vaquero, Juan Pablo y Batuecas Caletrío, Alfredo (coords.), *En torno a la privacidad y la protección de datos en la sociedad de información*, Granada, Comares, 2015, p. 206.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

3. *Análisis de la competencia judicial internacional*

Es el momento de responder a la segunda pregunta planteada anteriormente, ¿puede un usuario de esta red social con domicilio en España, acudir a los tribunales españoles para pedir esta indemnización?

Para poder responder a esta pregunta se debe hacer mención en primer lugar al posible carácter patrimonial existente en la relación entre la red social y sus usuarios. En efecto, existe un enorme debate doctrinal en relación con la gratuidad u onerosidad del contrato que surge entre una red social y su usuario, debate que puede ser entendible en redes sociales totalmente gratuitas para el usuario, aunque también en estos casos:

> ...cabría incluso cuestionar que el contrato de suscripción o afiliación a una red social en cuya virtud se presta el servicio sea un contrato gratuito pues, en realidad, hay prestaciones por ambas partes de claro contenido patrimonial, en relación sinalagmática: la de servicio, de un lado, y, por lo menos la cesión de datos que lo permite y que, en actos de ejecución posteriores, supone la propia actividad en la red.[46] Realmente, en el caso objeto de análisis, el debate anterior tiene una respuesta más sencilla, ya que, al tratarse *Ashley Madison* de una red social de pago, el claro contenido patrimonial de la relación contractual existente subyace en toda la relación.

La segunda cuestión que se debe aclarar es la relativa a la posible relación de consumo que existe entre los usuarios de esta red social y la misma. Como es sabido, la protección de los consumidores se encuentra llena de salvaguardas muy importantes, y que, en materia de competencia judicial, alteran el régimen aplicable. Para determinar si existe relación de consumo se debe acudir al Real Decreto Legislativo 1/2007, del 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,[47] LGDCU, concretamente a su artículo 3o. que establece que son consumidores o usuarios las personas físicas que actúen con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión.

---

[46] *Ibidem*, p. 208.

[47] Real Decreto Legislativo 1/2007, del 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, *BOE* núm. 287, del 30 de noviembre de 2007.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

El concepto de empresario aparece en el artículo 4o. como toda persona física o jurídica, ya sea privada o pública, que actúe directamente o a través de otra persona en su nombre o siguiendo sus instrucciones con un propósito relacionado con su actividad comercial, empresarial, oficio o profesión.

En función de lo establecido en la normativa, parece lógico concluir que en este caso en concreto sí existe una relación de consumo entre los usuarios de la red social y *Ashley Madison*, quien actúa como un empresario ofreciendo por medio de su red virtual el acceso a contactos al consumidor, que recíprocamente abona cantidades periódicas para permanecer en la citada red social. Además son contratos celebrados a distancia,[48] donde el consumidor no puede negociar ninguna de las cláusulas del mismo, son contratos de adhesión, es decir, o se acepta todo su contenido o no se puede acceder a la red social.

Es el momento de rescatar el contenido de la cláusula decimonovena de las condiciones de términos y servicios de *Ashley Madison*, donde se puede encontrar una sumisión obligatoria a resolver todas las controversias jurídicas que se planteen contra la red social mediante un proceso arbitral en Chipre, que además se desarrollará conforme a la Ley de Arbitraje de Chipre. En función del contenido de dicha cláusula aceptada por los usuarios, la respuesta a la pregunta planteada llevaría a afirmar la imposibilidad de poder reclamar en vía civil ante los tribunales españoles la inadecuada actuación de la red social; no obstante, esto no es del todo cierto. En efecto, la Directiva 93/13/CEE del Consejo, del 5 de abril de 1993, tratándose de las cláusulas abusivas en los contratos celebrados con consumidores,[49] establece en su artículo 3o. que las cláusulas contractuales que no se hayan negociado individualmente se considerarán abusivas[50] si, pese a las exigencias de la buena fe, causan en detrimento del consu-

[48] Los contratos celebrados a distancia se encuentran regulados en los artículos 23 a 29 de la LSSI, donde se establece que se regirán por lo dispuesto en dichos preceptos, por los códigos civil y de comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios, y de ordenación de la actividad comercial.

[49] Directiva 93/13/CEE del Consejo, del 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores, *DOUE* núm. 95, del 21 de abril de 1993.

[50] Martínez Espín, P., "¿Qué hay de nuevo en materia de cláusulas abusivas?", *Revista CESCO de Derecho de Consumo*, núm. 9, 2014, pp. 76-84.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

midor un desequilibrio importante entre los derechos y obligaciones de las partes que se derivan del contrato. Además, se considerará que una cláusula no se ha negociado individualmente cuando haya sido redactada previamente y el consumidor no haya podido influir sobre su contenido, en particular en el caso de los contratos de adhesión.

Esta Directiva hace mención a la redacción individual de las condiciones en los denominados contratos de adhesión, es decir, los contratos típicos de las redes sociales donde el usuario sólo puede aceptar o rechazar todas las condiciones en su conjunto. En virtud de la misma deben considerarse abusivas que restrinjan los derechos de los consumidores, y realmente una cláusula de sumisión expresa de arbitraje[51] ante un tribunal arbitral en Chipre sí puede considerase una restricción de los derechos de los consumidores, ya que difícilmente podrán acudir a dirimir las controversias a dichos países. Asimismo, la normativa española de protección de los consumidores establece en su artículo 90, prohibiciones similares en relación con los pactos de competencia y derecho aplicable impuestos individualmente por el empresario al consumidor.[52] Por tanto, la cláusula de sumisión a un proceso arbitral en Chipre debe considerarse abusiva, de tal suerte que la solución a la cuestión planteada vendrá determinada por el régimen de competencia judicial internacional existente tanto en las normativas internacionales como en las nacionales.

El Reglamento 1215/2012 del Parlamento Europeo y del Consejo del 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercan-

[51] Sobre la validez de las cláusulas de sumisión expresa a arbitraje en los contratos de adhesión, véase Gimeno Sendra, V., "La validez de los convenios arbitrales de adhesión en la doctrina del Tribunal Constitucional", *Diario La Ley*, núm. 7168, mayo de 2009, pp. 1-6; "Los convenios arbitrales de adhesión y su impugnación jurisdiccional", *Diario La Ley*, núm. 8097, junio de 2013, pp. 1-9.

[52] Artículo 90, LGDCU: "Son, asimismo, abusivas las cláusulas que establezcan: 1. La sumisión a arbitrajes distintos del arbitraje de consumo, salvo que se trate de órganos de arbitraje institucionales creados por normas legales para un sector o un supuesto específico. 2. La previsión de pactos de sumisión expresa a Juez o Tribunal distinto del que corresponda al domicilio del consumidor y usuario, al lugar del cumplimiento de la obligación o aquél en que se encuentre el bien si éste fuera inmueble. 3. La sumisión del contrato a un Derecho extranjero con respecto al lugar donde el consumidor y usuario emita su declaración negocial o donde el empresario desarrolle la actividad dirigida a la promoción de contratos de igual o similar naturaleza".

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

til, establece en sus artículos 17 a 19 un sistema de competencia especial en el caso de contratos celebrados con consumidores.[53] Concretamente, el artículo 18 estipula que el consumidor podrá interponer su acción judicial ante los órganos jurisdiccionales del Estado miembro en que esté domiciliada dicha parte o, con independencia del domicilio de la otra parte, ante el órgano jurisdiccional del lugar en que esté domiciliado el consumidor. Además, este régimen competencial deja sin aplicación la sumisión al proceso arbitral en Chipre que establecía el contrato de términos y servicios, ya que "estas cláusulas no podrán ser invocadas válidamente por el prestador de servicios *online* para desplazar la competencia reconocida por el sistema Bruselas a los tribunales de un Estado miembro a favor de un tercer Estado".[54]

Por tanto, y en virtud de lo expuesto anteriormente, la respuesta a la cuestión debe ser afirmativa. Si algún usuario que resida en España ha sufrido un inadecuado tratamiento de datos personales por parte de *Ashley Madison*, puede interponer una acción en vía civil ante los tribunales españoles, ya que la legislación ampara sus derechos como consumidor de esta red social.

IV. Conclusiones

Tras la exposición de la actividad jurídica de las redes sociales, y sentar las bases de la exigencia de una responsabilidad civil derivada de un incorrecto tratamiento de datos personales, es menester resaltar ciertas conclusiones fundamentales.

1. Las redes sociales son proveedoras de servicios *online* que, a través de Internet, ofrecen a usuarios de todo el mundo, la posibilidad de interaccionar con otros, ofreciendo en cada red social en cuestión, funcionalidades distintas. Como ha quedado demostrado, no cabe duda de que las redes sociales tratan datos personales de los usuarios, datos que en ocasiones pueden ser simples edades o indicación del sexo, pero que en otras pueden

[53] Véase la sentencia del TJUE (Gran Sala) del 7 de diciembre de 2010, en el asunto *Pammer*, donde se establecieron los requisitos que una empresa que presta servicios en Internet, debe reunir para considerar el contrato con sus usuarios como de consumo.

[54] Cordero Álvarez, C., *Litigios internacionales sobre difamación y derechos de la personalidad*, Madrid, Dykinson, 2015, p. 127.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

ser datos más sensibles, como los relativos a la salud o a la actividad sexual. Del tratamiento de datos personales que efectúan, éstas obtienen un importante beneficio económico, y, como consecuencia de ello, se les debe exigir en su actuación el respeto al régimen jurídico legal.

2. La comunidad europea lleva desde antiguo preocupándose por la privacidad y la protección de datos personales de los ciudadanos. La Directiva 95/46 de protección de datos personales, como se ha expuesto, establece una serie de principios, que han sido objeto de transposición en las normas de protección de datos personales, principios como el de protección de datos personales, que obligan a los prestadores de servicios y responsables del tratamiento de datos personales, a adoptar todas las medidas necesarias para garantizar un adecuado uso de los datos de sus usuarios. Pero, como ha quedado de manifiesto, las normas previstas en 1995 han quedado obsoletas, y a finales de 2016 se aprobó el nuevo Reglamento de protección de datos personales adaptado a los diferentes fallos judiciales que el Tribunal de Justicia de la Unión ha emitido en relación con la interpretación del derecho fundamental a la protección de datos personales.

3. A pesar de existir una serie de normas que en principio son aplicables a todas las redes sociales que dirigen sus servicios a Estados de la unión, no a todas se les aplicará con la misma intensidad. En efecto, en el presente trabajo se ha expuesto el caso de la red social de *Ashley Madison*, en el sentido del análisis de la responsabilidad de la misma, en relación con un inadecuado tratamiento de datos personales. En el análisis se llegó a la conclusión de que le resultaría de aplicación la normativa comunitaria y española, y que se podría interponer una acción civil por parte de los perjudicados ante los tribunales españoles. No obstante, este análisis no es extrapolable al resto de redes sociales *per se*, sino que si se piensa, por ejemplo, en el caso de Facebook, el análisis necesariamente debe ser distinto, ya que no es una empresa que se encuentre domiciliada en ningún Estado miembro.

4. Los usuarios de una red social, en muchos casos, pueden ser considerados como consumidores de las mismas. Se ha hecho mención en el presente trabajo a los denominados contratos de adhesión, es decir, aquellos contratos que son redactados por parte del empresario y que no permiten ningún ápice de negociación por parte de los usuarios. Estos contratos son los típicos de las redes sociales, ya que el usuario simplemente se puede limitar a aceptarlos o rechazarlos a través de un *click*, y, nor-

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

malmente, en el articulado de los mismos siempre suelen existir diferentes cláusulas abusivas, tanto de elección de fueros como de ley aplicable, y, ¿cómo no?, de exención de responsabilidad a las redes sociales. Es necesario comentar que en el presente trabajo se ha analizado la responsabilidad contractual de las redes sociales, aunque existe otro tipo de responsabilidad que posee un régimen jurídico diferente al desarrollado, como es la posible responsabilidad extracontractual de una red social; por ejemplo, por permitir que se publiquen mensajes difamatorios a una persona.

V. Bibliografía

Aberasturi Gorriño, U., "El derecho a la indemnización del artículo 19 de la Ley Orgánica de Protección de Datos de Carácter Personal", *Revista Aragonesa de Administración Pública*, núm. 41-42, 2013.

Adsuar Prieto, Y., "La elección de ser olvidado en la red: derecho o privilegio", *Actualidad Jurídica Aranzadi,* Pamplona, núm. 864, 2013.

Aparacio Vaquero, J., "Cuestiones de derecho aplicable y responsabilidad de los prestadores se servicios de red social y de sus usuarios", en Aparicio Vaquero, Juan Pablo y Batuecas Caletrío, Alfredo (coords.), *En torno a la privacidad y la protección de datos en la sociedad de información*, Granada, Comares, 2015.

Bartolini, C. y Siry, L., "The Right to be Forgotten in the Light of the Consent of the Data Subject", *Computer Law and Security Review*, núm. 32, 2016.

Batuecas Caletrío, A., "El control de los padres sobre el uso que sus hijos hacen de las redes sociales", en Aparicio Vaquero, Juan Pablo y Batuecas Caletrío, Alfredo (coords.), *En torno a la privacidad y la protección de datos en la sociedad de información*, Granada, Comares, 2015.

Cebrián Herreros, M., "La web 2.0 como red social de comunicación e información", *Estudios sobre el Mensaje Periodístico*, vol. 14, 2008.

Cordero Álvarez, C., *Litigios Internacionales sobre difamación y derechos de la personalidad*, Madrid, Dykinson, 2015.

Escribano Tortajada, P., "Algunas cuestiones sobre la problemática jurídica sobre el derecho al honor, a la intimidad y a la propia imagen en Internet y las redes sociales", en Fayós Gardó, Antonio (coord.), *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Madrid, Dykinson, 2014.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

GIMENO SENDRA, V., "Los convenios arbitrales de adhesión y su impugnación jurisdiccional", *Diario La Ley*, núm. 8097, junio de 2013.

———, "La validez de los convenios arbitrales de adhesión en la doctrina del Tribunal Constitucional", *Diario La Ley*, núm. 7168, mayo de 2009.

HEREDERO CAMPO, M., "Web 2.0: afectación de derechos en los nuevos desarrollos de la web corporativa", *Cuadernos Red de Cátedras Telefónica*, núm. 6, mayo de 2012.

HERT, P. y PAPAKONSTANTINOU, V., "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?", *Computer Law and Security Review*, núm. 32, 2016.

LLANEZA, P., "Derechos fundamentales e Internet", *Telos. Cuadernos de Comunicación e Innovación*, octubre-diciembre de 2010.

MAQUEO RAMÍREZ, M., "Análisis comparativo de las resoluciones emitidas por el tribunal de justicia de la Unión Europea y el Instituto Federal de Acceso y Protección de Datos respecto del motor de búsqueda gestionado por Google y la protección de datos personales", *Boletín Mexicano de Derecho Comparado*, núm. 145, enero-abril de 2016.

MARTÍNEZ ESPÍN, P., "¿Qué hay de nuevo en materia de cláusulas abusivas?, *Revista CESCO de Derecho de Consumo*, núm. 9, 2014.

MARTÍNEZ LÓPEZ, F. *et al*., *Evolution of the Web*, Suiza, Springer, 2016.

MARTÍNEZ MARTÍNEZ, R., "El derecho fundamental a la protección de datos: perspectivas", *Revista de Internet, Derecho y Política*, núm. 5, 2007.

MARTÍNEZ OTERO, J., "El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google *vs*. AEPD y Mario Costeja", *Revista de Derecho Político*, núm. 93, mayo-agosto de 2015.

MIGUEL ASENSIO, P., "Aspectos internacional de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia", *La Ley Unión Europea*, núm. 31, noviembre de 2015.

———, *Derecho privado en Internet*, *estudios y comentarios legislativos*, Madrid, Aranzadi, 2015.

MUÑOZ MASSOUH, A., "Eliminación de datos personales en Internet: el reconocimiento del derecho al olvido", *Revista Chilena de Derecho y Tecnología*, vol. 4, núm. 2, 2015.

PALACIOS GONZÁLEZ, M., "El poder de autodeterminación de los datos personales en Internet", *Revista de Internet, Derecho y Política*, núm. 14, mayo de 2012.

DOI: http://dx.doi.org/10.22201/iij.24484873e.2017.150.11839

RALLO LOMBARTE, A., *El derecho al olvido en internet. Google versus España,* Madrid, Centro de Estudios Políticos y Constitucionales, 2014.

RUBÍ PUIG, A., "Derecho al honor *online* y responsabilidad civil de ISPs. El requisito del conocimiento efectivo en la SSTS, Sala Primera, del 9 de diciembre de 2009 y 18 de mayo de 2010", *InDret, Revista para el Análisis del Derecho*, núm. 4, 2010.

SANJURO REBOLLO, B., *Manual de Internet y redes sociales*, Madrid, Dykinson, 2015.

SCHINASI, J., "Practicing Privacy Online: Examining Data Protection Regulations Through Google's Global Expansion", *Columbia Journal of Transnational Law*, vol. 52, núm. 2, 2014.

SOLER PRESAS, A., "Am I in Facebook?", *InDret, Revista para el Análisis del Derecho,* núm. 3, julio de 2011.

Fecha de recepción: 08 de septiembre de 2016
Fecha de aceptación: 11 de mayo de 2017

Boletín Mexicano de Derecho Comparado, núm. 150, pp. 1259-1288