Perfiles de las Ciencias Sociales, Volumen 6, Número 11, julio-diciembre 2018, 154-198 pp.
Http://revistas.ujat.mx/index.php/perfiles, México, UJAT.
ISSN: 2007-9362

EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS EN EL DERECHO A LA PROTECCIÓN DE DATOS DESDE LA PERSPECTIVA DEL DERECHO INTERNACIONAL PRIVADO: REDES SOCIALES DE INTERNET Y *CLOUD COMPUTING*

THE IMPACT OF NEW TECHNOLOGIES ON THE RIGHT TO DATA PROTECTION FROM THE PERSPECTIVE OF PRIVATE INTERNATIONAL LAW: SOCIAL NETWORKS OF INTERNET AND CLOUD COMPUTING

Artículo Científico Recibido: *1 de febrero de 2018* ***Aceptado:*** *29 de mayo de 2018*

Alfonso Ortega Giménez[1]
alfonso.ortega@umh.es

RESUMEN: Son las 9:00 horas de un día cualquiera... en cualquier parte del mundo... tranquilamente en tu casa... te conectas a una red social de Internet cualquiera, ves que X se ha ido a pasar unos días fuera, que, Y está malo, que se va a organizar una fiesta en la discoteca R y te han invitado, que tus amigos han colgado varias fotos de vuestro último fin de semana de fiesta

[1] Doctor de Derecho Internacional Privado de la Universidad Miguel Hernández de Elche

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

Internet cuyo establecimiento se encuentra en un "tercer país" no comunitario. 4.3 Redes sociales de Internet cuyo establecimiento se encuentra en un "tercer país" no comunitario pero se utilizan medios situados en España. 5. *Cloud computing*, protección de datos, y relaciones privadas internacionales. 6. *Cloud computing* y responsabilidad contractual y no contractual por vulneración del derecho a la protección de datos personales: problemas de Derecho internacional privado. 7. *Cloud computing*, protección de datos, y resolución de controversias. *7.1 El sistema español de competencia judicial internacional. 7.2 Foro de la sumisión de las partes. 7.2.1 Foro de la sumisión expresa. 7.2.2 Foro de la sumisión tácita. 7.2.3 Sumisión a tribunales extranjeros. 7.3 Foro del domicilio del demandado. 7.4 Foro especial en materia de obligaciones extracontractuales: el lugar donde se hubiere producido o pudiere producirse el hecho dañoso. 7.5 Foro especial en materia de obligaciones contractuales: el lugar en el que hubiere sido o debiere ser cumplida la obligación que sirviere de base a la demanda*. 8. Responsabilidad no contractual, *cloud computing*, y determinación de la ley aplicable. *8.1 Tratamientos de datos realizados en el marco de las actividades de un responsable del tratamiento establecido en el territorio de la Unión Europea. 8.2 Tratamientos de datos realizados en el marco de las actividades de un responsable del tratamiento establecido fuera del territorio de la Unión Europea.* 9. Responsabilidad contractual, *cloud computing*, y determinación de la ley aplicable: el Reglamento «Roma I». 10. Reflexiones finales.

1. Los posibles riesgos de las redes sociales de Internet, sus consecuencias jurídicas y el Derecho internacional privado.

Son las 9:00 horas de un día cualquiera... en cualquier parte del mundo... tranquilamente en tu casa... te conectas a una red social de Internet cualquiera, ves que X se ha ido a pasar unos días fuera, que Y está malo, que se va a organizar una

fiesta en la discoteca R y te han invitado, que tus amigos han colgado varias fotos de vuestro último fin de semana de fiesta… Y así un largo etcétera... Podemos tener una vida social más activa a través de la red, contar con 1.001 amigos, que todos se enteren de lo que te pasa o de lo que haces en cada momento, que todos vean que eres muy divertido y que estás a la última… Pero… ¡seamos claros!... esto va más allá de estas premisas, no somos conscientes de los peligros que nos supone, individualmente, el dar información personal... Hace años que luchamos por la protección de nuestros datos personales, y ahora los colgamos gratuitamente de la Red, a disposición de cualquiera... nos arriesgamos a que parte de nuestra intimidad quede a merced de los demás...

España, hoy día, es el segundo país europeo en participación en redes sociales de Internet, sólo por detrás de Reino Unido. Al menos 13.000.000 de españoles están conectados a través de *Twitter*, *Facebook*, *Tuenti,* o *MySpace*, por citar sólo las más conocidas. Son el 73.7% de los usuarios de Internet, según la auditora *Comscor*. Es de esas cosas para las que las estadísticas sólo vienen a confirmar algo que ya compruebas mirando a tu alrededor. El número de internautas españoles que están suscritos a una red social ha pasado en un año del 45% al 81%, según destaca el 2º Observatorio de Redes Sociales, elaborado por *The Coctel Analysis*.

Ahora bien, al utilizar las redes sociales de Internet son tres los momentos críticos para la protección de datos personales[2]: a) el primer momento crítico se encuentra en la *fase inicial de registro del usuario*, cuando este proporciona la información personal necesaria para poder operar en la red social. En este momento, los datos se pueden ver sometidos a varios riesgos: que el tipo de datos solicitados en el formulario de registro, aunque no obligatorios, sean excesivos, que el grado de publicidad del perfil de usuario sea demasiado elevado, que la finalidad de los datos no esté correctamente determinada, o la transferencia internacional de datos; b) el segundo momento considerado crítico para la protección de datos personales se sitúa en la *fase intermedia*, es decir, en la que el usuario desarrolla su actividad en la plataforma y utiliza los servicios y herramientas que ésta le ofrece. En este momento los aspectos que pueden poner en riesgo la seguridad y protección de datos personales de los usuarios son: la publicación excesiva de información personal (propia o de terceros), la instalación y uso de *cookies* sin conocimiento del usuario. El uso de *web beacons*, esto es, de imágenes electrónicas que permiten al sitio web conocer quién y qué contenido *online* ha sido visitado, que el perfil de usuario sea indexado

[2] *Vid.*, en sentido amplio, «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 (INTECO) y la Agencia Española de Protección de Datos (AEPD), (disponible en www.inteco.es y/o www.agpd.es); Dictamen 5/2009 del Grupo de Trabajo, creado por el artículo 29 de la Directiva 95/46/CE, sobre las redes sociales en línea (WP 163 -01189/09/ES), adoptado el 12 de junio de 2009; y, Resolución sobre Protección de la privacidad en los servicios de redes sociales, adoptada por la 30º Conferencia Internacional de Autoridades de Protección de Datos y privacidad, en Estrasburgo, 15-17 de octubre de 2008.

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

automáticamente por los buscadores de Internet, la recepción de publicidad hipercontextualizada, la recepción de comunicaciones comerciales electrónicas no solicitadas (*spam*), o la suplantación de identidad de los usuarios de la red social; y, c) el tercer momento crítico para la protección de datos personales se sitúa en la *fase en la que el usuario pretende darse de baja del servicio*. En este momento, deben tenerse en cuenta los siguientes aspectos que pueden poner en riesgo la seguridad y protección de datos personales de los usuarios: la imposibilidad de realizar la baja efectiva del servicio, la conservación de datos y el cumplimiento de los principios de calidad de los datos, consentimiento e información.

Las ya frecuentes críticas hacia las redes sociales de Internet se centran, al margen de su necesidad / utilidad, en su francamente mejorable funcionalidad, en su masiva proliferación, y, sobre todo, en su *amenaza a la intimidad*, que las puede convertir en una gran molestia. La crítica más extendida afecta a cómo estos servicios recopilan información personal y cómo la utilizan. Se exige un gran número de datos que quedan en manos extrañas y, en muchos casos, se debe aceptar unas condiciones que dejan al usuario totalmente expuesto e indefenso. Ahora bien, sin duda, son los usuarios de la Red, en general, y de las herramientas de software social, en particular, los que han de saber administrar muy bien la información que revelan sobre sí mismos (imágenes, datos de contacto, cuentas de correo electrónico, identidad en servicios de mensajería instantánea, preferencias personales, orientación sexual, ideología, etc.), porque la vida privada y la intimidad, cuando uno las hace públicas, pasan del espacio personal al social, y desde allí al mercado[3].

Nos encontramos ante una nueva situación tecnológica, social, económica y jurídica, que ha sido denominada comúnmente como Sociedad de la Información[4], que abre múltiples posibilidades, propicia el debate, trae consigo un importante incremento de los litigios transfronterizos[5], y va unida a importantes cambios en las conductas de los operadores jurídicos[6] con el fin de «buscar el material legislativo

[3] *Vid.*, en particular, FERNÁNDEZ BURGUEÑO, Pablo, «El peligro de las redes sociales y sus principales consecuencias jurídicas», en *Revista Economist & Jurist*, nº 131, Año XVII - Junio 2009, pp. 54-58; y, MONSORIU FLOR, Mar, *Manual de Redes Sociales en Internet*. Creaciones Copyright, Madrid, 2008.

[4] Podemos identificar la *Sociedad de la Información* como el conjunto de transformaciones sociales y económicas producidas como consecuencia del desarrollo exponencial y convergente de redes y servicios de telecomunicaciones, medios de comunicación y tecnologías de la información. Se trata de conseguir que las nuevas tecnologías se conviertan en herramientas para la creación de una sociedad nueva. *Vid.* CAMPUZANO, Herminia, *Vida privada y datos personales.* Madrid, Tecnos, 2000, pág. 20.

[5] Como bien señala PALAO MORENO, «la irrupción en nuestra sociedad de las denominadas Tecnologías de la Información y de la Comunicación, ha traído consigo un importante incremento de los litigios transfronterizos [...] ha fomentado y provocado un notable aumento en las relaciones internacionales de carácter privado y, por lo tanto, de los supuestos en los que pueden surgir controversias con ese carácter». *Vid.* PALAO MORENO, Guillermo, «Competencia judicial internacional en supuestos de responsabilidad civil en Internet», en PLAZA PENADÉS, Javier, *Cuestiones actuales de derecho y Tecnologías de la Información y Comunicación (TICs)*. Editorial Aranzadi, Cizur Menor (Navarra), 2006, pp. 275-276.

[6] En palabras de VAN OVERSTRAETEN, Internet es «un sueño para sus usuarios y una pesadilla para los prácticos del Derecho», *Vid.* VAN OVERSTRAETEN, T., «Droit aplicable et jurisdiction compétente sur Internet», en *IBLJ*, 1998, pp. 373-397.

adecuado para hacer frente a los cambios que comportan las nuevas formas de comunicación y de transmisión de datos»[7]. Sin duda, hablar de la Sociedad de la Información y de las redes sociales de Internet es hablar de *relaciones privadas internacionales*, esto es, es hablar de Derecho internacional privado. Gracias a Internet «resulta sencillo navegar entre páginas, y, por ello, entre países y jurisdicciones de tal forma que con sólo hacer *click* uno abandona una página ubicada en territorio español para pasar a ver otra página almacenada en Estados Unidos»[8]. Es más, «la mayor parte de las operaciones realizadas en Internet son *internacionales*: en tales situaciones hay presente uno o múltiples *elementos extranjeros* y/o producen *efectos* en varios países o incluso en todo el mundo»[9].

Los posibles problemas de vulneración de datos de carácter personal derivados de la utilización de redes sociales de Internet deben ser resueltos, a partir de las normas de Derecho internacional privado español relativas a la responsabilidad civil contractual o extracontractual. Debemos justificar que el Derecho internacional privado sea la rama del ordenamiento jurídico español que resuelva los litigios derivados de la vulneración del derecho a la protección de datos de carácter personal, proponiendo soluciones tales como la unificación de las normas estatales de Derecho internacional privado para evitar la relatividad de las soluciones y/o la utilización de criterios subjetivos, flexibles y particulares, que permitan la vinculación del supuesto concreto con un país determinado. Así, por ejemplo, supongamos que la empresa WWW, establecida en Portugal, es la responsable de la *red social de Internet FATBOOK*. Los usuarios de dicha red social, a la hora de registrarse, deben cumplimentar un extenso formulario donde se solicita, p. ej., información relativa a su ideología política, orientación sexual o preferencia religiosa; estos datos son, a su vez, sin el consentimiento del usuario, cedidos a empresas norteamericanas que cruzan los datos con bases de datos de diferentes procedencias y que luego venden a las empresas para que puedan elaborar perfiles de usuarios... Teniendo en cuenta que las redes sociales de Internet son de ámbito global pero su establecimiento, jurídicamente hablando, se limita a pocos países concretos... Ante la vulneración del derecho a la protección de datos personales... ¿En caso de litigio, ¿cuáles serían los *Tribunales competentes* para conocer de la demanda interpuesta, p. ej., por un usuario domiciliado en España?...y, sobre todo, ¿cuál sería la *ley aplicable*?...[10].

---

[7] ***Vid.*** **CAMPUZANO, Herminia, *Vida privada y datos personales*. Madrid, Tecnos, 2000, pág. 19.**
[8] ***Vid.*** **LLANEZA GONZÁLEZ, Paloma, *Aplicación práctica de la LSSI-CE*. Bosch, Barcelona, 2003, pág. 161.**
[9] ***Vid.*** **CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Derecho internacional privado. Vol. II*, 8ª edición, Comares, Granada, 2007, p. 652; y, CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Conflictos de leyes y conflictos de jurisdicción en Internet*, Colex, Madrid, 2001, pág. 13.**
[10] ***Vid.*****, en sentido amplio, ORTEGA GIMÉNEZ, Alfonso, "Derecho Internacional Privado, Protección de Datos y Redes Sociales de Internet" (Capítulo XI), en RALLO LOMBARTE, Artemi y MARTINEZ MARÍINEZ, Ricard (Coords.), *Derecho y Redes Sociales*, Civitas Thomson Reuters, Cizur Menor (Navarra), 2010, pp. 299-318.**

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT.
ISSN: 2007-9362

2. Redes sociales de Internet y responsabilidad no contractual por vulneración del derecho a la protección de datos personales: problemas de Derecho internacional privado.

En el ámbito del Derecho internacional privado, los problemas para el derecho a la protección de datos personales el uso de las redes sociales de Internet que plantean están relacionados con la determinación del órgano jurisdiccional competente para conocer de un determinado litigio, así como de la determinación de la ley aplicable para resolver el conflicto planteado. La delimitación de ambos aspectos será de vital importancia ya que, como es bien sabido, cada sistema jurídico tiene establecido un sistema de normas de conflicto, en virtud del cuál se determina quién será el órgano jurisdiccional competente y cual será la ley aplicable para resolver la controversia que se plantee[11].

El daño derivado de la intromisión ilegítima en el derecho a la protección de datos, manifestado en el uso indebido o ilegítimo de sus datos personales, consecuencia de la utilización de redes sociales de Internet, sobre la base de la existencia o no de una vinculación jurídica entre el causante del daño y el afectado, puede dar lugar a la exigencia de responsabilidad civil contractual (= cuando entre el autor y la víctima hubiere existido una previa relación contractual y se hubiere producido un incumplimiento de lo pactado), o extracontractual (= exigencia de una indemnización por los daños y perjuicios ocasionados).

La vulneración del derecho a la protección de datos por el uso de redes sociales de Internet traerá como resultado la exigencia de responsabilidad civil objetiva[12], derivándose el derecho a indemnización del afectado por el tratamiento de sus datos, tal y como señala el artículo 19.1 de la LOPD[13]: «los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley [Orgánica de Protección de Datos de carácter Personal] por el responsable o el encargado del

[11] *Vid.*, sobre la materia, en particular, BING, J., «*Data protection, jurisdiction and the choice of law* », en *Privacy Law & Policy. Reporter*, volume 6, 1999, pp. 92-98; y, REIDENBERG, Joel R., «Technology and Internet Jurisdiction», en *UNIVERSITY OF PENNSYLVANIA LAW REVIEW*, Vol. 153, pp. 1951-1974.

[12] Es más, se debe fortalecer el uso de la responsabilidad civil extracontractual objetiva como mecanismo regulatorio para garantizar los derechos fundamentales en las aplicaciones en la Sociedad de la Información y Conocimiento, Internet y redes sociales digitales, Vid., en particular, Memorandum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, hecho en Montevideo, el 28 de julio de 2009.

[13] Este precepto viene a coger la responsabilidad civil extracontractual o aquiliana de los artículos 1902 y 1903 de nuestro Código Civil. Este tipo de responsabilidad es de aplicación cuando el daño se haya producido por los ficheros de titularidad privada, en aquellos supuestos en los que no existe una relación entre los interesados, perjudicado y responsable, sino que se trata de dos personas entre las que nace el derecho y obligación de indemnizar como consecuencia de actos del responsable en los que no ha intervenido la voluntad del perjudicado.

tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados».

La exigencia de una indemnización por daños y perjuicios derivada del tratamiento ilícito de datos, gracias al uso de las redes sociales de Internet, no excluye la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación frente al responsable del fichero de datos. Los afectados o interesados por el tratamiento de sus datos, como titulares del derecho fundamental a la protección de datos, se encuentran facultados para conocer y acceder a las informaciones que les pudieran afectar, archivadas en bancos de datos, y controlar su calidad, permitiendo que puedan ser corregidos o cancelen los datos inexactos o indebidamente procesados, y la disposición sobre su transmisión.

3. Redes sociales de Internet, protección de datos, y competencia judicial internacional.

3.1 El sistema español de competencia judicial internacional.

La determinación de la competencia judicial internacional en materia de reclamaciones por vulneración del derecho a la protección de datos, derivadas de la utilización de las redes sociales de Internet, nos lleva a un laberinto normativo de intrínseca complejidad, ya que se acumulan fuentes de origen diverso: institucional o comunitario, convencional y autónomo; así, debemos acudir a los siguientes instrumentos normativos: al *limitado*[14] Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Bruselas, el 27 de septiembre de 1968 (en adelante, CB); a su *gemelo*[15], el Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Lugano, el 16 de septiembre de 1988 (en adelante, CL)[16] – aunque, no olvidemos que, por una Decisión de 15 de octubre de 2007[17], la Comunidad Europea ha aprobado la firma del Convenio relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y

[14] El CB se aplica, en la actualidad, únicamente con relación a los territorios franceses de ultramar y a las Antillas holandesas.
[15] El CB y el CL poseen un contenido normativo prácticamente idéntico, siendo sus únicas diferencias las referidas al contrato individual de trabajo y a los contratos de arrendamiento de corta duración.
[16] *BOE* núm. 243, de 10 de octubre de 1979.
[17] *DOUE* L 339, de 21 de diciembre de 2007. Una vez aprobado por las partes (UE, Suiza, Noruega e Islandia) derogará al actual Convenio de Lugano 1988 y, por fin, el llamado *Espacio Judicial Europeo* (con unas mismas reglas de jurisdicción y un sistema simplificado de ejecución de sentencias) se extenderá a 30 Estados.

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

mercantil, que sustituirá al Convenio de Lugano de 16 de septiembre de 1988–; al Reglamento (UE) núm. 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil —Reglamento «Bruselas I bis»—[18]; o, a la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante, LOPJ)[19]. La aplicación de un instrumento jurídico u otro dependerá del domicilio del demandado.

Centrándonos en la materia que nos ocupa, lo habitual será que nos encontremos ante una *reclamación por daños y perjuicios por vulneración del derecho a la protección de datos en el ámbito de las redes sociales de Internet*, en aplicación del RB, del CB/CL, los criterios atributivos de competencia son los siguientes: a) el foro del domicilio del demandado, esto es, los tribunales del país donde esté domiciliado el *presunto vulnerador-demandado* conocerá de todas las pretensiones que se deduzcan contra él, independientemente del país o países en los que se haya producido el hecho dañoso; b) el foro de la sumisión, expresa o tácita, que nos permite concentrar los litigios a los que las partes se refieran, bajo el conocimiento de los tribunales de un solo país; y, c) el foro del lugar del hecho dañoso, que atribuye competencia a los tribunales del «lugar donde se hubiere producido o pudiere producirse el hecho dañoso» del que nace la responsabilidad extracontractual, pudiendo considerarse como *país donde ocurre el hecho dañoso* tanto el país donde ocurre el hecho causal como el país donde se verifica el resultado lesivo, esto es, el país donde radica el fichero de datos.

Ahora bien, esto no tiene por qué ser siempre así, ya que, por ejemplo, si la actividad consiste en la recogida ilícita de datos en España para su ulterior almacenaje informático en un fichero sito en Lisboa, el lugar del daño es tanto España como Portugal. Y, en otras ocasiones, el daño puede ser consecuencia de la vulneración de un contrato *interpartes*, en cuyo caso se concede competencia a los Tribunales del país en el que se incumplió la obligación contractual, por lo que, siguiendo con nuestro ejemplo, si según el contrato, los datos debían tratarse en Portugal y allí son objeto de tratamiento ilegal, los Tribunales *lusos* son competentes, sin

[18] ***DOUE*** **L 351/1 de 20/12/2012. Modificado por el Reglamento (UE) núm. 542/2014 del Parlamento y del Consejo, de 15 de mayo de 2014, por el que se modifica el Reglamento (UE) núm. 1215/2012 en lo relativo a las normas que deben aplicarse por lo que respecta al Tribunal Unificado de Patentes y al Tribunal de Justicia del Benelux (*DOUE* L 163 de 29/05/2014).**

[19] ***BOE*** **núm. 157, de 2 de julio de 1985. Modificada por la Ley Orgánica 7/2015, de 21 de julio, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. *BOE núm.* 174, de 22 de julio de 2015.**

perjuicio de la competencia de los tribunales del país del domicilio del demandado o de los tribunales pactados, expresa o tácitamente.

En definitiva, los foros de competencia operativos en materia de reclamación por daños y perjuicios por vulneración del derecho a la protección de datos en el ámbito de las redes sociales de Internet serían los siguientes: los *Tribunales elegidos por las partes en virtud de sumisión expresa o tácita*, el *domicilio del demandado* y el *lugar donde se hubiere producido o pudiere producirse el hecho dañoso*. Veamos cada uno de ellos:

3.2 Foro de la sumisión de las partes.

Este fuero de atribución de competencia (= sumisión expresa o tácita de las partes a favor de los Tribunales de un determinado Estado) viene contemplado en los instrumentos internacionales de atribución de competencia judicial internacional antes mencionados, y no introduce ningún cambio sustancial respecto a los criterios aplicables al resto de litigios transfronterizos. Por su parte, la LOPJ afirma que los tribunales españoles serán competentes «cuando las partes se hayan sometido expresa o tácitamente a los Juzgados o Tribunales españoles». El *acuerdo de sumisión* es un pacto entre las partes de una relación jurídica en cuya virtud éstas determinan el órgano jurisdiccional competente para conocer de los litigios que eventualmente pudieran surgir entre las partes. Tal sumisión puede realizarse mediante acuerdo *expreso* o mediante ciertas prácticas que denotan la voluntad de las partes de someterse a un órgano jurisdiccional: es la sumisión *tácita*.

Para que el acuerdo de *sumisión expresa* sea válido es necesario, fundamentalmente, que: a) se designen claramente los tribunales a los que se someten las partes; y, b) el acuerdo de sumisión expresa puede realizarse en cualquier momento, antes o después de la conclusión de un contrato o negocio internacional.

Por su parte, se entiende que las partes se someten tácitamente a los tribunales españoles cuando el demandante acude a tales tribunales interponiendo la demanda o formulando petición o solicitud que haya de presentarse ante el tribunal competente para conocer de la demanda, y cuando el demandado realiza, después de personado en el juicio tras la interposición de la demanda, cualquier gestión que no sea la de proponer en forma la declinatoria.

La validez de un acuerdo atributivo de competencia exige la prueba del acuerdo efectivo entre el demandante y el demandado: la sumisión debe hacerse

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

por escrito[20]; en este sentido, el RB, sensible con su adaptación al entorno de Internet, admite la formalización de la sumisión expresa por medios electrónicos; esto es, la elección *online* del tribunal competente, siempre que se encuentre en el territorio cubierto por la aplicación del RB; y, la elección del mismo podrá efectuarse bien mediante intercambio de *emails* o especificándose claramente en el contrato *interpartes*[21].

3.2.1 Foro de la sumisión expresa.

Constituye una prolongación de la autonomía de la voluntad al campo de la competencia judicial internacional, ya que permiten a las partes (a ambas o a una con el consentimiento de la otra) atribuir a los tribunales de un Estado la competencia para conocer de las controversias que puedan surgir del mismo. Asimismo, las partes se pueden someter tácitamente a un tribunal nacional que, en principio, no resultaría competente.

En este contexto, p. ej., la letra de las Condiciones de uso de **Tuenti** nos permite concluir que las partes (Tuenti y el usuario) « [...] con renuncia expresa a cualquier otro fuero que pudiera corresponderles, se someten a los *Juzgados y Tribunales de la ciudad de Madrid* [...]».

3.2.2 Foro de la sumisión tácita.

Se considera que existe *sumisión tácita*[22] la siguiente conducta procesal de las partes: cuando el demandante presenta una demanda ante el tribunal de un Estado miembro y la comparecencia del demandado ante ese tribunal no tiene por objeto impugnar su competencia judicial[23]. En tal caso, debe entenderse que las partes aceptan tácitamente someter el litigio a ese tribunal.

---

[20] *Vid.*, en general sobre la validez de las cláusulas atributivas de competencia en el comercio electrónico, DE MIGUEL ASENSIO, Pedro, *Derecho privado de Internet.* 3ª edición, Civitas, Madrid, 2002, pp. 448-455.

[21] *Vid.*, en relación con la elección *online* de los Tribunales competentes, CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Conflictos de leyes y conflictos de jurisdicción en Internet.* Colex, Madrid, 2001, pp. 43-46.

[22] El foro del acuerdo de sumisión tácita para la determinación del Tribunal internacionalmente competente permite el ahorro de costes procesales y (al igual que con la sumisión expresa) que las partes decidan ante qué tribunal quieren litigar. *Vid.*, en general, sobre el concepto, límites y requisitos de la sumisión tácita como foro de competencia judicial internacional, *Vid.* CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, «La sumisión tácita como foro de competencia judicial internacional y el artículo 24 del Reglamento 44/2001, de 22 de diciembre 2000», en CALVO CARAVACA, Alfonso-Luis y AREAL LUDEÑA, Santiago, *Cuestiones actuales del Derecho mercantil internacional*. Colex, Madrid, 2005, pp. 203-215.

[23] Tampoco operará la sumisión tácita cuando nos encontremos ante materias que son objeto de competencias exclusivas, *Vid*. CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Derecho internacional privado*. vol. I, Comares, Granada, 2003, pág. 130.

Los requisitos básicos para que se entienda que se ha producido sumisión tácita son los siguientes: por un lado, que, interpuesta la demanda por el demandante ante los órganos jurisdiccionales de un Estado concreto, el demandado efectúe después de personado en juicio cualquier gestión distinta de la de impugnar la competencia; y, por otro lado, que la controversia no verse sobre ninguna de las denominadas *competencias exclusivas*.

Para que no exista sumisión tácita, la impugnación de la competencia del tribunal ante el que se presenta la demanda debe realizarse de acuerdo con las normas de Derecho procesal del Estado del foro (esto es, el Derecho procesal del país cuyos tribunales conocen del asunto). En el caso de España, la impugnación debe realizarse en el momento y de acuerdo con los cauces procesales previstos en el artículo 64 de nuestra LEC.

3.2.3 Sumisión a tribunales extranjeros.

Y ¿qué ocurriría si el actor presentara su demanda ante los tribunales españoles, pero, existiera un acuerdo de sumisión entre las partes a favor de tribunales extranjeros?...¿deberían los tribunales españoles declararse incompetentes por la razón de que existe un pacto de sumisión a favor de los tribunales extranjeros? (= admitir o no la declinatoria internacional –*derogatio fori*– sobre la base de la *sumisión a tribunales extranjeros*). En otras palabras, ¿pueden derogar las partes las partes la competencia judicial internacional atribuida a los órganos jurisdiccionales españoles vía LOPJ, a través de un acuerdo en virtud del cual someten el litigio a tribunales extranjeros o a arbitraje privado internacional?

Si bien la LOPJ guarda silencio sobre esta cuestión, la jurisprudencia del TS ha sido la que ha arrojado algo de luz sobre la materia: en un primer momento, se mostró radicalmente contraria a admitir la *derogatio fori*; pero, en un segundo momento, aceptó y acepta una admisión matizada de la misma. Por tanto, hoy día, si el asunto ha sido sometido por las partes a tribunales extranjeros (o a arbitraje privado internacional), estos (o la Corte arbitral) y no los tribunales españoles, son los que deben conocer del litigio[24].

En nuestro caso, las principales redes sociales abogan por esta solución: así, de la lectura de las diferentes Condiciones de uso se deduce: en el caso de *Facebook*, que: « [...] Al visitar o hacer uso del Sitio o el Servicio, aceptas que las leyes del estado de Delaware, sin tener en cuenta los principios del conflicto de leyes, regularán estas condiciones de uso así como cualquier disputa que pudiera surgir entre tú y la

[24] *Vid.*, en sentido amplio, CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Derecho internacional privado.* vol. I, 9ª edición, Comares, Granada, 2008, pp. 200-205.

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

Compañía o con alguno de nuestros afiliados. Respecto a toda disputa o queja no sujeta a arbitraje (tal y como se indica abajo), estás de acuerdo en no emprender ninguna acción fuera del estado y de los tribunales federales de California, y con esto das el consentimiento, y prescindes de toda defensa de carencia de jurisdicción personal o de foro de no conveniencia respecto a esto, lugar de reunión y órgano jurisdiccional del estado y *tribunales federales de California*_[...] »; y, en el caso de *MySpace* las partes « [...] aceptan someterse a la jurisdicción exclusiva de los *tribunales con asiento en el Estado de Nueva York* para resolver cualquier controversia que surja en relación con el Acuerdo o los Servicios MySpace [...] ».

3.3 Foro del domicilio del demandado.

La aplicación del foro general del domicilio del demandado (= *forum defensoris*) viene contemplado en los diferentes instrumentos jurídicos relativos a la atribución de competencia judicial internacional antes reseñados; así, a falta de pacto expreso o tácito atributivo de jurisdicción, el criterio que atribuye competencia es el del *domicilio del demandado*, que lo hace a favor de los tribunales del domicilio del juez natural, esto es, del demandado (= *actor sequitur forum rei*).

Las personas domiciliadas en un Estado miembro/contratante estarán sometidas, sea cual fuere su nacionalidad, a los órganos jurisdiccionales de dicho Estado. Sin perjuicio de esta disposición, el artículo 3.1 establece que estas personas podrán ser demandadas ante los tribunales de otro Estado miembro/contratante en virtud de las reglas establecidas en el RB o en el CB/CL. Dichos foros de competencia resultan aplicables, como hemos señalado, en defecto de cláusula de elección de foro a los tribunales de un Estado miembro/contratante.

Eso sí, el domicilio del demandado se configura como una nueva forma de ataque del demandante; una solución fácil, neutra y práctica[25]. El *domicilio* constituye un concepto jurídico cuyo significado debe venir determinado por una norma legal.

Se considera que las *personas jurídicas* están domiciliadas en aquel Estado miembro en el que tienen: a) su sede estatutaria, o b) su administración central, o c) su centro de actividad principal.

En el caso de las *personas físicas* para determinar si están domiciliadas en el Estado miembro cuyos tribunales conocen del asunto, el juez aplicará su ley interna[26].

[25] ***Vid.*, en relación con los motivos que favorecen el recurso al foro general del domicilio del demandado en los supuestos de responsabilidad civil producidos a través de Internet, PALAO MORENO, Guillermo, «Competencia judicial internacional en supuestos de responsabilidad civil en Internet», *op. cit.*, pp. 282-283.**

[26] **En el caso de España, el artículo 40 del CC señala que «para el ejercicio de los derechos y el cumplimiento de las obligaciones civiles, el domicilio de las personas naturales es el lugar de su residencia habitual, y en su caso, el que determine la Ley de Enjuiciamiento Civil».**

Cuando sea necesario determinar si el demandado está domiciliado en otro Estado miembro, se aplicará la ley de dicho Estado.

Ahora bien, en la práctica, esta atribución de competencia plantea dos *dificultades principales*[27], que justifican la habitual derogación de tal foro general por medio del recurso a la autonomía de la voluntad: la falta de neutralidad de la jurisdicción resultante y la llamada genérica que realiza a todos los órganos en ella integrados: a) en primer lugar, el recurso al foro general situaría al demandante en la nada cómoda situación de tener que litigar en casa de su contraparte, con lo que ello supone: desconocimiento del idioma, aumento de los costes, desconocimiento de las normas procesales aplicables, etc.; y, b) en segundo lugar, nos conduce a la designación de la jurisdicción competente en términos genéricos: tribunales españoles, alemanes, suizos, belgas, etc.; y, a partir de ahí, serán las normas de reparto territorial de la organización jurisdiccional correspondiente quienes deban designar el órgano jurisdiccional concreto ante el cual plantear la reclamación.

Es más, se trata de un foro de competencia poco útil en nuestro caso por dos razones prácticas más: a) por un lado, porque en ocasiones el presunto responsable actúa desde países lejanos o exóticos, de modo que el demandante no conoce o puede no averiguar fácilmente el domicilio del demandado; y, b) por otro lado, porque es un foro de competencia poco adecuado para acciones de cesación cuando el servidor en el que se aloja la página web o la información se halla en un país distinto al país del domicilio del demandado[28].

3.4 Foro especial en materia de obligaciones extracontractuales: el *lugar donde se hubiere producido o pudiere producirse el hecho dañoso*.

Se trata de una norma –manifestación del principio de proximidad– que en el mundo analógico, en los últimos tiempos, ha planteado numerosos interrogantes: p. ej., su aplicación en supuestos donde la acción causal y el resultado dañoso se presentan disociados en diversos países, o su aplicación en casos de plurilocalización del hecho dañoso; y, cuya aplicación en el mundo virtual se hace difícil, pues la duda nos embarga: ¿dónde debe considerarse que se ha producido un hecho dañoso cometido a través de Internet.

---

[27] *Vid.*, en particular, sobre los problemas que plantea este foro en materia de comercio electrónico, CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Conflictos de leyes y conflictos de jurisdicción…* *op. cit*, pp. 37-41; y, DE MIGUEL ASENSIO, Pedro, *Derecho privado de Internet*. 3ª edición, *op. cit*, pp. 455-456.

[28] *Vid.* CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Derecho internacional privado*. vol. I, 9ª edición, Comares, Granada, 2008, pág. 783.

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

En lo que respecta a la responsabilidad civil extracontratcual en esta materia «[...] las personas domiciliadas en un Estado miembro podrán ser demandas en otro Estado miembro [...] en materia delictual o cuasidelictual, ante el tribunal del lugar donde se hubiere producido el hecho dañoso [...]»; además, permite la indeterminación del lugar de producción del hecho dañoso, al señalar que «[...] las personas domiciliadas en un Estado miembro podrán ser demandas en otro Estado miembro [...] en materia delictual o cuasidelictual, ante el tribunal del lugar donde se hubiere producido o pudiere producirse el hecho dañoso [...]».

Por su parte, la LOPJ señala que, en defecto de cláusula de elección de foro, cuando el demandado está domiciliado en un tercer Estado, los tribunales españoles se pueden declarar competentes.

La LOPJ ofrece una serie de foros de competencia judicial internacional en cuya virtud los Tribunales españoles pueden conocer de situaciones privadas internacionales. En la materia que nos ocupa los tribunales españoles pueden resultar competentes cuando el hecho del que derivan haya ocurrido en territorio español.

El principal problema que plantea el *forum locus delicti commissi* es el de determinar si por país en que se produce el daño debemos entender el del lugar en el que se localiza el hecho causal (p. ej. el Estado desde el que se introduce el contenido ilícito en Internet, siendo irrelevante el lugar donde radica el servidor que aloja la *webpage*) o el del lugar en que se verifica el resultado dañoso (p. ej., el Estado desde el que se accede al contenido ilícito vertido en Internet)[29], sobre todo, en casos de disociación geográfica del ilícito (cuando el daño y el hecho generador se localizan en distintos países).

La determinación del *lugar donde se ha producido el hecho dañoso* plantea, en el mundo virtual, dos dificultades: por un lado, la determinación del lugar donde tienen lugar el evento generador del daño; y, por otro lado, la concreción del lugar del resultado lesivo. Respecto de la primera cuestión, la doctrina mayoritaria entiende que se debe ubicar dicho lugar donde se han introducido tales contenidos perjudiciales por parte del causante del daño. Y, respecto de la segunda cuestión, decir que, en tales supuestos, dicho lugar puede ser: a) el lugar desde donde se han introducido los datos; b) en el marco de Internet, el lugar donde está ubicado el servidor que los alberga; c) el lugar desde donde se puede tener acceso a los datos;

[29] El *forum locus delicti commissi* plantea algunas dificultades de adaptación cuando nos encontramos ante «delitos a distancia», ya que abre al demandante tres alternativas posibles a la hora de localizar el lugar del hecho dañoso: a) el lugar donde se hubiere cometido la acción lesiva (= lugar de acción); b) el lugar donde se hubiere sufrido el perjuicio (= lugar de resultado); o, c) optar por uno u otro. *Vid.* PALAO MORENO, Guillermo, «Competencia judicial internacional en supuestos de responsabilidad civil en Internet», *op. cit.*, pág. 287.

o, d) el lugar donde reside el titular del derecho infringido, que es, en definitiva, donde se ha producido el hecho dañoso.

Lo habitual es que el hecho dañoso se produzca en el *país donde radica el fichero de datos*, aunque no tiene por qué ser siempre así[30]; ya que, el lugar donde se ha producido el hecho dañoso puede ser, efectivamente, el país o países (si se han producido transferencias de datos sucesivas, y sólo para los perjuicios causados en cada uno de esos territorios) donde se han transferido los datos (que en las transferencias de datos de España al extranjero, ese lugar será, por aplicación del artículo 2.1 de la LOPD, España), así como, el país donde se haya manifestado el daño por el tratamiento de datos realizado en ese lugar, por parte del que recibió los datos.

4. Redes sociales de Internet, protección de datos, y determinación de la ley aplicable.

La determinación de la ley aplicable en materia de tratamiento de datos de carácter personal a través de una red social de internet supone la aplicación del artículo 2.1 de la LOPD, que transpone el artículo 4 de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Directiva 95/46/CE)[31], y que implica alinearse en alguno de estos dos bandos: el de la liberalización de la circulación de datos automatizados, o el de la protección del derecho a la intimidad de las personas[32]. Así, mientras el artículo 4 de la Directiva 95/46/CE opta por la aplicación de la ley del lugar de residencia del responsable del fichero de datos (no es relevante el lugar de tratamiento de los datos ni la nacionalidad, domicilio o residencia habitual del sujeto cuyos datos se tratan o del sujeto responsable del tratamiento, sino que sólo es relevante el lugar de su establecimiento); el artículo 2.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo, LOPD)[33] opta por la ley del lugar de tratamiento de los datos de carácter personal[34].

La Directiva 95/46/CE opta por el criterio de la residencia del responsable del fichero en la medida en que de esta forma, « [...] 1º) Se evita la aplicación de la regla general en materia de responsabilidad no contractual: no se aplica la *lex loci delicti commissi* o ley del país donde se produce el tratamiento ilícito de los datos [...] 2º) [Se

[30] ***Vid.*** **CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Conflictos de leyes y conflictos de jurisdicción… op. cit*, pág. 153.**
[31] ***DOCE*** **núm. L 281, de 23 de noviembre de 1995.**
[32] ***Vid.*****, en el mismo sentido, *ibidem*, pp. 154-155.**
[33] ***BOE*** **núm. 298, de 14 de diciembre de 1999**
[34] **Nos encontramos ante dos preceptos que, por su contradicción, inducen a la confusión, que cubren tanto las relaciones administrativas como las relaciones entre particulares en asuntos internacionales, y que aparecen preocupadas por fijar el ámbito de aplicación de la normativa del Estado cuyos Tribunales conocen del asunto. *Vid.*, *ibidem*, pp. 156-157.**

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

recurre a una argumentación económica que se aleja] de la Ley del país más vinculado al supuesto [, de forma que] la proximidad del supuesto con un país no guía la mano del legislador comunitario a la hora de construir la solución de Derecho internacional privado en esta materia [favoreciendo, así, a las empresas informáticas que operan en este sector por cuatro razones:] 1º) El criterio promueve la actividad internacional de tratamiento de datos en la UE, ya que, sean cuales sean los países en los que la empresa desarrolle sus actividades, la Ley aplicable al tratamiento de datos será siempre la misma, la Ley del fichero [...] 2º) Se trata, además, de una Ley conocida por la empresa [...] 3º) Por otro lado, la empresa que trata los datos queda sometida a un mismo Derecho nacional tanto por lo que respecta a sus relaciones administrativas con las Autoridades públicas, como por lo que se refiere a las relaciones con los particulares afectados por el tratamiento de datos [...] 4º) La norma de conflicto contenida en el artículo 4 [de la] Directiva es una norma de conflicto específica, diseñada para una materia concreta. Por eso, difícilmente admite excepciones o reducciones teleológicas, desviaciones que permitan apartarse del criterio de la aplicación de la Ley de situación del responsable del fichero, lo que sería factible si la norma fuera una norma general o principal. Tampoco el artículo 4 [de la] Directiva se ve corregido por una cláusula de escape o por una cláusula de excepción [...] ».

Además, el artículo 4 de la Directiva 95/46/CE concreta el criterio de la ubicación del fichero de datos en dos supuestos especiales que, por su fisionomía, la localización del fichero de datos supone casi misión imposible: a) según el artículo 4.1.a *in fine* de la Directiva, si el responsable del fichero de datos posee distintos establecimientos en diferentes Estados de la UE, el tratamiento de datos realizado *en el marco de las actividades de cada establecimiento* se rige por la Ley del país donde radica cada establecimiento; y, b) en virtud del artículo 4.1.b de la Directiva, en el supuesto de un responsable del tratamiento establecido en un lugar que no pertenece a la UE, pero en el que se aplica la legislación nacional de un Estado miembro en virtud del Derecho internacional público, se aplicará la Directiva 95/46/CE.

El panorama cambiará a partir del próximo mes de mayo de 2018, con la aplicación del Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), de 25-01-2012[35]. Éste fija como primer criterio que su ámbito territorial comprende el tratamiento de datos «en el contexto de las actividades de un

[35] ***COM (2012) 11 final.***

establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no» (artículo 3.1). Las innovaciones respecto al texto del artículo 4.1.a) de la Directiva son aquí menores, pues se limitan a que el Reglamento General de Protección de Datos hace referencia expresa no sólo al «responsable» sino también al «encargado» del tratamiento. Por otra parte, se elimina la referencia a las situaciones en las que un mismo responsable del tratamiento esté establecido en varios Estados miembros como circunstancia que llevaba a tener que cumplir con sus respectivas legislaciones, lo que se corresponde con que el Reglamento General de Protección de Datos sustituye a las legislaciones de todos los Estados miembros.

Para garantizar un alto nivel de protección, se mantiene la interpretación muy amplia y flexible del concepto de establecimiento, que se extiende «a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable», como recoge el Considerando 22 del Reglamento General de Protección de Datos. Ahora bien, es necesario que el tratamiento se produzca en el contexto de las actividades del establecimiento.

No obstante, a fecha de hoy, con carácter general, para la determinación de la ley aplicable en materia de responsabilidad civil extracontractual por vulneración del derecho a la protección de datos en el ámbito de las redes sociales de Internet se distinguen dos supuestos: a) cuando el responsable del tratamiento de datos está situado en un Estado miembro de la UE (= Redes sociales de Internet cuyo establecimiento se encuentra en un Estado miembro de la Unión Europea); y, b) cuando el responsable del tratamiento se encuentra en un tercer Estado no comunitario (= Redes sociales de Internet cuyo establecimiento se encuentra en un *tercer país* no comunitario y Redes sociales de Internet cuyo establecimiento se encuentra en un "tercer país" no comunitario pero se utilizan medios situados en España.). Veamos cada uno de estos supuestos:

4.1 Redes sociales de Internet cuyo establecimiento se encuentra en un Estado miembro de la Unión Europea.

Cuando el tratamiento de datos, a través de la red social de Internet, es llevado a cabo por un responsable situado en un Estado miembro de la Unión Europea, se aplicará la Ley de dicho Estado miembro, en virtud del artículo 4 de la Directiva 95/46/CE. Además, si el tratamiento es efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento, se aplicará la Ley española (= LOPD), en virtud del mencionado artículo 2.1 de la LOPD.

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

4.2 Redes sociales de Internet cuyo establecimiento se encuentra en un "tercer país" no comunitario.

En este supuesto, y en virtud de una combinación del artículo 2 de la LOPD y del artículo 4 del Reglamento «Roma II»[36], el tratamiento de datos personales por parte de un responsable cuyo establecimiento se encuentra en un tercer Estado no comunitario se rige por las siguientes Leyes: a) la Ley elegida por las partes; b) en su defecto, se aplicará la Ley del país de residencia habitual común de las partes; c) en su defecto, se aplicará la Ley del país donde se lleve a cabo el tratamiento de datos, sea un Estado miembro o un tercer Estado (= Ley del país de comisión del hecho dañoso); y, d) no obstante, si del conjunto de circunstancias se desprende que el hecho dañoso presenta vínculos manifiestamente más estrechos con otro país distinto, se aplicará la Ley de ese otro país[37]. Ahora bien, si el hecho dañoso se produce en varios países, entonces el perjudicado deberá reclamar con arreglo a cada una de las Leyes de los países en los que su derecho ha sido vulnerado y por los daños allí sufridos.

Las principales redes sociales de Internet abogan por la autonomía de la voluntad (= Ley elegida por las partes): así, de la lectura de sus Condiciones de uso se deduce: en el caso de *Facebook*, que: « [...] Al visitar o hacer uso del Sitio o el Servicio, aceptas que las *leyes del estado de Delaware*, sin tener en cuenta los principios del conflicto de leyes, regularán estas condiciones de uso así como cualquier disputa que pudiera surgir entre tú y la Compañía o con alguno de nuestros afiliados. Respecto a toda disputa o queja no sujeta a arbitraje (tal y como se indica abajo), estás de acuerdo en no emprender ninguna acción fuera del estado y de los tribunales federales de California, y con esto das el consentimiento, y prescindes de toda defensa de carencia de jurisdicción personal o de foro de no conveniencia respecto a esto, lugar de reunión y órgano jurisdiccional del estado y tribunales federales de California [...] »; que en el caso de *LinkedIn* las partes acuerdan que « [...] Este Contrato y cualquier conflicto con LinkedIn o sus sociedades relacionadas en virtud de este Contrato o de LinkedIn (los "Conflictos") se regirán por la *legislación vigente en California*, sin hacer referencia a disposiciones relativas al principio de conflicto de leyes y excluyendo las disposiciones de la CNUCCIM-CISG [...] »; o, que os usuarios de

[36] Reglamento (CE) Nº 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, relativo a la ley aplicable a las obligaciones extracontractuales («Roma II»), *DO* L 199/40, de 31/07/2007.
[37] *Vid.* CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Derecho internacional privado.* vol. I, 9ª edición, Comares, Granada, 2008, pág. 796.

MySpace saben que « [...] El Acuerdo se regirá e interpretará de acuerdo con las *leyes del Estado de Nueva York*, sin tener en cuenta sus disposiciones sobre conflictos de leyes [...])».

4.3 Redes sociales de Internet cuyo establecimiento se encuentra en un "tercer país" no comunitario pero se utilizan medios situados en España.

Finalmente, es de reseñar el siguiente supuesto: cuando el responsable del tratamiento de datos no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos, *medios* situados en territorio español (= ordenadores personales, terminales, cámaras de televisión, *cookies*, etc.), salvo que tales medios se utilicen únicamente con fines de tránsito (= artículo 4.1.c de la Directiva 95/46/CE)[38]. Se halla ampliamente extendido el criterio de que esas normas imponen la aplicación del régimen comunitario de protección de datos personales en los diversos supuestos en los que sitios *web* cuyos responsables no estén establecidos en la Unión Europea emplean dispositivos para la recogida activa de datos procedentes de los ordenadores de los usuarios situados en Estados miembros con el objetivo de su tratamiento futuro. En los supuestos en los que el sitio *web* se limita a obtener datos personales mediante formularios en los que los usuarios facilitan cierta información, resulta más controvertido en qué medida ello implica utilizar medios situados en el territorio de un Estado miembro, si bien tiende a afirmarse que no es determinante que ahí se encuentre el ordenador desde el que el usuario accede al servicio sino que desde el punto de vista técnico más relevante sería dónde se ubica el servidor en el que se aloja el correspondiente sitio *web*.

Una interpretación amplia del ámbito de aplicación de la Directiva 95/46/CE ha sido objeto de críticas, en la medida en que puede conducir en la práctica a extender la aplicación de la normativa española (= la LOPD) y, por ende, de la europea (=Directiva 95/46/CE) y, por supuesto, la competencia de las correspondientes autoridades de protección, a un número extraordinario de entidades de todo el mundo (en nuestro caso, redes sociales de Internet), incluso respecto de supuestos en los que la captación de datos en la Unión Europea puede ser no sólo ocasional sino incluso accidental. Por lo tanto, el criterio de que la actividad vaya dirigida a un determinado territorio resultaría también determinante en este entorno, lo que contribuiría a excluir de la exigencia de cumplir con la legislación europea

[38] Nada dispone la Directiva 95/46/CE sobre la Ley aplicable al tratamiento de datos personales realizado en territorio de terceros Estados sin intervención de medios técnicos en Estados de la Unión Europea. Ello explica que la Directiva 95/46/CE someta a un régimen muy estricto la circulación de datos personales desde la Unión Europea con destino a terceros países. *Vid. íbidem*, pág. 795.

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

(Directiva 95/46/CE), entre otros, a sitios *web* cuya captación de datos en la Unión Europea sea meramente accidental.

5. *Cloud computing*, protección de datos, y relaciones privadas internacionales.

El *cloud computing o computación en nube*, como modelo flexible de prestación de servicios tecnológicos, no es el futuro, sino que es, en estos momentos, una realidad[39]. Se trata de un modelo que no sólo les permite a las empresas (grandes y pequeñas) ahorrar costes, sino también les proporciona mayor agilidad. Aspectos como el almacenamiento y la capacidad de cómputo, el software de análisis, el software de gestión empresarial, los entornos de desarrollo, los puestos de trabajo o las herramientas de comunicación o de colaboración quedan en la *nube*, privada –*cloud* propiedad de la empresa– o pública –*cloud* propiedad de un prestador de servicios externo, que proporciona acceso al cliente bajo un modelo de pago por suscripción–, permitiendo a las empresas acceder a la tecnología sin asumir fuertes inversiones. Bueno, pero seamos claros: la nube no es otra cosa que la propia Internet, cuya tecnología hace posible que todo un sistema informático deje de estar en un lugar concreto para «evaporarse» y «mezclarse» en la *nube* de Internet. En un único servidor descentralizado gracias a Internet se consigue, por parte de las empresas, trabajar con una nueva infraestructura común a todas las aplicaciones informáticas (*software* y *hardware*) con las que trabajan, y con un ahorro que podemos cifrar entre el 30 % y el 70 %.

Ahora bien, como en todo, existe cierto temor cuando se habla del *cloud computing*. Son muchos los interrogantes que se articulan y que pueden llegar a hacernos cuestionar el uso de este nuevo modelo de prestación de servicios tecnológicos: ¿qué tenemos que tener en cuenta desde un punto de vista legal a la hora de afrontar un proyecto en la nube?; ¿es legal «colocar» en Internet los datos personales de nuestros clientes, proveedores y trabajadores?; ¿pierde la empresa el control de sus sistemas de información?; ¿qué tenemos que tener en cuenta en la negociación de la gestión contractual de los servicios en la nube?; ¿cómo se

[39] La computación en nube es un modelo para permitir el acceso conveniente por red bajo demanda a un conjunto compartido de recursos informáticos configurables (p. ej., redes, servidores, almacenamiento, aplicaciones o servicios) que pueden proporcionarse y servirse rápidamente con un esfuerzo mínimo de gestión o interacción por parte del proveedor del servicio.

configura contractualmente el pago por uso?; ¿cuál es la ley aplicable a los tratamientos de datos que se realizan en la nube?; ¿cómo se configuran los controles de acceso al *cloud*?; ¿cómo se gestiona la seguridad de la información en la nube?; ¿cómo deben evaluarse modelos de computación en nube diferentes por lo que respecta a la Directiva 95/46/CE?; o, ¿siguen siendo útiles los conceptos de responsable del tratamiento de datos, encargado del tratamiento de datos e interesado o titular de los datos, tal y como se definen en la Directiva 95/46/CE?

Sin duda alguna, hablar de la Sociedad de la Información y de la computación en nube es hablar de *relaciones privadas internacionales*, esto es, es hablar de Derecho internacional privado. Gracias a Internet «resulta sencillo navegar entre páginas, y, por ello, entre países y jurisdicciones de tal forma que con sólo hacer *click* uno abandona una página ubicada en territorio español para pasar a ver otra página almacenada en Estados Unidos»[40]. Es más, «la mayor parte de las operaciones realizadas en Internet son *internacionales*: en tales situaciones hay presente uno o múltiples *elementos extranjeros* y/o producen *efectos* en varios países o incluso en todo el mundo»[41].

En una Comunicación de la Comisión al Parlamento Europeo de finales del año 2010 ya se mencionaba *la computación en la nube como uno de los grandes retos en materia de protección de datos.* El almacenamiento de datos en la *nube* ha facilitado el acceso e intercambio de información, pero, lamentablemente, también ha simplificado el camino hacia el robo o pérdida de datos de carácter personal[42]. El reciente robo de datos a los servidores de Sony, que ha afectado a más de cien millones de usuarios en todo el mundo, o la caída de los servidores de Amazon, en abril de 2011, con la consecuente pérdida de parte de la información de clientes como Foursquare o Quora, son meros ejemplos de ello.

La mayoría de los servicios en Internet, a la vez, solicitan al usuario sus datos personales para acceder a ellos. No todos los internautas saben que su derecho a reclamación en caso de incidencia depende en parte de dónde se encuentran ubicados físicamente los servidores de las empresas que ofrecen el servicio y, por tanto, sus datos. Los grandes operadores de Internet no almacenan sus datos en España, y esto provoca que en ocasiones intenten acogerse a ello para no indemnizar

---

[40] *Vid.* LLANEZA GONZÁLEZ, PALOMA. *Aplicación práctica de la LSSI-CE*. Bosch, Barcelona, 2003, pág. 161.
[41] *Vid.* CALVO CARAVACA, ALFONSO-LUIS y CARRASCOSA GONZÁLEZ, JAVIER. *Derecho internacional privado. Vol. II*, 8ª edición, Comares, Granada, 2007, pág. 652; y, CALVO CARAVACA, ALFONSO-LUIS y CARRASCOSA GONZÁLEZ, JAVIER. *Conflictos de leyes y conflictos de jurisdicción en Internet*. Colex, Madrid, 2001, pág. 13.
[42] *Vid.* LEENES, RONALD (2010). «¿Quién controla la nube?». En: «VI Congreso Internet, Derecho y Política. *Cloud Computing*: El Derecho y la Política suben a la Nube» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N. º 11. UOC. [Fecha de consulta: 21/06/2011].
<http://idp.uoc.edu/ojs/index.php/idp/article/view/n11-leenes/n11-leenes-esp>

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

a sus usuarios ante robo o pérdida de datos. Sirva este supuesto de ejemplo: Microsoft también ofrece servicios de *cloud computing* y almacena datos de sus clientes. De hecho, acaba de presentar en pruebas Office 365, un producto para empresas diseñado para trabajar online. Los servicios en la nube que Microsoft lanza en España tanto para usuarios como para empresas almacenan los archivos de los usuarios en un complejo de 50.000 metros cuadrados con 200.000 servidores ubicados en Irlanda.

Los posibles problemas de vulneración del derecho a la protección de datos de carácter personal derivados de la computación en nube deben ser resueltos a partir de las *normas de Derecho internacional privado español*, relativas a la responsabilidad civil contractual o extracontractual. Debemos justificar que el Derecho internacional privado sea la rama del ordenamiento jurídico español que resuelva estos litigios proponiendo soluciones tales como la unificación de las normas estatales de Derecho internacional privado para evitar la relatividad de las soluciones y/o la utilización de criterios subjetivos, flexibles y particulares, que permitan la vinculación del supuesto concreto con un país determinado [43].

6. *Cloud computing* y responsabilidad contractual y no contractual por vulneración del derecho a la protección de datos personales: problemas de Derecho internacional privado.

En el ámbito del Derecho internacional privado, los problemas para el derecho a la protección de datos personales que plantea el *cloud computing* están, fundamentalmente, relacionados con la determinación del órgano jurisdiccional competente para conocer de un determinado litigio, así como de la determinación de la ley aplicable para resolver el conflicto planteado. La delimitación de ambos aspectos será de vital importancia ya que, como es bien sabido, cada sistema jurídico tiene establecido un sistema de normas de conflicto, en virtud del cual se determina quién será el órgano jurisdiccional competente, y cuál será la ley aplicable para resolver la controversia que se plantee[44]. Ambas cuestiones están interrelacionadas: la

[43] *Vid.*, en sentido amplio, ORTEGA GIMÉNEZ, Alfonso, "*Cloud Computing*, Protección de datos y Derecho internacional privado (Resolución de controversias y determinación de la ley aplicable)", en MARTÍNEZ MARTÍNZ, Ricard (Editor), *Derecho y Cloud Computing*, Civitas, Thomson Reuters, Cizur Menor (Navarra), 2012, pp. 255-287.

[44] *Vid.*, en particular, BING, J. «*Data protection, jurisdiction and the choice of law*», en *Privacy Law & Policy. Reporter*, volume 6, 1999, pp. 92-98; y, REIDENBERG, J. R. «Technology and Internet Jurisdiction», en *UNIVERSITY OF PENNSYLVANIA LAW REVIEW*, Vol. 153, pp. 1951-1974.

determinación de la ley aplicable no es independiente de la jurisdicción competente (= determinación de la competencia judicial internacional): la obtención de una sentencia que ponga fin al litigio privado internacional planteado por las partes exige: primero, determinar el tribunal competente de todos aquellos que tienen cierta conexión con el litigio; y, segundo, que el tribunal elegido determine la ley aplicable al fondo del asunto.

Visto que el mundo está dividido en Estados, que estos cuentan con su propia organización de tribunales y sus propias leyes, y que son diferentes de país a país; los interrogantes son claros: ¿qué tribunales estatales serían competentes? y ¿qué ley aplicarán? ante un litigio derivado de la vulneración del derecho a la protección de datos personales, como consecuencia del *cloud computing*?[45]

En el ámbito del Derecho internacional privado, los problemas para el derecho a la protección de datos personales que la computación en nube plantean están relacionados con la determinación del órgano jurisdiccional competente para conocer de un determinado litigio, así como de la determinación de la ley aplicable para resolver el conflicto planteado. La delimitación de ambos aspectos será de vital importancia ya que, como es bien sabido, cada sistema jurídico tiene establecido un sistema de normas de conflicto, en virtud del cual se determina quién será el órgano jurisdiccional competente y cuál será la ley aplicable para resolver la controversia que se plantee[46]. Así, p. ej., pensemos en aquella empresa española que usa Google Docs y otras aplicaciones de Google para colaborar con una empresa extranjera en un proyecto empresarial europeo cualquiera. Se presta el servicio a la empresa española a través de un servidor alojado en Bruselas (Bélgica), con una copia de seguridad en Ámsterdam (Holanda). Si se produjera una "fuga de datos", y la empresa española recibiera una reclamación por parte de un sujeto español con domicilio también en España, por el tratamiento informatizado y transferencia internacional de sus datos sin su consentimiento, dos serían, básicamente, las cuestiones *iusinternacionalprivatistas* a resolver: ¿ante qué órganos jurisdiccionales se debería interponer la demanda: los españoles, los holandeses, o los belgas? y ¿cuál sería la ley aplicable: la española, la belga o la holandesa?

El daño derivado de la intromisión ilegítima en el derecho a la protección de datos, manifestado en el uso indebido o ilegítimo de sus datos personales, consecuencia de la prestación de servicios tecnológicos en la nube, sobre la base de

[45] Otra cuestión es que, en la práctica, desgraciadamente, el tribunal ante el que se plantea un *caso internacional* ni tan siquiera se planteen estas cuestiones, bien por desconocimiento, bien por comodidad.

[46] *Vid.*, sobre la materia, en particular, BING, J. «*Data protection, jurisdiction and the choice of law*», en *Privacy Law & Policy. Reporter*, volume 6, 1999, pp. 92-98; y, REIDENBERG, JOEL R. «Technology and Internet Jurisdiction», en *UNIVERSITY OF PENNSYLVANIA LAW REVIEW,* Vol. 153, pp. 1951-1974.

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

la existencia o no de una vinculación jurídica entre el causante del daño y el afectado, puede dar lugar a la exigencia de responsabilidad civil contractual (= cuando entre el autor y la víctima hubiere existido una previa relación contractual y se hubiere producido un incumplimiento de lo pactado –responsabilidad derivada de un contrato de prestación de servicios en la nube–), o extracontractual (= exigencia de una indemnización por los daños y perjuicios ocasionados –responsabilidad no contractual por vulneración del derecho a la protección de datos personales derivada de la computación en nube–).

En estos supuestos, la vulneración del derecho a la protección de datos traerá como resultado la exigencia de responsabilidad civil objetiva[47], derivándose el derecho a indemnización del afectado por el tratamiento de sus datos, tal y como señala el artículo 19.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo, LOPD)[48]: «los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley [Orgánica de Protección de Datos de carácter Personal] por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados»[49].

La exigencia de una indemnización por daños y perjuicios no excluye la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación frente al responsable del fichero de datos. Los afectados o interesados por el tratamiento de sus datos, como titulares del derecho fundamental a la protección de datos, se encuentran facultados para conocer y acceder a las informaciones que les pudieran afectar, archivadas en bancos de datos, y controlar su calidad, permitiendo que puedan ser corregidos o cancelen los datos inexactos o indebidamente procesados, y la disposición sobre su transmisión.

7. *Cloud computing*, protección de datos, y resolución de controversias.

[47] Es más, se debe fortalecer el uso de la responsabilidad civil extracontractual objetiva como mecanismo regulatorio para garantizar los derechos fundamentales en las aplicaciones en la Sociedad de la Información y Conocimiento, Internet y redes sociales digitales, *Vid.*, en particular, *Memorandum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes*, hecho en Montevideo, el 28 de julio de 2009.

[48] *BOE* núm. 298, de 14 de diciembre de 1999.

[49] Este precepto viene a coger la responsabilidad civil extracontractual o aquiliana de los artículos 1902 y 1903 de nuestro Código Civil. Este tipo de responsabilidad es de aplicación cuando el daño se haya producido por los ficheros de titularidad privada, en aquellos supuestos en los que no existe una relación entre los interesados, perjudicado y responsable, sino que se trata de dos personas entre las que nace el derecho y obligación de indemnizar como consecuencia de actos del responsable en los que no ha intervenido la voluntad del perjudicado.

7.1 El sistema español de competencia judicial internacional.

La determinación de la competencia judicial internacional en materia de reclamaciones por la vulneración del derecho a la protección de datos derivada del *cloud computing*, nos lleva a un laberinto normativo de intrínseca complejidad, ya que se acumulan fuentes de origen diverso: institucional o comunitario, convencional y autónomo. Así, debemos acudir a los siguientes instrumentos normativos: 1º) al «limitado»[50] Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Bruselas, el 27 de septiembre de 1968 (en lo sucesivo, CB); 2º) a su «gemelo»[51], el «también limitado» Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Lugano, el 16 de septiembre de 1988 (a partir de ahora, CL)[52], y su «sucesor», el Convenio de «Lugano II», de 30 de octubre de 2007, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil[53] (en adelante, CL II); 3º) al Reglamento (UE) núm. 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil —Reglamento «Bruselas I bis»—[54]; o, 4º) a la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante, LOPJ)[55]. La aplicación de un instrumento jurídico u otro dependerá del domicilio del demandado.

Centrándonos en la materia que nos ocupa, lo habitual será que consecuencia de un contrato de prestación de servicios en la nube, se haya utilizado, de forma inconsentida un dato de carácter personal dando lugar a una reclamación por daños y perjuicios los criterios atributivos de competencia serían los siguientes: a) el foro del domicilio del demandado, esto es, los tribunales del país donde esté domiciliado el «presunto vulnerador-demandado» conocerá de todas las pretensiones que se deduzcan contra él, independientemente del país o países en los que se haya producido el hecho dañoso; b) el foro de la sumisión, expresa o tácita, que nos permite concentrar los litigios a los que las partes se refieran, bajo el conocimiento de los tribunales de un solo país; y, c) el foro del lugar del hecho dañoso, que atribuye

---

[50] El CB se aplica, en la actualidad, únicamente con relación a los territorios franceses de ultramar y a las Antillas holandesas.

[51] El CB y el CL poseen un contenido normativo prácticamente idéntico, siendo sus únicas diferencias las referidas al contrato individual de trabajo y a los contratos de arrendamiento de corta duración.

[52] *BOE* núm. 243, de 10 de octubre de 1979.

[53] *DOUE* L 339, de 21 de diciembre de 2007. Este texto convencional entró en vigor el 01/01/2010. Son Estados parte: los Estados miembros de la UE, incluido Dinamarca (desde el 01/01/2010), Noruega (desde el 01/01/2010), Suiza (desde el 01/01/2011), e Islandia (desde el 01/05/2011).

[54] *DOUE* L 351/1 de 20/12/2012. Modificado por el Reglamento (UE) núm. 542/2014 del Parlamento y del Consejo, de 15 de mayo de 2014, por el que se modifica el Reglamento (UE) núm. 1215/2012 en lo relativo a las normas que deben aplicarse por lo que respecta al Tribunal Unificado de Patentes y al Tribunal de Justicia del Benelux (*DOUE* L 163 de 29/05/2014).

[55] *BOE* núm. 157, de 2 de julio de 1985. Modificada por la Ley Orgánica 7/2015, de 21 de julio, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. *BOE núm.* 174, de 22 de julio de 2015.

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

competencia a los tribunales del «lugar donde se hubiere producido o pudiere producirse el hecho dañoso» del que nace la responsabilidad extracontractual, pudiendo considerarse como «país donde ocurre el hecho dañoso» tanto el país donde ocurre el hecho causal como el país donde se verifica el resultado lesivo, esto es, el país donde radica el fichero de datos de carácter personal.

Ahora bien, esto no tiene por qué ser siempre así, ya que, por ejemplo, si la actividad consiste en la recogida ilícita de datos personales en España para su ulterior almacenaje informático en un fichero sito en Lisboa, el lugar del daño es tanto España como Portugal.

En definitiva, en el marco de la prestación de servicios en la nube, los foros de competencia operativos serían los siguientes: los Tribunales elegidos por las partes, en virtud de sumisión expresa o tácita, el domicilio del demandado, el lugar donde se hubiere producido o pudiere producirse el hecho dañoso, y el lugar en el que hubiere sido o debiere ser cumplida la obligación que sirviere de base a la demanda. Veamos cada uno de ellos:

7.2 Foro de la sumisión de las partes.

El «acuerdo de sumisión» es un pacto entre las partes de una relación jurídica en cuya virtud éstas determinan el órgano jurisdiccional competente para conocer de los litigios que eventualmente pudieran surgir entre las partes. Tal sumisión puede realizarse mediante acuerdo *expreso* o mediante ciertas prácticas que denotan la voluntad de las partes de someterse a un órgano jurisdiccional: es la «sumisión tácita».

Para que el acuerdo de «sumisión expresa» sea válido es necesario, fundamentalmente, que: a) se designen claramente los tribunales a los que se someten las partes; y, b) el acuerdo de sumisión expresa puede realizarse en cualquier momento, antes o después de la conclusión de un contrato o negocio internacional.

Por su parte, se entiende que las partes se someten tácitamente a los tribunales españoles cuando el demandante acude a tales tribunales interponiendo la demanda o formulando petición o solicitud que haya de presentarse ante el tribunal competente para conocer de la demanda, y cuando el demandado realiza, después de personado en el juicio tras la interposición de la demanda, cualquier gestión que no sea la de proponer en forma la declinatoria.

La validez de un acuerdo atributivo de competencia exige la prueba del acuerdo efectivo entre el demandante y el demandado: la sumisión debe hacerse

por escrito[56]; en este sentido, se admite la formalización de la sumisión expresa por medios electrónicos; esto es, la elección *online* del tribunal competente, siempre que la elección del mismo pueda efectuarse bien mediante intercambio de *emails* o especificándose claramente en el contrato *interpartes*[57].

7.2.1. Foro de la sumisión expresa.

Constituye una prolongación de la autonomía de la voluntad al campo de la competencia judicial internacional, ya que permiten a las partes (a ambas o a una con el consentimiento de la otra) atribuir a los tribunales de un Estado la competencia para conocer de las controversias que puedan surgir del mismo. Asimismo, las partes se pueden someter tácitamente a un tribunal nacional que, en principio, no resultaría competente.

7.2.2. Foro de la sumisión tácita.

Se considera que existe «sumisión tácita»[58] la siguiente conducta procesal de las partes: cuando el demandante presenta una demanda ante el tribunal de un Estado miembro y la comparecencia del demandado ante ese tribunal no tiene por objeto impugnar su competencia judicial[59]. En tal caso, debe entenderse que las partes aceptan tácitamente someter el litigio a ese tribunal.

Los requisitos básicos para que se entienda que se ha producido sumisión tácita son los siguientes: por un lado, que, interpuesta la demanda por el demandante ante los órganos jurisdiccionales de un Estado concreto, el demandado efectúe después de personado en juicio cualquier gestión distinta de la de impugnar la competencia; y, por otro lado, que la controversia no verse sobre ninguna de las denominadas «competencias exclusivas».

Para que no exista sumisión tácita, la impugnación de la competencia del tribunal ante el que se presenta la demanda debe realizarse de acuerdo con las

---

[56] ***Vid.***, en general, sobre la validez de las cláusulas atributivas de competencia en el comercio electrónico, DE MIGUEL ASENSIO, PEDRO. *Derecho privado de Internet.* Civitas, 3ª edición, Madrid, 2002, pp. 448-455.

[57] ***Vid.***, en relación con la elección *online* de los Tribunales competentes, CALVO CARAVACA, ALFONSO-LUIS y CARRASCOSA GONZÁLEZ, JAVIER. *Conflictos de leyes y conflictos de jurisdicción en Internet*. Colex, Madrid, 2001, pp. 43-46.

[58] El foro del acuerdo de «sumisión tácita» para la determinación del Tribunal internacionalmente competente permite el ahorro de costes procesales y (al igual que con la sumisión expresa) que las partes decidan ante qué tribunal quieren litigar. ***Vid.***, en general, sobre el concepto, límites y requisitos de la sumisión tácita como foro de competencia judicial internacional, ***Vid.*** CALVO CARAVACA, ALFONSO-LUIS y CARRASCOSA GONZÁLEZ, JAVIER. «La sumisión tácita como foro de competencia judicial internacional y el artículo 24 del Reglamento 44/2001, de 22 de diciembre 2000», en CALVO CARAVACA, ALFONSO-LUIS y AREAL LUDEÑA, SANTIAGO. *Cuestiones actuales del Derecho mercantil internacional*. Madrid, 2005, pp. 203-215.

[59] Tampoco operará la «sumisión tácita» cuando nos encontremos ante materias que son objeto de competencias exclusivas, ***Vid***. CALVO CARAVACA, ALFONSO-LUIS y CARRASCOSA GONZÁLEZ, JAVIER. *Derecho internacional privado.* vol. I, Comares, Granada, 2003, pág. 130.

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

normas de Derecho procesal del Estado del foro (esto es, el Derecho procesal del país cuyos tribunales conocen del asunto). En el caso de España, la impugnación debe realizarse en el momento y de acuerdo con los cauces procesales previstos en el artículo 64 de nuestra LEC.

7.2.3 Sumisión a tribunales extranjeros.

Y ¿qué ocurriría si el actor presentara su demanda ante los tribunales españoles, pero, existiera un acuerdo de sumisión entre las partes a favor de tribunales extranjeros?... ¿deberían los tribunales españoles declararse incompetentes por la razón de que existe un pacto de sumisión a favor de los tribunales extranjeros? (= admitir o no la declinatoria internacional –*derogatio fori*– sobre la base de la «sumisión a tribunales extranjeros»). En otras palabras, ¿pueden derogar las partes las partes la competencia judicial internacional atribuida a los órganos jurisdiccionales españoles vía LOPJ, a través de un acuerdo en virtud del cual someten el litigio a tribunales extranjeros o a arbitraje privado internacional?

Si bien la LOPJ guarda silencio sobre esta cuestión, la jurisprudencia del TS ha sido la que ha arrojado algo de luz sobre la materia: en un primer momento, se mostró radicalmente contraria a admitir la *derogatio fori*; pero, en un segundo momento, aceptó y acepta una admisión matizada de la misma. Por tanto, hoy día, si el asunto ha sido sometido por las partes a tribunales extranjeros (o a arbitraje privado internacional), estos (o la Corte arbitral) y no los tribunales españoles, son los que deben conocer del litigio[60].

7.3 Foro del domicilio del demandado.

La aplicación del foro general del domicilio del demandado (= *forum defensoris*) viene contemplado en los diferentes instrumentos jurídicos relativos a la atribución de competencia judicial internacional antes reseñados; así, a falta de pacto expreso o tácito atributivo de jurisdicción, el criterio que atribuye competencia es el del «domicilio del demandado», que lo hace a favor de los tribunales del domicilio del juez natural, esto es, del demandado (= *actor sequitur forum rei*)[61].

[60] ***Vid.***, en sentido amplio, CALVO CARAVACA, ALFONSO-LUIS y CARRASCOSA GONZÁLEZ, JAVIER. ***Derecho internacional privado.*** vol. I, Comares, 9ª edición, Granada, 2008, pp. 200-205.

[61] Para determinar si una persona está domiciliada en un Estado o en otro, el Tribunal competente aplicará su ley interna, según señalan los artículos 59 y 60 del RB, y 52 y 53 del CB/CL.

Las personas domiciliadas en un Estado miembro/contratante estarán sometidas, sea cual fuere su nacionalidad, a los órganos jurisdiccionales de dicho Estado.

Eso sí, el domicilio del demandado se configura como una nueva forma de ataque del demandante; una solución fácil, neutra y práctica. El «domicilio» constituye un concepto jurídico cuyo significado debe venir determinado por una norma legal.

En el caso de las «personas jurídicas» se considera que, en el sentido del Reglamento, las personas jurídicas están domiciliadas en aquel Estado miembro en el que tienen: a) su sede estatutaria, o b) su administración central, o c) su centro de actividad principal.

En el caso de las «personas físicas» para determinar si están domiciliadas en el Estado miembro cuyos tribunales conocen del asunto, el juez aplicará su ley interna[62]. Cuando sea necesario determinar si el demandado está domiciliado en otro Estado miembro, se aplicará la ley de dicho Estado.

Ahora bien, en la práctica, esta atribución de competencia plantea dos «dificultades principales»[63], que justifican la habitual derogación de tal foro general por medio del recurso a la autonomía de la voluntad: la falta de neutralidad de la jurisdicción resultante y la llamada genérica que el artículo 2 realiza a todos los órganos en ella integrados: a) en primer lugar, el recurso al foro general situaría al demandante en la nada cómoda situación de tener que litigar en casa de su contraparte, con lo que ello supone: desconocimiento del idioma, aumento de los costes, desconocimiento de las normas procesales aplicables, etc.; y, b) en segundo lugar, el artículo 2 nos conduce a la designación de la jurisdicción competente en términos genéricos: tribunales españoles, alemanes, suizos, belgas, etc.; y, a partir de ahí, serán las normas de reparto territorial de la organización jurisdiccional correspondiente quienes deban designar el órgano jurisdiccional concreto ante el cual plantear la reclamación.

Es más, se trata de un foro de competencia poco útil en nuestro caso por una razón práctica de peso: en ocasiones el presunto responsable actúa desde países lejanos o exóticos, de modo que el demandante no conoce o puede no averiguar fácilmente el domicilio del demandado.

---

[62] En el caso de España, el artículo 40 del CC señala que "para el ejercicio de los derechos y el cumplimiento de las obligaciones civiles, el domicilio de las personas naturales es el lugar de su residencia habitual, y en su caso, el que determine la Ley de Enjuiciamiento Civil".

[63] *Vid.*, en particular, sobre los problemas que plantea este foro en materia de comercio electrónico, CALVO CARAVACA, ALFONSO-LUIS y CARRASCOSA GONZÁLEZ, JAVIER. *Conflictos de leyes y conflictos de jurisdicción... op. cit.*, pp. 37-41; y, DE MIGUEL ASENSIO, PEDRO. *Derecho privado de Internet.* 3ª edición, *op. cit.*, pp. 455-456.

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

7.4 Foro especial en materia de obligaciones extracontractuales: el *lugar donde se hubiere producido o pudiere producirse el hecho dañoso*.

En lo que respecta a la responsabilidad civil extracontractual en esta materia (= vulneración del derecho a la protección de datos personales derivada de la prestación de servicios en la nube) «[...] las personas domiciliadas en un Estado miembro podrán ser demandadas en otro Estado miembro [...] en materia delictual o cuasidelictual, ante el tribunal del lugar donde se hubiere producido el hecho dañoso [...]»; además, se permite la indeterminación del lugar de producción del hecho dañoso, al señalar que «[...] las personas domiciliadas en un Estado miembro podrán ser demandadas en otro Estado miembro [...] en materia delictual o cuasidelictual, ante el tribunal del lugar donde se hubiere producido o pudiere producirse el hecho dañoso [...]».

Por su parte, la LOPJ señala que, en defecto de cláusula de elección de foro, cuando el demandado está domiciliado en un tercer Estado, los tribunales españoles se pueden declarar competentes.

La LOPJ ofrece una serie de foros de competencia judicial internacional en cuya virtud los Tribunales españoles pueden conocer de situaciones privadas internacionales. En la materia que nos ocupa, los tribunales españoles pueden resultar competentes cuando el hecho del que derivan haya ocurrido en territorio español[64].

El principal problema que plantea el *forum locus delicti commissi* es el de determinar si por país en que se produce el daño debemos entender el del lugar en el que se localiza el hecho causal (p. ej. el Estado donde radica el servidor desde el que se recaban de forma inconsentida los datos) o el del lugar en que se verifica el resultado dañoso (p. ej., el Estado donde se encuentra el servidor desde el que se accede a dichos datos personales), sobre todo, en casos de disociación geográfica del ilícito (cuando el daño y el hecho generador se localizan en distintos países).

La determinación del *lugar donde se ha producido el hecho dañoso* plantea, en el mundo virtual, dos dificultades a reseñar: por un lado, la determinación del lugar donde tienen lugar el evento generador del daño; y, por otro lado, la concreción del lugar del resultado lesivo. Respecto de la primera cuestión, la doctrina mayoritaria entiende que se debe ubicar dicho lugar donde se han introducido tales contenidos perjudiciales por parte del causante del daño. Y, respecto de la segunda cuestión,

[64] El artículo 22.3 otorga también la competencia a los tribunales españoles, en materia extracontractual, si «el autor del daño y la víctima tengan su residencia habitual común en España». A hora bien, esto implica que el demandado tendrá su domicilio en un Estado miembro, por lo que se estaría dando el elemento necesario para aplicar los artículos 2 y 5 del RB, por lo que este foro previsto en el artículo 22.3 ya no resulta aplicable.

decir que, en tales supuestos, dicho lugar puede ser: a) el lugar desde donde se han introducido los datos; b) en el marco de Internet, el lugar donde está ubicado el servidor que los alberga; c) el lugar desde donde se puede tener acceso a los datos; o, d) el lugar donde reside el titular del derecho infringido, que es, en definitiva, donde se ha producido el hecho dañoso.

Lo habitual es que el hecho dañoso se produzca en el *país donde radica el fichero de datos*, aunque no tiene por qué ser siempre así[65]; ya que, el lugar donde se ha producido el hecho dañoso puede ser, efectivamente, el país o países (si se han producido transferencias de datos sucesivas, y sólo para los perjuicios causados en cada uno de esos territorios) donde se han transferido los datos (que en las transferencias de datos de España al extranjero, ese lugar será, por aplicación del artículo 2.1 de la LOPD, España), así como, el país donde se haya manifestado el daño por el tratamiento de datos realizado en ese lugar, por parte del que recibió los datos.

7.5 Foro especial en materia de obligaciones contractuales: *el lugar en el que hubiere sido o debiere ser cumplida la obligación que sirviere de base a la demanda*.

Lo normal es que se recoja en el contrato de prestación de servicios en la nube una cláusula que indique que los servicios se van a prestar *online*, en el *Cyberspace*. Pues bien, el lugar de prestación de los servicios, será el lugar donde se almacenan los datos en los que consiste el «servicio», entendiendo por «lugar de prestación de los servicios» el país del domicilio del *demandante*, ya sea el prestador de servicios o ya sea el receptor de los servicios.

De esta forma, ante, p. ej., el incumplimento de un contrato de arrendamiento de software entre una empresa española y otra empresa alemana, donde la prestación de dicho servicio se realizaría en una nube privada, propiedad de esta última, lo primero que tendríamos que determinar es la obligación que se ha incumplido: pago del precio o prestación del servicio. Una vez fijada la *obligación que sirviere de base a la demanda* (supongamos, p. ej., la falta de pago por la empresa española), primero tendríamos que acudir al «lugar pactado entre las partes» en el contrato y en su defecto, al «lugar de pago». Efectivamente, existe pacto *interpartes* sobre el lugar de pago: lo que ocurre es que se pactó que el pago se realizara «en Internet» (= lugar de pago: el *Cyberspace*). Por tanto, el pacto interpartes no sirve, literalmente interpretado, para concretar un «lugar físico» de pago. Así las cosas, hay que entender que las partes han pactado que el pago de precio tenga lugar en el

[65] ***Vid.*** CALVO CARAVACA, **ALFONSO-LUIS** y CARRASCOSA GONZÁLEZ, **JAVIER.** ***Conflictos de leyes y conflictos de jurisdicción... op. cit*****, pág. 153.**

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

país del domicilio o sede del «contratante no pagador». Ello le permitirá litigar en su país, lo que incentivará al pagador a cumplir con el pago si no quiere ser demandado en el extranjero.

Finalmente, señalar que cuando el demandado tiene su domicilio en un tercer Estado, la competencia judicial internacional de los tribunales españoles se rige por la LOPJ. Tales sujetos pueden ser demandados ante tribunales españoles cuando la obligación contractual deba cumplirse en España o la obligación contractual haya «nacido en España».

8. Responsabilidad no contractual, *cloud computing*, y determinación de la ley aplicable.

Teniendo en cuenta que la vulneración del derecho a la protección de datos derivada de la prestación de servicios en la nube genera obligaciones extracontractuales, podríamos pensar que el nuevo instrumento jurídico de origen comunitario: el Reglamento (CE) Nº 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, relativo a la ley aplicable a las obligaciones extracontractuales (en adelante, «Roma II»)[66] podría ser de aplicación. No obstante, no es así ya que los Estados miembros no alcanzaron un acuerdo satisfactorio para todos en torno a esta cuestión (= artículo 30.2 del Reglamento «Roma II»). Tampoco se ha incorporado a nuestro ordenamiento jurídico un convenio internacional de Derecho internacional privado uniforme, ni existe ley específica española, que forme parte de nuestro sistema jurídico.

En consecuencia, la Ley aplicable a las consecuencias jurídicas de la infracción del derecho a la propia imagen se determinará con arreglo al párrafo primero del artículo 10.9 de nuestro Código Civil (= «las obligaciones no contractuales se regirán por la Ley del lugar donde hubiere ocurrido el hecho de que deriven» *–lex loci delicti commissi–*). Dicha ley regulará el tipo de responsabilidad y la extensión de la responsabilidad, la existencia del hecho dañoso y los medios para su reparación, los derechos a ejercitar por el perjudicado, en su caso, los daños indemnizables –patrimoniales y/o no patrimoniales–, la cuantía y las modalidades de la indemnización, así como las personas con derecho a indemnización.[67]

[66] ***DO*** **L 199/40, de 31/07/2007.**
[67] ***Vid.*** **VV. AA., *Lecciones de Derecho Civil Internacional*, Tecnos, Madrid, 1996, pp. 302-303.**

El artículo 10.9 del Código Civil conduce a la aplicación de la Ley del país donde se produce el hecho que genera la responsabilidad extracontractual (= «lugar del hecho dañoso»). El *Locus Damni* (= lugar del daño) será aquél en el que, efectivamente, se difunden las imágenes que suponen la lesión del derecho a la propia imagen.

La *lex loci delicti commissi* plantea problemas si los hechos que presuntamente vulneran el derecho a la protección de datos por *cloud computing* se verifican, como puede ocurrir en la práctica con cierta frecuencia en esta materia, en varios países. En estos casos la solución pasa por la aplicación de la denominada «teoría del mosaico»: el daño sufrido en cada uno se regulará por la Ley del país correspondiente.

Es posible también que la vulneración del derecho a la protección de datos constituya un *ilícito plurilocalizado*, esto es, un ilícito iniciado en un país y concluido en otro país. En este caso, el artículo 10.9 del Código Civil debe interpretarse en sintonía con el mencionado Reglamento «Roma II»; y, debe aplicarse, exclusivamente, la Ley del país donde se verifica el daño (= *Lex Damni*). No debe darse opción a la aplicación de la Ley del país donde se haya verificado el acto inicial o causal. Ahora bien, debe dejarse muy claro que en multitud de supuestos, el acto inicial constituye ya de por sí, un ilícito. En dicho caso, la posible responsabilidad civil derivada de tal acto causal se rige por la ley del país en cuyo territorio tuvo lugar.

La determinación de la ley aplicable en materia de tratamiento de datos de carácter personal a través de la computación en nube supone la aplicación del artículo 2.1 de la LOPD, que transpone el artículo 4 de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Directiva 95/46/CE)[68], y que implica alinearse en alguno de estos dos bandos: el de la liberalización de la circulación de datos automatizados, o el de la protección del derecho a la intimidad de las personas[69]. Así, mientras el artículo 4 de la Directiva 95/46/CE opta por la aplicación de la ley del lugar de residencia del responsable del fichero de datos (no es relevante el lugar de tratamiento de los datos ni la nacionalidad, domicilio o residencia habitual del sujeto cuyos datos se tratan o del sujeto responsable del tratamiento, sino que sólo es relevante el lugar de su establecimiento); el artículo 2.1 de la Ley Orgánica 15/1999, de

[68] ***DOCE*** **núm. L 281, de 23 de noviembre de 1995.**
[69] ***Vid.*****, en el mismo sentido,** ***ibidem*****, pp. 154-155.**

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo, LOPD)[70] opta por la ley del lugar de tratamiento de los datos de carácter personal[71].

La Directiva 95/46/CE opta por el criterio de la residencia del responsable del fichero en la medida en que de esta forma, «[...] 1º) Se evita la aplicación de la regla general en materia de responsabilidad no contractual: no se aplica la *lex loci delicti commissi* o ley del país donde se produce el tratamiento ilícito de los datos [...] 2º) [Se recurre a una argumentación económica que se aleja] de la Ley del país más vinculado al supuesto [, de forma que] la proximidad del supuesto con un país no guía la mano del legislador comunitario a la hora de construir la solución de Derecho internacional privado en esta materia [favoreciendo, así, a las empresas informáticas que operan en este sector por cuatro razones:] 1º) El criterio promueve la actividad internacional de tratamiento de datos en la UE, ya que, sean cuales sean los países en los que la empresa desarrolle sus actividades, la Ley aplicable al tratamiento de datos será siempre la misma, la Ley del fichero [...] 2º) Se trata, además, de una Ley conocida por la empresa [...] 3º) Por otro lado, la empresa que trata los datos queda sometida a un mismo Derecho nacional tanto por lo que respecta a sus relaciones administrativas con las Autoridades públicas, como por lo que se refiere a las relaciones con los particulares afectados por el tratamiento de datos [...] 4º) La norma de conflicto contenida en el artículo 4 [de la] Directiva es una norma de conflicto específica, diseñada para una materia concreta. Por eso, difícilmente admite excepciones o reducciones teleológicas, desviaciones que permitan apartarse del criterio de la aplicación de la Ley de situación del responsable del fichero, lo que sería factible si la norma fuera una norma general o principal. Tampoco el artículo 4 [de la] Directiva se ve corregido por una cláusula de escape o por una cláusula de excepción [...]».

Además, el artículo 4 de la Directiva 95/46/CE concreta el criterio de la ubicación del fichero de datos en dos supuestos especiales que, por su fisonomía, la localización del fichero de datos supone casi misión imposible: a) según el artículo 4.1.a *in fine* de la Directiva, si el responsable del fichero de datos posee distintos establecimientos en diferentes Estados de la UE, el tratamiento de datos realizado «en el marco de las actividades de cada establecimiento» se rige por la Ley del país donde radica cada establecimiento; y, b) en virtud del artículo 4.1.b de la Directiva, en el supuesto de un responsable del tratamiento establecido en un lugar que no

[70] ***BOE* núm. 298, de 14 de diciembre de 1999**

[71] **Nos encontramos ante dos preceptos que, por su contradicción, inducen a la confusión, que cubren tanto las relaciones administrativas como las relaciones entre particulares en asuntos internacionales, y que aparecen preocupadas por fijar el ámbito de aplicación de la normativa del Estado cuyos Tribunales conocen del asunto. *Vid.*, *ibidem*, pp. 156-157.**

pertenece a la UE, pero en el que se aplica la legislación nacional de un Estado miembro en virtud del Derecho internacional público, se aplicará la Directiva 95/46/CE.

En este supuesto, y en virtud de una combinación del artículo 2 de la LOPD y del artículo 4 del Reglamento «Roma II», el tratamiento de datos personales por parte de un responsable cuyo establecimiento se encuentra en un tercer Estado no comunitario se rige por las siguientes Leyes: a) la Ley elegida por las partes; b) en su defecto, se aplicará la Ley del país de residencia habitual común de las partes; c) en su defecto, se aplicará la Ley del país donde se lleve a cabo el tratamiento de datos, sea un Estado miembro o un tercer Estado (= Ley del país de comisión del hecho dañoso); y, d) no obstante, si del conjunto de circunstancias se desprende que el hecho dañoso presenta vínculos manifiestamente más estrechos con otro país distinto, se aplicará la Ley de ese otro país[72]. Ahora bien, si el hecho dañoso se produce en varios países, entonces el perjudicado deberá reclamar con arreglo a cada una de las Leyes de los países en los que su derecho ha sido vulnerado y por los daños allí sufridos.

La Directiva 95/46/CE opta por el criterio de la residencia del responsable del fichero en la medida en que de esta forma, «[...] 1º) Se evita la aplicación de la regla general en materia de responsabilidad no contractual: no se aplica la *lex loci delicti commissi* o ley del país donde se produce el tratamiento ilícito de los datos [...] 2º) [Se recurre a una argumentación económica que se aleja] de la Ley del país más vinculado al supuesto [, de forma que] la proximidad del supuesto con un país no guía la mano del legislador comunitario a la hora de construir la solución de Derecho internacional privado en esta materia [favoreciendo, así, a las empresas informáticas que operan en este sector por cuatro razones:] 1º) El criterio promueve la actividad internacional de tratamiento de datos en la UE, ya que, sean cuales sean los países en los que la empresa desarrolle sus actividades, la Ley aplicable al tratamiento de datos será siempre la misma, la Ley del fichero [...] 2º) Se trata, además, de una Ley conocida por la empresa [...] 3º) Por otro lado, la empresa que trata los datos queda sometida a un mismo Derecho nacional tanto por lo que respecta a sus relaciones administrativas con las Autoridades públicas, como por lo que se refiere a las relaciones con los particulares afectados por el tratamiento de datos [...] 4º) La norma de conflicto contenida en el artículo 4 [de la] Directiva es una norma de conflicto específica, diseñada para una materia concreta. Por eso, difícilmente admite excepciones o reducciones teleológicas, desviaciones que permitan apartarse del criterio de la aplicación de la Ley de situación del responsable del fichero, lo que sería factible si la norma fuera una norma general o principal. Tampoco el artículo 4 [de la]

[72] ***Vid.*** CALVO CARAVACA, **ALFONSO-LUIS** y CARRASCOSA GONZÁLEZ, **JAVIER.** ***Derecho internacional privado.*** **vol. I, Comares, 9ª edición, Granada, 2008, pág. 796.**

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

Directiva se ve corregido por una cláusula de escape o por una cláusula de excepción [...]».

Además, el artículo 4 de la Directiva 95/46/CE concreta el criterio de la ubicación del fichero de datos en dos supuestos especiales que, por su fisionomía, la localización del fichero de datos supone casi misión imposible: a) según el artículo 4.1.a *in fine* de la Directiva, si el responsable del fichero de datos posee distintos establecimientos en diferentes Estados de la UE, el tratamiento de datos realizado *en el marco de las actividades de cada establecimiento* se rige por la Ley del país donde radica cada establecimiento; y, b) en virtud del artículo 4.1.b de la Directiva, en el supuesto de un responsable del tratamiento establecido en un lugar que no pertenece a la UE, pero en el que se aplica la legislación nacional de un Estado miembro en virtud del Derecho internacional público, se aplicará la Directiva 95/46/CE.

El panorama cambiará a partir del próximo mes de mayo de 2018, con la aplicación del Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), de 25-01-2012[73]. Éste fija como primer criterio que su ámbito territorial comprende el tratamiento de datos «en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no» (artículo 3.1). Las innovaciones respecto al texto del artículo 4.1.a) de la Directiva son aquí menores, pues se limitan a que el Reglamento General de Protección de Datos hace referencia expresa no sólo al «responsable» sino también al «encargado» del tratamiento. Por otra parte, se elimina la referencia a las situaciones en las que un mismo responsable del tratamiento esté establecido en varios Estados miembros como circunstancia que llevaba a tener que cumplir con sus respectivas legislaciones, lo que se corresponde con que el Reglamento General de Protección de Datos sustituye a las legislaciones de todos los Estados miembros.

Para garantizar un alto nivel de protección, se mantiene la interpretación muy amplia y flexible del concepto de establecimiento, que se extiende «a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable», como recoge el Considerando 22 del Reglamento General de Protección de Datos. Ahora bien, es necesario que el tratamiento se produzca en el contexto de las actividades del establecimiento.

---

73 ***COM (2012) 11 final.***

No obstante, a día de hoy, con carácter general, para la determinación de la ley aplicable en materia de responsabilidad civil extracontractual, por vulneración del derecho a la protección de datos, en el marco del *cloud computing*, se distinguen dos supuestos: a) cuando el responsable del tratamiento de datos está situado en un Estado miembro de la UE (= *nubes* cuyo propietario tiene su establecimiento en un Estado miembro de la Unión Europea); y, b) cuando el responsable del tratamiento se encuentra en un tercer Estado no comunitario (= *nubes* cuyo propietario tiene su establecimiento en un *tercer país* no comunitario y *nubes* cuyo propietario tiene su establecimiento se encuentra en un "tercer país" no comunitario, pero se utilizan *medios* situados en España). Veamos cada uno de estos supuestos:

8.1 Tratamientos de datos realizados en el marco de las actividades de un responsable del tratamiento establecido en el territorio de la Unión Europea.

Para aquellos tratamientos de datos realizados en el marco de las actividades de un establecimiento de un responsable del tratamiento de un Estado miembro de la UE, se aplicará la Ley de dicho Estado miembro, en virtud del artículo 4 de la Directiva 95/46/CE. Resulta de capital importancia, en este sentido, la consolidación del criterio asentado por el «Grupo de Trabajo del Artículo 29» (= Grupo de trabajo sobre protección de datos creado en virtud del artículo 29 Directiva 95/46/CE), en *su Informe 8/2010 sobre Derecho Aplicable* por medio del cual se pretende aclarar el ámbito de aplicación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995*, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*[74] (y, en particular, del artículo 4, que determina qué legislación nacional de protección de datos conforme a dicha Directiva puede ser aplicable al tratamiento de datos personales en el contexto; p. ej., de bases de datos centralizadas sobre recursos humanos, servicios de geolocalización, *cloud computing*, o redes sociales) según el cual «el elemento decisivo para calificar que en un establecimiento está sometido a la Directiva es el ejerció real y efectivo de actividades, en el contexto de las cuales se traten datos de carácter personal», con independencia de la forma jurídica bajo la que se desarrollen dichas actividades o de los acuerdos privados a los que se pretendan someter[75].

[74] **0836/10/EN WP 179.**

[75] **No siempre existe una única ley aplicable para todas las operaciones de un determinado responsable de tratamiento de datos personales: si el tratamiento se efectuara en varios Estados miembros, porque hubieran varios establecimientos, se tendría que cumplir con la ley de cada uno de ellos.**

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

Además, si el tratamiento es efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento, se aplicará la Ley española (= LOPD), en virtud del mencionado artículo 2.1 de la LOPD. Así, p. ej., se aplicaría la LOPD cuando el tratamiento sea efectuado en territorio español en el marco de actividades de un establecimiento del responsable del tratamiento, o cuando se utilicen medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

8.2 Tratamientos de datos realizados en el marco de las actividades de un responsable del tratamiento establecido fuera del territorio de la Unión Europea.

En cuanto a aquellos responsables del tratamiento no establecidos en el territorio de la UE, sería de aplicación la ley del Estado miembro al que se dirija específicamente sus servicios; como criterio ampliamente consolidado, en España, gracias al artículo 4 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico. Así, p. ej., en el caso de un proveedor de servicios en la nube con establecimiento en EE.UU., pero que utiliza, para determinados tratamientos de datos, servidores ubicados en un Estado miembro de la UE, la ley aplicable a los mismos sería la de dicho Estado miembro; o, en el caso de un cliente de un servicio de computación en nube, y responsable del tratamiento de datos, no establecido en la UE, pero su proveedor de servicios utilice medios o equipos ubicados en un Estado miembro de la UE para prestarle los servicios, se aplicará la ley de dicho Estado miembro.

No obstante, habrá que ver si ese tercer Estado tiene un "nivel de protección equiparable o adecuado". Si lo tiene, se aplicará el régimen general de protección de datos; si no lo tiene (= recursos situados en países terceros sin nivel de protección adecuado) se aplicaría el régimen particular de protección de datos.

En este supuesto, y en virtud de una combinación del artículo 2 de la LOPD y del artículo 4 del Reglamento «Roma II»[76], el tratamiento de datos personales por parte de un responsable cuyo establecimiento se encuentra en un tercer Estado no comunitario se rige por las siguientes Leyes: a) la Ley elegida por las partes; b) en su defecto, se aplicará la Ley del país de residencia habitual común de las partes; c) en su defecto, se aplicará la Ley del país donde se lleve a cabo el tratamiento de datos,

[76] Reglamento (CE) Nº 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, relativo a la ley aplicable a las obligaciones extracontractuales («Roma II»), *DO* L 199/40, de 31/07/2007.

sea un Estado miembro o un tercer Estado (= Ley del país de comisión del hecho dañoso); y, d) no obstante, si del conjunto de circunstancias se desprende que el hecho dañoso presenta vínculos manifiestamente más estrechos con otro país distinto, se aplicará la Ley de ese otro país[77]. Ahora bien, si el hecho dañoso se produce en varios países, entonces el perjudicado deberá reclamar con arreglo a cada una de las Leyes de los países en los que su derecho ha sido vulnerado y por los daños allí sufridos.

Uno de los aspectos más controvertidos de la legislación europea sobre protección de datos personales es el relativo a su ámbito de aplicación espacial; en particular, con respecto a los supuestos en los que el responsable del tratamiento se encuentra establecido en un tercer Estado, lo que es frecuente en el caso de prestación de servicios en la nube. Para garantizar el cumplimiento de la Directiva 95/46/CE cuando el responsable del tratamiento tenga su establecimiento en un Estado tercero, se prevé la aplicación de la ley del Estado miembro en cuyo territorio se encuentren situados los medios –automatizados o no– a los que recurra el responsable para el tratamiento de datos de carácter personal, salvo que los utilice con fines de mero tránsito (= artículos 4.1.c) Directiva 95/46/CE, 2.1.c) LOPD y 3.1.c) RLOPD).

El mencionado Informe 8/2010 hace referencia a algunas áreas de posible mejora con respecto al derecho aplicable al tratamiento de datos personales entre los Estados Miembros de la UE, También pretende establecer una mayor comprensión de la legislación aplicable para garantizar la seguridad jurídica de los controladores de datos y un marco más claro para los individuos y otras partes interesadas en el procesamiento de datos personales, así como garantizar que no existan lagunas o vacíos legales sobre protección de datos personales de conformidad con la interpretación de las disposiciones de la Directiva 95/46. Dicho Informe hace distintas aclaraciones con respecto al establecimiento y ubicación del responsable del tratamiento de datos y el uso de los equipos utilizados por controladores que no estén establecidos en la Unión Europea. Establece algunos criterios que podrían aplicarse cuando el controlador se encuentra establecido fuera de la UE, con el fin de asegurar que exista una conexión suficiente con el territorio de la UE, evitando al mismo tiempo que el territorio de la UE sea utilizado para llevar a cabo actividades de procesamiento ilegal de datos establecidos en terceros países. Entre algunos otros criterios que establece se encuentran: a) la focalización de los individuos, que resulte en la aplicación de la legislación comunitaria de protección de datos cuando las actividades de tratamiento de datos personales sean dirigidas a individuos ubicados en la UE; y, b) la aplicación del criterio de «equipo» en forma residual y limitada que se

[77] ***Vid.*** **CALVO CARAVACA, ALFONSO-LUIS y CARRASCOSA GONZÁLEZ, JAVIER.** ***Derecho internacional privado.*** **vol. I, 9ª edición, Comares, Granada, 2008, pág. 796.**

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

ocuparía de algunos casos (p. ej., la información sobre individuos no pertenecientes a la Unión Europea, o los controladores que no tienen vínculo con la UE), donde exista infraestructura relevante de procesamiento de datos en la UE. La idea, en definitiva, es evitar la exigencia del cumplimiento de la Directiva 95/46/CE en supuestos en los que la conexión con la UE es escasa o «accidental» y su aplicación excesiva.

El aspecto clave es la interpretación del artículo 2.1.c) de la LOPD que incorpora al Derecho español el artículo 4.1.c) de la Directiva 95/46/CE. Cuando el responsable del tratamiento tenga su establecimiento en un tercer Estado, se prevé la aplicación respecto de las actividades de empresas que no están establecidas en un país de la UE de la ley del Estado miembro, en cuyo territorio se encuentren situados los medios a los que recurra esa entidad para el tratamiento de datos personales, salvo que los utilice con fines de mero tránsito. Ahora bien, el significado de la referencia en los artículos 4.1.c) de la Directiva 95/46/CE y del 2.1.c) de la LOPD al término «medios» situados en un país de la UE resulta especialmente controvertido con relación a la prestación de servicios en la nube: habrá que ver si se emplean o no dispositivos para la recogida activa de datos procedentes de la nube.

9. Responsabilidad contractual, *cloud computing*, y determinación de la ley aplicable: el Reglamento «Roma I».

Sin lugar a dudas, uno de los problemas fundamentales que nos podemos encontrar en un contrato de prestación de servicios en la nube es la pugna entre la universalidad de la Red *vs.* compartimentación de las normas estatales. La Red no conoce de fronteras (= la información fluye de un Estado a otro), mientras los ordenamientos jurídicos estatales tienden a establecer el territorio como ámbito de aplicación[78]. De esta forma, debemos establecer algún criterio objetivo que nos permita dotar a la contratación de prestación de servicios en la nube de cierta seguridad jurídica; y, ese no es otro que el Reglamento (CE) Nº 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2000, relativo a la ley aplicable a las obligaciones contractuales (en lo sucesivo, «Roma I»)[79].

El Derecho aplicable a los contratos de prestación de servicios en la nube, se determinará con arreglo al Reglamento «Roma I»: 1º) la Ley elegida por las partes (= artículo 3 del Reglamento «Roma I»), independientemente de que dicha elección

[78] *Vid.* CSA-ES (Cloud Security Alliance- España) – ISMS Forum Spain, *Cloud Compliance Report*, Versión 1 – mayo 2011, pp. 96-97.
[79] *DO* L 177/6, de 04/07/2008.

tenga lugar electrónicamente, mediante intercambio de emails, o a través de una página web interactiva; o, 2º) en defecto de la anterior, la Ley determinada por el artículo 4.1.b) del Reglamento «Roma I» a los contratos de prestación de servicios es la «ley del país donde el prestador del servicio tenga su residencia habitual». No obstante lo anterior, si del conjunto de circunstancias se desprende claramente que el contrato presenta vínculos manifiestamente más estrechos con otro país distinto del indicado en el artículo 4.1 y 4.2 del Reglamento «Roma I», entonces el contrato se regirá por la Ley de este otro país (= artículo 4.3 del Reglamento «Roma I»).

10. Reflexiones finales.

PRIMERA.- Un buen día abres tu correo, y te encuentras algo nuevo: una invitación para unirte a *Facebook, MySpace o Tuenti*. Has oído hablar de ello, parece que la gente se divierte, queda con los colegas, se reencuentra con antiguos amigos... Es por la mañana, no estás para leerte las Condiciones de uso (de las cuales en el momento de ingresar sólo aparece un pequeño fragmento, por cierto), aceptas sin miramientos y ya eres uno más. Cuando quieres acordarte, te dejas llevar por la emoción de saber más y más sobre otros usuarios, porque *éste era vecino mío*, porque *mira mi ex ahora con quién se junta*, porque *si mi madre viera estas fotos, se caía redonda*, etc. No hay control. Quiere haberlo, es cierto, pero no lo hay, el tema de la privacidad está cogido con pinzas de papel, y no se puede hacer mucho para luchar contra ello, salvo informar y formar a los usuarios de las redes sociales de los problemas que acarrea el exponer su intimidad a los cuatro vientos.

El imparable desarrollo tecnológico al que asistimos en los últimos tiempos está poniendo en jaque los criterios tradicionales de garantía de la privacidad y exige una actualización urgente. Uno de nuestros principales desafíos actuales en el marco de la sociedad globalizada y el mundo interconectado, está protagonizado por el constante desarrollo y expansión de sistemas de comunicación que, como las redes sociales, permiten una divulgación de información personal sin precedentes, y ponen a disposición de cualquier persona extraordinarias herramientas para la el uso de información de terceros.

Así las cosa, las relaciones jurídicas en la Sociedad de la Información exigen una unificación y/o armonización normativa de los diferentes países y una *reconstrucción del Derecho internacional privado* a partir de una concepción *discreta y realmente universalista del Derecho internacional privado*, donde los conceptos de soberanía y territorialidad no tienen cabida… en definitiva, ante la realidad actual de

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

las redes sociales de Internet debemos caminar hacia la adaptación, que no hagamos una revolución.

Confiemos en que las iniciativas legislativas en curso y las numerosas recomendaciones, guías de uso y códigos de conducta promovidas, tanto a iniciativa pública como privada, por los distintos países, nos ayuden sobre todo a conocer y maximizar las ventajas que el uso de tales plataformas de comunicación y sus múltiples utilidades nos pueden reportar como usuarios, al tiempo de que nos permitan minimizar los riesgos legales que su uso ilegítimo o inadecuado puede llevar aparejado ya que, en última instancia, como usuarios, somos responsables de nuestros datos... Cuando eres pequeño, te enseñan que si un niño te pregunta ¿quieres ser mi amigo? debes decir que sí. Con las redes sociales de Internet nos ocurre lo mismo, nos cuesta decir que no a alguien que nos invita. Sin embargo, nuestros padres también nos advirtieron otra cosa: *no hables con extraños*…

SEGUNDA.- La *nube* está de moda. Va camino de convertirse en la *panacea* para todo tipo de empresas que quieren tratar cantidades ingentes de información, de forma eficiente y a coste bajo. La previsión del IDC *(International Data Corporation)* de la evolución de las tecnologías *cloud computing* en España es de que en el año 2012 el mercado supere los 1.800 millones de euros, con al menos un 18% de las empresas haciendo uso de estas tecnologías en la modalidad de *cloud software as a service*[80]. El mercado mundial de servicios *Cloud Computing* tuvo en 2009 un valor superior a 17.000 millones de dólares, estando previsto un crecimiento anual superior al 27% durante los siguientes cuatro años, hasta alcanzar los 44.200 millones de dólares en 2013 (IDC), siendo el área de mayor potencial de crecimiento es la de almacenamiento, dentro de la modalidad *cloud infraestructure as a service*[81].

La gran ventaja, *a priori*, de *subirse a la nube* es el ahorro de costes, gracias a las economías de escala de los grandes proveedores: ancho de banda y gestión de *data centers* les resultan más baratos a quienes manejan gran cantidad de datos personales. En todo caso, la computación en nube es un nuevo escenario en el que, en un futuro no muy lejano, vamos a tener que estar, siempre y cuando, seamos capaces de conocer y valorar los riesgos y ventajas que su utilización supone y que, hoy día, no conocemos a ciencia cierta.

---

[80] Al usuario se le ofrece la capacidad de que las aplicaciones que su proveedor le suministra corran en una infraestructura *cloud*, siendo las aplicaciones accesibles a través de, por ejemplo, un navegador web como en el caso del *webmail*, que es posiblemente el ejemplo más representativo, por lo extendido, de este modelo de servicio. El usuario carece de cualquier control sobre la infraestructura o sobre las propias aplicaciones, excepción hecha de las posibles configuraciones de usuario o personalizaciones que se le permitan.

[81] El proveedor ofrece al usuario recursos como capacidad de procesamiento, de almacenamiento, o comunicaciones, que el usuario puede utilizar para ejecutar cualquier tipo de software, desde sistemas operativos hasta aplicaciones.

En mi opinión, el principal problema del *cloud computing* no es la seguridad[82], sino más bien la privacidad y la protección de datos personales[83]: la pérdida de control sobre el tratamiento de la información, las dificultades de encajar jurídicamente y con suficiente agilidad las situaciones de tratamiento de los datos por cuenta de terceros, la problemática derivada de las transferencias internacionales de datos, el respeto al principio de calidad de los datos, la adopción de medidas de seguridad, o la resolución de las controversias derivadas de la vulneración del derecho fundamental a la protección de datos personales en situaciones de multiterritorialidad.[84] Ahora bien, el problema principal radica en que con la *nube* no sabemos dónde están nuestros datos... ¡pueden estar en cualquier parte del mundo!...por lo que hay que preguntarse: *¿seguimos animados a trasladar nuestros datos personales a la nube?*

En un mundo globalizado como el actual, levantar barreras legislativas que impidan el desarrollo de un mercado sin lograr una mejora en la protección de datos, ante un nuevo fenómeno como el *cloud computing*, no tiene sentido. La normativa sobre protección de datos debe evolucionar: simplificarse, propiciar una mayor seguridad, y reforzar su naturaleza preventiva[85].

La complejidad de la nube, en los próximos años, seguramente va a incrementar. El Estado se ha quedado pequeño para afrontar este nuevo desafío jurídico; es más, los casi 200 ordenamientos jurídicos existentes en nuestro mundo actual exigen una solución que ofrezca seguridad jurídica a la hora de resolver un litigio derivado de la prestación de un servicio en la nube; y, esa solución, sin duda alguna, no es otra que el Derecho internacional privado, una disciplina capaz de construir unos principios jurídicos de validez mundial para el *cloud computing*.[86]

---

[82] Si echamos un vistazo a los cortes en servicios de *cloud computing* durante los dos últimos años, veremos que la mayoría son mínimos. Muy pocos *apagones en la nube* han producido pérdidas masivas de datos. Sin embargo, tras examinar la mayoría de estos apagones, está claro que los proveedores de servicios en la *nube* aún están ajustando el método para realizar actualizaciones o estimar cargas en la red a la hora de realizar el mantenimiento. Los resultados proceden de investigaciones realizadas por Mark Williams, un consultor británico sobre *cloud computing*. La duración general de los cortes está basada en las investigaciones de Williams. Éste busca activamente más incidencias de cortes y está pidiendo a los usuarios que le envíen informes con ejemplos de problemas. Williams ha encontrado 23 informas de fallos en *cloud computing*. Google ha tenido 12 cortes. Amazon ha tenido cinco. Según él, Microsoft ha tenido cuatro cortes. Salesforce.com ha tenido dos. La mayoría de los cortes afectaron al correo electrónico, y han sido de poca gravedad.

[83] En el *cloud computing* los datos personales pertenecen «por propiedad» a la empresa (y, «por consentimiento» del usuario), pero pertenecen «por gestión» al prestador del servicio.

[84] *Vid.* MIRALLES, Ramón (2010). «*Cloud computing* y protección de datos». En: «VI Congreso Internet, Derecho y Política. *Cloud Computing*: El Derecho y la Política suben a la Nube» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N. º 11. UOC. [Fecha de consulta: 21/06/2011].
<http://idp.uoc.edu/ojs/index.php/idp/article/view/n11-miralles/n11-miralles-esp>

[85] *Vid.* GARCÍA MEXÍA, PABLO. «Internet y protección de datos. Los desafíos de la revolución digital», en *Diario La Ley*, Nº 7577, Sección Tribuna, 25 febrero 2011, Año XXXII, editorial La Ley, Madrid.

[86] *Vid.* GARCÍA MEXÍA, PABLO. «Cloud computing. Sus implicaciones legales», en *Revista de Derecho y Nuevas Tecnologías*, Nº 23, Año 2010-2, Aranzadi Thomson Reuters, Cizur Menor (Navarra).

Perfiles de las Ciencias Sociales, Vol. 6, Núm. 16, julio-diciembre 2018, México. UJAT. ISSN: 2007-9362

En definitiva, a la espera de futuros cambios normativos, que respondan a los nuevos cambios tecnológicos que representan el *cloud computing*, yo creo que no nos queda otra salida: debemos rendirnos a los avances tecnológicos, mentalizarnos, repetir constantemente: la virtualización es imparable… y, sin duda, *¡debemos irnos a vivir a la nube!*...

Bibliohemerografía

FERNÁNDEZ BURGUEÑO, Pablo, «El peligro de las redes sociales y sus principales consecuencias jurídicas», en Revista Economist & Jurist, nº 131, Año XVII - Junio 2009, pp. 54-58; y, MONSORIU FLOR, Mar, Manual de Redes Sociales en Internet. Creaciones Copyright, Madrid, 2008.

Podemos identificar la Sociedad de la Información como el conjunto de transformaciones sociales y económicas producidas como consecuencia del desarrollo exponencial y convergente de redes y servicios de telecomunicaciones, medios de comunicación y tecnologías de la información. Se trata de conseguir que las nuevas tecnologías se conviertan en herramientas para la creación de una sociedad nueva.

CAMPUZANO, Herminia, Vida privada y datos personales. Madrid, Tecnos, 2000, pág. 20.

PALAO MORENO, «la irrupción en nuestra sociedad de las denominadas Tecnologías de la Información y de la Comunicación, ha traído consigo un importante incremento de los litigios transfronterizos [...] ha fomentado y provocado un notable aumento en las relaciones internacionales de carácter privado y, por lo tanto, de los supuestos en los que pueden surgir controversias con ese carácter».

PALAO MORENO, Guillermo, «Competencia judicial internacional en supuestos de responsabilidad civil en Internet», en PLAZA PENADÉS, Javier, Cuestiones actuales de derecho y Tecnologías de la Información y Comunicación (TICs). Editorial Aranzadi, Cizur Menor (Navarra), 2006, pp. 275-276.

CAMPUZANO, Herminia, Vida privada y datos personales. Madrid, Tecnos, 2000, pág. 19.

LLANEZA GONZÁLEZ, Paloma, *Aplicación práctica de la LSSI-CE*. Bosch, Barcelona, 2003, pág. 161.

CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Derecho internacional privado*. *Vol. II*, 8ª edición, Comares, Granada, 2007, p. 652; y, CALVO

CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Conflictos de leyes y conflictos de jurisdicción en Internet*, Colex, Madrid, 2001, pág. 13.

en sentido amplio, ORTEGA GIMÉNEZ, Alfonso, "Derecho Internacional Privado, Protección de Datos y Redes Sociales de Internet" (Capítulo XI), en RALLO LOMBARTE, Artemi y MARTINEZ MARÍINEZ, Ricard (Coords.), *Derecho y Redes Sociales*, Civitas Thomson Reuters, Cizur Menor (Navarra), 2010, pp. 299-318.