DOI: 10.19135/revista.consinter.00008.12

Artigos Originais

RÉGIMEN JURÍDICO ACTUAL DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES. ESPECIAL REFERENCIA A SU APLICACIÓN EN SERVICIOS DE NUBE PÚBLICA SUSCRITOS POR PEQUEÑOS EMPRESARIOS EUROPEOS Y ESPAÑOLES

CURRENT LEGAL REGIMEN OF INTERNATIONAL TRANSFERS OF PERSONAL DATA. SPECIAL REFERENCE TO ITS APPLICATION IN PUBLIC CLOUD SERVICES SUBSCRIBED BY SMALL EUROPEAN AND SPANISH BUSINESSMEN

Francisca M. Rosselló Rubert[1] – ORCID: https://orcid.org/0000-0002-6143-8220

Resumen

Los servicios de nube pública implican generalmente constantes transferencias internacionales de datos personales, ya que se tratan datos en centros informáticos remotos. Tras la entrada en vigor del nuevo Reglamento Europeo, el cliente empresario que utilice herramientas *cloud* para tratar datos personales se configura como responsable del tratamiento, aunque no siempre tendrá la transparencia y el control deseables sobre los datos personales que migra a la nube. En este trabajo se analizan las garantías establecidas por la normativa actual, europea y española, en materia de transferencias internacionales de datos, y su efectividad práctica en entornos de nube pública.

Palabras clave: Reglamento europeo; Protección de datos; Transferencias internacionales; Privacidad; Nube pública; Pequeña empresa.

Abstract

Public cloud services generally involve constant international transfers of personal data, since data is processed in remote computing centers. After the entry into force of the new European Regulation, the business client that uses cloud tools to process personal data is configured as responsible for the treatment, although it will not always have the desired transparency and control over the personal data that migrates

[1] Profesora Ayudante de Derecho Mercantil. Universitat de les Illes Balears.

to the cloud. This paper analyzes the guarantees established by current European and Spanish regulations regarding international data transfers and this practical effectiveness in public cloud environments.

Keywords: European regulation; Data protection; International transfers; Privacy; Public cloud; Small business.

1 INTRODUCCIÓN[2]

En la actualidad vivimos una revolución digital derivada de Internet y de los servicios de *Cloud Computing* o computación en la "nube"[3]. Delimitar en qué consiste este fenómeno no es sencillo, ya que no existe unanimidad sobre los servicios que abarca y su distinción de otras técnicas informáticas como la Web 2.0[4].

---

[2] El presente trabajo se ha realizado en el marco del Proyecto "*Big data, Cloud Computing* y otros nuevos retos jurídicos planteados por las tecnologías emergentes; en particular, su incidencia en el sector turístico" (DER2015-63595), bajo la dirección de la Catedrática Apol·lònia Martínez Nadal como investigadora principal, financiado por la Dirección General de Investigación, del Ministerio de Economía y Competitividad y desarrollado en la Universitat de les Illes Balears.

[3] No existe unanimidad sobre el concepto técnico del *Cloud Computing*, con lo cual, por lo que respecta a este trabajo, se tomará como referencia la definición adoptada por el *National Institute of Standards and Technology* (NIST), que es la que sigue: "el Cloud Computing es un modelo para proporcionar el acceso, bajo demanda y a través de la red, a un conjunto de recursos compartidos configurables (por ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente suministrados y lanzados al cliente con un sencillo manejo y con mínima interacción con el proveedor"(traducción propia del original en inglés). Asimismo, según el NIST, existen cuatro modelos de implementación de la nube: privada, comunitaria, pública e híbrida, pero al centrar este trabajo en los servicios de nube pública, nos acogeremos a la definición de nube pública aportada por el mismo organismo: "la infraestructura *cloud* se suministra en línea para el público en general. Puede ser propiedad de una organización empresarial, organización académica o entidad pública, o varias de ellas, sobre quienes recaerá la administración y control. Se sustenta gracias a las instalaciones de un proveedor *cloud*" (traducción propia del original en inglés). La nube pública, según el NIST, ofrece al gran público servicios tan populares como el correo electrónico. El NIST actualmente forma parte del Departamento de Comercio de EE.UU. y es un referente mundial dentro del sector de las tecnologías de la información y la comunicación. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST; *Special Publication 800-145. The NIST definition for Cloud Computing* (en línea), 2011. Disponible en: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>. (Fecha de consulta: 5 de marzo de 2019). Para más información sobre el concepto de nube pública y sus características técnicas, nos remitimos a ROSSELLÓ RUBERT, Francisca M., "Cloud Computing. Régimen jurídico para empresarios", 1ª edición, Navarra, 2018, p. 31 a 49.

[4] Por ejemplo, autores como Simon Bradshaw, Ian Walden y Christopher Millard, de la *Queen Mary University of London*, o Michael Gordon y Kathreen Marchesini, de la University of North Carolina, consideran a las redes sociales y al correo electrónico como software como servicio, y, por tanto, servicios de computación en la nube. En el mismo sentido, la norma ISO-IEC 17788:2014 considera las comunicaciones como servicio (es decir, correo electrónico y redes sociales) una "categoría de servicio *cloud* en la cual la capacidad provista al cliente es interacción y colaboración en tiempo real" (traducción propia). Sin embargo, Michael Armbrust y Armando Fox, de la Universidad de Berkeley, consideran que las redes sociales son servicios diferentes a la computación en la nube, aunque se sirven de ella como tecnología de soporte. BRADSHAW, Simon; MILLARD, Christopher; WALDEN, IAN; "Standard contracts for Cloud Computing Services", *Cloud Computing Law*, 1ª edición, Oxford, 2013, p. 41. GORDON, Michael; MARCHESINI, Kathryn; *Examples of Cloud Computing Services* (en línea), 2010. Disponible en: <https://www.unc.edu/courses/2010spring/law/357c/001/cloudcomputing/examples.html>. (Fecha de consulta: 30 de marzo de 2017). ARMBRUST, Michael; FOX, Armando (et al); *Above the Clouds: a Berckeley View of Cloud Computing* (en línea), 2009, p. 8. Disponible en: <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html>. (Fecha de consulta: 14 de marzo de 2019).

A nuestro parecer, existen indicios que permiten indicar que nos encontramos ante un verdadero servicio de nube pública, como por ejemplo la exigencia de autenticación del usuario, que implique la migración y el almacenamiento remoto de datos digitales, que sea razonable implementar su pago por su uso, que ofrezca cierto grado de personalización, que la aplicación informática tenga cierto grado de complejidad y potencia, o que obligue a suscribir condiciones generales[5]. Por ello, consideramos como ejemplos de servicios de nube pública el correo electrónico, el alojamiento externalizado de datos digitales, las bases de datos digitales y otras soluciones que permitan compartir, editar y almacenar datos entre usuarios.

El suscriptor de servicios de nube pública, y especialmente al pequeño empresario que los utiliza para tratar datos personales de terceros, debe ser consciente de ciertos riesgos, tales como la falta de transparencia sobre el funcionamiento interno de la nube, el desconocimiento sobre la ubicación de los centros informáticos donde se almacenan y replican los datos migrados o la existencia de subproveedores, así como los movimientos transfronterizos de datos personales. Todos los factores mencionados pueden provocar vulneraciones de la privacidad, falta de control en las medidas de seguridad o desviaciones del marco jurídico europeo hacia regulaciones de terceros países menos exigentes con la privacidad digital. Por tanto, la suscripción de estos servicios es susceptible de crear potenciales incumplimientos normativos, los cuales devengarán en responsabilidades legales para el pequeño empresario que los suscribe.

En este trabajo, nos centraremos en la regulación de las transferencias internacionales de datos personales y analizaremos la problemática que suelen presentar para pequeño empresario español que suscribe servicios de Cloud *Computing* como herramienta para tratar datos personales de terceros.

2 LA PROBLEMÁTICA DE LA LOCALIZACIÓN FÍSICA DE LOS DATOS PERSONALES EN LA NUBE PÚBLICA

En la prestación de servicios de nube pública se produce una migración de datos que se originan generalmente en los sistemas del cliente, se transmiten a través de una red de comunicaciones (generalmente, Internet) y se almacenan en centros de datos digitales propiedad del proveedor de servicios o de un subproveedor al servicio de este. Como resultado de este flujo constante de información digital entre diferentes centros de procesamiento, nos encontramos con datos personales localizados en ubicaciones múltiples, dispares y simultáneas. Por ello, es habitual que el responsable del tratamiento desconozca la ubicación física de los datos inicialmente transmitidos, en qué lugar o lugares están almacenados o replicados, y a qué destinos están siendo transferidos en cada momento[6]. Tal información no suele facilitarse en los contratos de servicios *cloud* que suscribe el cliente[7]. Exista o no previsión contractual[8], la realidad es

---

5 Al respecto, ROSSELLÓ RUBERT, Francisca M., *Cloud Computing. Régimen* …, op. cit., p. 43 a 49.

6 PUYOL MONTERO, Javier, *Algunas consideraciones sobre Cloud Computing*, 1ª edición, Madrid, 2013, p. 154-155.

7 Algunos grandes proveedores se comprometen por vía contractual a mantener los datos de sus clientes dentro de centros de procesamiento ubicados en determinadas "zonas regionales", restringiendo de este modo la transferencia a países que queden fuera de estas zonas. Por ejemplo, el servicio de *Amazon Web*

que el responsable del tratamiento difícilmente puede conocer la ubicación de sus datos a tiempo real, ni cuantas copias o transferencias de información sensible pueden estar llevándose a cabo, con lo cual existe el riesgo de que los datos acaben en países de destino con un nivel de protección de datos inferior al europeo[9].

No obstante, el principal problema no radica tanto en conocer su ubicación exacta[10], sino en saber quién puede tener acceso a los datos, las garantías y riesgos que ofrece el proceso de transmisión o tránsito; y la legislación aplicable y las autoridades que puedan acceder a esos datos[11]. Debemos ser conscientes de que es el proveedor quien tiene la capacidad y el poder de decisión en cuanto a la provisión de la seguridad de sus propias instalaciones, sistemas y conexiones de red.

Consecuentemente, esta falta de información choca con la obligación del cliente empresario, como responsable del tratamiento, de impedir la transferencia de datos a aquellos países fuera del Espacio Económico Europeo[12] que no cumplan con los requisitos legales comunitarios. Como veremos más adelante, en nuevo Reglamento

---

Services S3 (*Simple Storage Services*), dedicado al almacenamiento de datos (en especial para empresas y profesionales TIC que desarrollen aplicaciones en la nube, distribuyan contenidos o utilicen herramientas de análisis de *Big Data*), permite al suscriptor elegir una región, dentro de la cual los datos se almacenarán de forma redundante en diferentes dispositivos de instalaciones que se encuentran allí localizadas, y desde donde serán accesibles. Los criterios de elección de la región por el cliente pueden basarse en el cumplimiento de requisitos legales, pero también en otros motivos como la reducción de la latencia de acceso a los datos, la consecución de redundancia geográfica que le garantice la recuperación de los datos, o la reducción de costes, dado que algunas zonas son más económicas que otras. En su sitio web se ofrece información sobre las regiones en su sección "Preguntas Más Frecuentes", y el contrato lo recoge en su cláusula 3.2 (en línea). Disponible en: <https://aws.amazon.com/es/s3/faqs/>; y <http://aws.amazon.com/es/agreement/>. (Fecha de consulta: 8 de marzo de 2019). Otros proveedores, sin embargo, no mencionan los lugares de posible ubicación de los datos. Por ejemplo, Google permite visitar virtualmente, a través de su web, algunos de sus centros de datos, su política de privacidad no menciona las diferentes localizaciones físicas en las cuales pueden almacenarse y replicarse los datos de los ciudadanos europeos. Disponible en: <http://www.google.com/intl/es-419/about/datacenters/gallery/#/>; y <https://policies.google.com/privacy>. (Fecha de consulta: 8 de marzo de 2019). Aun lo anterior, Google se halla adherido al marco de protección de datos *Privacy Shield*., y cuenta con las certificaciones oficiales al respecto, como muestra en su sitio oficial, disponible en <https://policies.google.com/privacy/frameworks> y <http://googleforwork.blogspot.com.es/2016/08/Google-adopts-Privacy-Shield.html?m=1>. (Fecha de consulta: 8 de marzo de 2019).

8 Sin embargo, cuando no existe previsión contractual sobre la localización de los datos, el suscriptor empresario responsable del tratamiento debe poder averiguar dónde, cuándo y quién ha almacenado o procesado los datos personales bajo su tutela dentro de la cadena de recursos del proveedor, y en qué condiciones de seguridad. En caso contrario, como afirma la Agencia Española de Protección de Datos, nos encontraremos ante un servicio opaco, carente de transparencia y que no permite al usuario auditar y controlar la información. AEPD, *Guía para clientes que contraten servicios de Cloud Computing* (en línea), p. 10. Disponible en: <https://www.aepd.es/media/guias/guia-cloud-clientes.pdf>. (Fecha de consulta: 8 de marzo de 2019).

9 ALAMILLO DOMINGO, Ignacio, "El control de localización de los datos e informaciones en el Cloud", en *Derecho y Cloud Computing* (coord. Ricard Martínez Martínez), Navarra, 2012, p. 72.

10 Por otra parte, proporcionar al detalle ubicaciones exactas puede redundar en riesgos en la seguridad de los sistemas físicos de los proveedores, haciéndolos más susceptibles a ataques. Por otro lado, la flexibilidad del proveedor para mover y replicar los datos coadyuva a las mayores ventajas en cuanto a precio, disponibilidad y resiliencia de los servicios computación en la nube.

11 Así lo afirmaba el Grupo de Expertos en *Cloud Computing* de la Comisión Europea, en su *Discussion paper on Data Location and Security*, de marzo de 2014, y en su *Discusion Paper Topics to be Covered by the Experts Group* (ambos documentos en línea), de noviembre de 2013. Disponibles en: <https://ec.europa.eu/info/business-economy-euro/doing-business-eu/con tract-rules/cloud-computing/expert-group-cloud-computing-contracts_en>. (Fecha de consulta: 8 de marzo de 2019).

12 El Espacio Económico Europeo integra los 28 países de la Unión Europea más Islandia, Noruega y Liechtenstein.

Europeo permite la transferencia internacional de datos personales a países fuera del EEE únicamente cuando el país o entidad importadores garanticen un nivel adecuado de protección de datos, como veremos en posteriores apartados.

3 LA REGULACIÓN DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

Llegados a este punto, consideramos apropiada una aproximación a la regulación de las transferencias internacionales de datos personales en la legislación actual y su puesta en relación con la prestación de servicios de *Cloud Computing*.

3.1 Contexto general de la regulación de transferencias internacionales de datos personales

Como punto de partida, es destacable el amplio alcance del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)[13], puesto que se aplicará, por una parte, a las actividades de establecimientos de responsables y encargados de la Unión Europea, independientemente de que ese tratamiento tenga lugar o no en la Unión (art. 3.1 RGPD), y, por otra parte, al tratamiento de datos personales de interesados que se encuentren en la Unión, aunque el responsable o el encargado del tratamiento no estén establecidos en la Unión, cuando ese tratamiento esté relacionado con la oferta de bienes o servicios (entre ellos, servicios digitales y servicios *cloud*) a tales interesados, así como en lo referente a mecanismos que controlen su comportamiento (art. 3.2 RGPD)[14].

En cuanto a los derechos de transparencia e información del titular de los datos personales, este debe dar su consentimiento para que puedan efectuarse transferencias internacionales de sus datos personales, y debe informársele de las medidas que garanticen la legalidad de esta transferencia (arts. 13.1.f, 14.1.f y 15.2 RGPD). En el mismo sentido, las remisiones al Reglamento Europeo realizadas por su norma de desarrollo española, la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (arts. 11 y 13 LOPDGDD).

---

[13] Completan el marco jurídico europeo otras normas, como la Directiva 2002/58/CE sobre privacidad y comunicaciones electrónicas (modificada por la Directiva 2009/136/CE o Directiva de *Cookies*), la cual está siendo revisada actualmente mediante la Propuesta de Reglamento sobre la Privacidad y las Comunicaciones Electrónicas (Reglamento *e-Privacy*). Esta normativa se aplica a servicios de comunicaciones electrónicas y de mensajería instantánea, y la Propuesta de Reglamento la adecúa a los avances técnicos del sector y al Reglamento General de Protección de Datos. Existen otras normas europeas en materia de protección de datos, como la Directiva 2016/680 CE, en materia de cooperación policial y judicial, o el Reglamento 2018/1725, relativo al tratamiento de datos personales por las instituciones y organismos comunitarios. Por motivos de extensión de este trabajo, no entraremos en su análisis.

[14] Asimismo, el Reglamento Europeo también se aplicará a tratamientos efectuados por un responsable del tratamiento a quien, en virtud de la aplicación del Derecho Internacional Público, le sea aplicable el Derecho de algún Estado miembro (art. 3.3 RGPD).

El Reglamento Europeo dedica a las transferencias internacionales de datos personales los tres artículos que integran su Capítulo V[15]. El artículo 44 exige el exige el cumplimiento de ciertos requisitos de legalidad a las transferencias internacionales de datos personales. Los obligados al cumplimiento de estos requisitos son el responsable y el encargado del tratamiento, quien debe seguir las instrucciones del responsable (arts. 28.3.a y 29 RGPD). A continuación, se establece un triple régimen aplicable a las transferencias de datos, estableciéndose diferencias en las garantías exigidas. El Reglamento Europeo estima que, con el cumplimiento de las garantías recogidas en este título, no es necesario obtener una autorización específica al respecto (arts. 45.1. 46.2, 47.1 y 49.1 RGPD). En próximos apartados de este trabajo veremos con más detalle este triple régimen de garantías.

Asimismo, las empresas con más de 250 trabajadores, las que efectúen un tratamiento implique riesgos habituales para los derechos y libertades de los interesados o las que traten con datos personales especialmente sensibles (art. 9 RGPD), o condenas e infracciones penales (art. 10 RGPD), deben efectuar la llevanza de un Registro de actividades del tratamiento que recoja las transferencias internacionales efectuadas y, en su caso, las garantías que acredita la legalidad de esa transferencia (art. 30.1.e RGPD), para requerimientos de la autoridad de control competente (art. 30.4 RGPD). Esta obligación recae, concretamente, sobre el responsable del tratamiento y, en su caso, sobre el encargado. En el caso del *Cloud Computing*, implicaría que el responsable debe conocer el funcionamiento interno del servicio. Sin embargo, no todos los proveedores ofrecen ese nivel de transparencia.

Por su parte, la LOPDGDD, en su Título VI (arts. 40 a 43) remite al régimen del Reglamento Europeo en lo referente a transferencias internacionales de datos personales, y determina, como se verá más adelante, la competencia de la autoridad nacional de control (en nuestro caso, la Agencia Española de Protección de Datos o AEPD y las agencias de protección de datos autonómicas) para adoptar cláusulas contractuales tipo y aprobar otras garantías de las transferencias internacionales. Además, para aquellos casos en los que las transferencias no se amparen en una decisión de adecuación de la Comisión Europea o en alguna de las garantías referenciadas por el Reglamento, el responsable del tratamiento deberá obtener una autorización de la autoridad de control competente, estableciendo el artículo 42 de la LOPDGDD el procedimiento para ello.

La LOPDGDD también prevé la posibilidad de crear normas de desarrollo en materia de transferencias internacionales de datos personales (disposición final 15).

---

[15] Ni la anterior Directiva 95/46/CE ni el nuevo Reglamento Europeo aportan una definición de transferencia internacional, como tampoco lo hace la nueva Ley Orgánica de Protección de Datos 3/2018. Del puede deducirse que un exportador de datos transmite información personal a un importador de datos situado fuera del EEE, para que este los trate (lo cual, puesto en relación a sistemas de nube pública, incluye conservarlos o replicarlos) como responsable o por cuenta del responsable. Implicará una salida física de datos fuera del EEE. A mayor abundamiento, aportamos la definición recogida por el derogado Reglamento de desarrollo de la anterior LOPD, en su artículo 5.1.s: "tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español".

3.2 Transferencias basadas en una decisión de adecuación. El Acuerdo *Privacy Shield* con EE. UU.

La Comisión Europea considera que un conjunto de países fuera del EEE queda eximido de autorización específica, al ofrecer un nivel normativo de protección a la privacidad equivalente al europeo[16]. Cabe destacar que la gran mayoría de países no han obtenido este reconocimiento por parte de la Unión Europea, ni tampoco se prevé, en opinión de algunos expertos, que a medio plazo esta lista aumente considerablemente[17].

En el caso de EE. UU., la Comisión Europea únicamente reconoce el nivel adecuado de protección a aquellas empresas y entidades acogidos a los principios de puerto seguro o *Safe Harbor*[18], de acuerdo con la Decisión 2000/520/CE[19] y, tras su anulación por el Tribunal de Justicia de la Unión Europea en 2015, al acuerdo *Privacy Shield* de 2016, cuyas medidas de protección son más reforzadas[20]. Así, esta Decisión no reconoce que todo el territorio estadounidense tenga un nivel de protección con garantías equiparables al sistema europeo, sino que las empresas norteamericanas suscriptoras de los "principios de puerto seguro" se comprometen a mantener ciertas garantías en cuanto al tratamiento de datos personales procedentes de Europa. Actualmente, este acuerdo se revisa de forma anual por el Comité Europeo de Protección de Datos[21].

---

16 Según la Comisión, los siguientes países ofrecen un nivel adecuado de protección en toda su normativa: Suiza, Argentina, Guernesey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, el Principado de Mónaco y Japón, esta última adoptada el 23 de enero de 2019. En el caso de EE. UU y Canadá, únicamente se considerarán transferencias internacionales legales en ciertos casos. Todas las decisiones están disponibles en: <https://ec.europa.eu/info/law/law-topic/ data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>. (Fecha de consulta: 12 de marzo de 2019).

17 GUASCH PORTAS, "La transferencia internacional de datos de carácter personal", *Revista de Derecho UNED*, núm. 11. 2012, p. 413 a 453.

18 La decisión de Canadá también se refiere únicamente a aquellas entidades amparadas por el *Canadian Personal Information Protection and Electronic Documents Act*. Más información en: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protect ion-personal-data-non-eu-countries_en>. (Fecha de consulta: 12 de marzo de 2019).

19 Aunque este sistema ya recibió numerosas críticas desde su aprobación, entre las que destacaban las efectuadas por el Grupo de Trabajo del Art. 29 en su Opinión 4/2000 sobre el nivel de protección que proporcionaban los principios de puerto seguro, siguió utilizándose este sistema por motivos políticos y comerciales. Para más información sobre el anulado acuerdo *Safe Harbor*, nos remitimos a ROSSELLÓ RUBERT, Francisca M, "La transferencia de datos personales entre PYMEs españolas y proveedores norteamericanos de *Cloud Computing* tras la reciente anulación del Acuerdo Safe Harbor por el Tribunal de Justicia de la Unión Europea", *Diario La Ley*, núm. 8725, 2016.

20 En el caso de Canadá, únicamente se reconoce el nivel adecuado de protección a los obligados por la *Personal Information and Electronic Documents Act*. Según su Opinión 2/2001 sobre el nivel adecuado de protección de la ley canadiense *Personal Information and Electronic Documents Act*. El Grupo de Trabajo del Artículo 29 cree que la consideración de la normativa canadiense como adecuada también es susceptible de mejoras.

21 El Comité Europeo de Protección de Datos, anteriormente denominado Grupo de Trabajo del Artículo 29, es un organismo europeo independiente compuesto por representantes de las distintas autoridades de control nacionales de protección de datos. Actualmente está regulado por el RGPD (art. 68 y ss).

3.3 Transferencias mediante otras garantías

Si nos encontramos ante un país sobre el cual la Comisión Europea no ha adoptado decisión alguna sobre su adecuación como destinatario de datos personales de ciudadanos europeos conforme al artículo 45 del Reglamento Europeo, las transferencias que tengan como destino este país pueden efectuarse con otras garantías, entre las que cabe destacar las cláusulas tipo, los códigos de conducta verificados y vinculantes, los certificados de cumplimiento y las normas corporativas vinculantes (arts. 42, 46 y 47 RGPD).

Las cláusulas tipo cumplen la función de contrarrestar, con sus efectos vinculantes entre las partes contractuales, la falta de una normativa suficientemente protectora de la privacidad en el país receptor, incluyendo los elementos esenciales para conseguir el amparo del titular de los datos y los efectos prácticos equivalentes a la cobertura legal que ofrece el Reglamento Europeo. Estas cláusulas se suscriben en el marco de relaciones contractuales entre responsables del tratamiento, entre responsables y encargados, y entre encargados y subencargados del tratamiento. Son competentes para elaborarlas tanto la Comisión Europea como las autoridades de control nacionales, aunque estas últimas deberán ser aprobadas también por la Comisión (art. 93.2 RGPD). En la actualidad, son vigentes ciertas cláusulas tipo anteriores a la entrada en vigor del Reglamento, pero que la Comisión Europea considera que mantienen su validez, por el momento[22]. Además, en los contratos entre responsable y encargado o entre dos encargados, pueden añadirse cláusulas y garantías adicionales que complementen la protección de las cláusulas tipo (considerando 109 RGPD). A pesar de lo anterior, se necesitará autorización expresa de la autoridad de control española (nacional o autonómica, en su caso) cuando las garantías adecuadas se aporten mediante cláusulas contractuales entre responsable y encargado o entre encargado y subencargado que no sean coincidentes con las cláusulas tipo adoptadas por la Comisión (art. 42 LOPDGDD). Las autorizaciones otorgadas por la AEPD antes de la entrada en vigor del nuevo Reglamento siguen siendo válidas.

Otro sistema de garantías previsto por el Reglamento Europeo en su artículo 46 (y por el art. 38 de la LOPDGDD) es la suscripción de códigos de conducta promovidos por asociaciones y otros organismos que representen a un conjunto de responsables o encargados del tratamiento, con la finalidad de conseguir una eficaz aplicación práctica del Reglamento Europeo y de establecer las obligaciones de responsables y encargados conforme a la actividad del sector empresarial involucrado. Están especialmente ideados para sectores de similar actividad, pymes y microempresas (considerando 98 RGPD). Son mecanismos de autorregulación que deben ser aprobados, registrados y publicados por la autoridad de control competente, y sometidos a supervisión por parte de un

[22] En la actualidad, las cláusulas tipo adoptadas por la Comisión Europea que siguen siendo válidas, hasta que sean sustituidas o derogadas, son la Decisión 2001/497/CE, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales entre responsables del tratamiento a un tercer país, la Decisión 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países; y la Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Más información en: <https://www.aepd.es/reglamento/cumplimiento/transferencias-internacionales.html>. (Fecha de consulta: 12 de marzo de 2019).

organismo acreditado también por la autoridad de control (arts. 40 y 41 RGPD). Pueden adherirse a estos códigos de conducta responsables y encargados para llevar a cabo transferencias internacionales legítimas (art. 40.3 y 46 RGPD). Por su parte, el Comité Europeo de Protección de Datos trabaja en unas directrices para la elaboración de estos códigos de conducta[23]. Los códigos de conducta anteriores al Reglamento Europeo deberán modificarse antes del 7 de diciembre de 2019, y la autoridad de control verificará su adaptación al nuevo marco normativo (art. 40.2 RGPD y disposición transitoria 2ª LOPDGDD). Además de otros incentivos[24], la adhesión y cumplimiento de estos códigos de conducta podrán ayudar a demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento (art. 24.3 RGPD).

El Reglamento también promueve la creación de mecanismos de certificación voluntaria en materia de protección de datos, así como sellos y marcas que demuestren el cumplimiento y el sometimiento a controles periódicos de las garantías de seguridad en materia de privacidad (art. 42 y 43 RGPD, y art. 39 LOPDGDD). El Comité Europeo de Protección de Datos ha elaborado también unas directrices para la creación de este tipo de certificaciones[25].

El Grupo de Trabajo del Artículo 29 desarrolló en su momento las llamadas reglas corporativas vinculantes (*Binding Corporate Rules*) como alternativa a los acuerdos *Safe Harbor* (vigentes en aquel momento) y a las cláusulas modelo de la Unión Europea. Se enmarcan en transferencias internacionales de datos personales que tienen lugar dentro de grupos empresariales multinacionales, garantizan el cumplimiento de los principios y el ejercicio de los derechos reconocidos en el actual Reglamento. Son adicionales a las cláusulas contractuales tipo y pueden utilizarse para complementarlas. El Grupo de Trabajo del Artículo 29 elaboró algunos informes que completaban su contenido y procedimiento previo[26], y las adaptaron para extender su uso a encargados del tratamiento[27]. El nuevo Reglamento Europeo pretende fomentar y generalizar la adopción de las BCR dentro de los grupos multinacionales, flexibilizando el proceso de aprobación por las autoridades de control (considerandos 108 y 110, y art. 47 RGPD).

---

[23] Se trata de la versión para consulta pública de las directrices *EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*. Disponible en: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en >. (Fecha de consulta 12 de marzo de 2019).

[24] Más información sobre los códigos de conducta y sus incentivos en el sitio web de la AEPD: <https://www.aepd.es/reglamento/cumplimiento/codigos-de-conducta.html>. (Fecha de consulta: 12 de marzo de 2019).

[25] Estas directrices, tituladas EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679), se encuentran disponibles en inglés en el sitio web del Comité Europeo de Protección de Datos: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en>. (Fecha de consulta: 12 de marzo de 2019).

[26] Concretamente, los siguientes informes del Grupo de Trabajo del Artículo 29: WP 155 (Preguntas más frecuentes sobre *Binding Corporate Rules*), WP 154 (Estructura de las *Binding Corporate Rules*), WP 153 (elementos y principios que deben recoger las *Binding Corporate Rules*), WP 108 (modelo de solicitud de autorización de transferencia internacional basado en *Binding Corporate Rules* dentro del procedimiento coordinado), WP 107 (competencias de las autoridades de control en el procedimiento coordinado de aprobación de las *Binding Corporate Rules*) y WP 74 (Documento sobre la aplicación del artículo 26.2 de la Directiva 95/46/CE a las *Binding Corporate Rules*).

[27] En concreto, estas *Binding Corporate Rules* para encargados se exponen en los Documentos Explicativos sobre las normas corporativas vinculantes para encargados del tratamiento, de abril de 2013 (WP 204) y su versión revisada de mayo de 2015.

3.4 Transferencias internacionales excepcionales

Para ciertos casos especiales (art. 49 RGPD), el Reglamento Europeo establece la legalidad de puntuales transferencias internacionales de datos personales que carecen de decisión de adecuación por parte de la Comisión Europea y de garantías adecuadas conforme a sus artículos 46 y 47. Para que sea aplicable este régimen extraordinario, debe cumplirse alguna de las condiciones exigidas, como la autorización expresa e informada del titular de los datos, o la necesidad de la transferencia para ejecutar un contrato entre el titular de los datos y el responsable del tratamiento, entre otras[28].

Por último, el Reglamento Europeo recoge en su artículo 49.1 *in fine* la posibilidad de que se efectúen transferencias de datos puntuales y con fines de intereses legítimos imperiosos (art. 13 y 14 RGPD)[29].

3.5 Transferencias no autorizadas por el Reglamento Europeo

Si se produce una transferencia internacional de datos personales sin las garantías recogidas en el triple sistema ofrecido por el Reglamento Europeo, y careciendo de la autorización de la autoridad de control en aquellos casos en los que pueda ser exigible, tal transmisión internacional de datos personales se considerará ilegal (art. 44 RGPD y 40 LOPDGDD). Como tal, será sancionada de acuerdo con las normativas nacionales de desarrollo del Reglamento Europeo.

De acuerdo con el régimen sancionador previsto por nuestra LOPDGDD, están sujetos a este régimen los responsables y encargados del tratamiento, estén o no establecidos en la Unión Europea[30]. La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento Europeo se considera una infracción grave (art. 72.l LOPDGDD) y está sancionada con multas administrativas de hasta 20 millones de euros (83.5.c RGPD), y para su determinación, podrán tenerse en cuenta, por parte de las autoridades nacionales de control, circunstancias agravantes o atenuantes de los hechos (art. 76.2 LOPDGDD y 83.2.k RGPD).

---

[28] Atendiendo a la letra del Reglamento Europeo, podría plantearse si un contrato de nube pública destinado al tratamiento de datos personales del interesado en cumplimiento del puede considerarse como excepción a la exigencia de autorización. Interpretamos que no, por su carácter excepcional y por existir otros mecanismos que presentan menos riesgos para la privacidad del interesado, y para evitar posibles abusos de la norma o usos en fraude de ley.

[29] En el caso de España, los responsables o encargados del tratamiento que pretendan realizar una transferencia internacional con base a este fundamento deberán informar previamente a la Agencia Española de Protección de Datos o, en su caso, a la utilidad de control autonómica competente, e informar a los afectados de la transferencia y a los afectados por el interés legítimo imperioso perseguido (art. 43 LOPDGDD). A nuestro parecer, sería necesario determinar el alcance de la expresión "intereses legítimos imperiosos" por parte de la Comisión y/o de las autoridades de control o judiciales competentes, para una mayor seguridad jurídica.

[30] También pueden ser responsables otras entidades, como las entidades de certificación, o las entidades de acreditación de códigos de conducta, en la infracción de sus obligaciones legales (art. 70 LOPDGDD).

4 LAS TRANSFERENCIAS DE DATOS PERSONALES DERIVADAS DE SERVICIOS DE NUBE PÚBLICA

Debido a las particularidades del funcionamiento de la nube pública, la regulación anterior resultaba poco flexible en su aplicación al entorno *cloud*, ya que este contexto no fue tomado en consideración al generarse aquel marco legal[31]. El Reglamento Europeo vigente está ideado para solventar las eventuales carencias de la normativa precedente y para reforzar las garantías de la privacidad digital, lo cual implica un régimen de transferencias internacionales que permita mantener salvaguardados los derechos de los ciudadanos del EEE. A continuación, observaremos las particularidades de la aplicación práctica del marco jurídico actual en el ámbito del *Cloud Computing* y, más concretamente, de las transferencias internacionales de datos personales.

4.1 Los roles de encargado y responsable del tratamiento

El Dictamen 5/2012 sobre el *Cloud Computing* del Grupo de Trabajo del Artículo 29 interpreta que, puesto que el empresario suscriptor de servicios en la nube pública es quien define el propósito del tratamiento y la externalización de todo o parte de este tratamiento, está actuando como responsable del tratamiento, y como tal, debe asumir su parte de responsabilidad y su sujeción a todos los deberes legales[32]. Esta idea se mantiene con el nuevo Reglamento Europeo, puesto que la definición de responsable es, en esencia, la misma que existía con la normativa anterior.

Sin embargo, a pesar de esta categorización genérica del empresario suscriptor de servicios *cloud* como responsable, debe tenerse en cuenta su capacidad de control efectivo sobre el tratamiento, en cuanto sufre una considerable merma desde el momento en el que introduce datos personales de terceros en la nube. Por ello, será sumamente

---

[31] Concretamente, nos referimos a 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, y a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[32] De acuerdo con las definiciones del Reglamento Europeo, en la relación jurídica entre proveedor de servicios de nube pública y cliente profesional que utiliza tales servicios como herramienta para el tratamiento de datos personales de terceros, es este último quien determina la finalidad del tratamiento, y quien decide externalizar ese tratamiento con herramientas en la nube. Por tanto, el cliente de servicios *cloud* asume el rol de responsable del tratamiento, mientras que el proveedor se configura como encargado. Así se afirmó en el Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento" del Grupo de Trabajo del Artículo 29 (en línea), donde se adelantaba la dificultad de distinguir responsabilidades especialmente en entornos en la nube y en servicios de red social: "En el otro extremo han surgido cuestiones nuevas y complejas relacionadas con el uso de la informática distribuida, en particular la "computación en la nube" y la "informática en malla (grid)". Disponibles en: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf>. (Fecha de consulta: 13 de marzo de 2019). Asimismo, para más detalle, nos remitimos a APARICIO VAQUERO, Juan Pablo "Cuestiones de derecho aplicable y responsabilidad de los prestadores de servicios de red social y de sus usuarios", *En torno a la privacidad y la protección de datos en la sociedad de la información* (Coord. Juan Pablo Aparicio, Alfredo Batuecas), Granada, 2015, p. 187 a 231.

necesario, para que pueda seguir considerándosele responsable, que el proveedor le permita cumplir con sus obligaciones legales al respecto, poniendo a su disposición los mecanismos necesarios para facilitar esta labor, y que se someta a sus instrucciones en cuanto al tratamiento de los datos de carácter personal facilitados. Por lo anterior, coincidimos con lo afirmado por el Grupo de Trabajo del Artículo 29: deben matizarse las responsabilidades del cliente de servicios de computación en la nube de acuerdo con su capacidad de control efectivo del tratamiento[33]. Consideramos que el nuevo Reglamento Europeo ha introducido mecanismos complementarios que compensan en gran parte la imposibilidad práctica de control pleno del tratamiento que realiza el proveedor *cloud*, como las evaluaciones de impacto en la protección de datos previas al tratamiento, la adscripción a códigos de conducta vinculantes, o las certificaciones verificadas.

4.2 La importancia del contrato entre proveedor y cliente

Es preciso que el suscriptor de servicios de computación en la nube revise las condiciones contractuales puestas a disposición por el proveedor, para asegurarse la adecuada previsión sobre las finalidades del tratamiento, las transferencias de datos personales y el destino de la información una vez terminada la relación contractual. Muchos de estos extremos suelen encontrarse en anexos *ad hoc*, a modo de políticas de privacidad[34].

---

[33] El Dictamen 1/2010 del Grupo de Trabajo del Artículo 29 reconoce que "El concepto de responsable del tratamiento es autónomo, en el sentido de que debe interpretarse fundamentalmente con arreglo a la legislación comunitaria de protección de datos, y funcional, en el sentido de que su objetivo es asignar responsabilidades en función de la capacidad de influencia de hecho, y, por consiguiente, se basa en un análisis de los hechos más que en un análisis formal". Asimismo, nos sumamos a la opinión de RUBÍ NAVARRETE, cuando propone que las fórmulas alternativas sean jurídicamente vinculantes, permitan a las autoridades de control ejercer sus competencias, y que incorporen opciones que permitan a los titulares de datos ejercer sus derechos y obtener compensaciones en caso de vulnerarse sus garantías. RUBÍ NAVARRETE, Jesús, "El proveedor de *cloud* como encargado del tratamiento", en *Derecho y Cloud Computing*, (Coord. Ricard Martínez), 1ª edición, Navarra, 2012, p. 101.

[34] Estas políticas suelen contener: a) El tipo de información que se requiere para proporcionar los servicios: datos de identificación y facturación del usuario, datos de los contactos que tiene usuario, fotos u otros contenidos migrados, mensajes de correo electrónico, direcciones IP, información sobre dispositivos desde los cuales se realiza el acceso al servicio *cloud*, ubicación física, etc.; b) el modo en el cual se recaban (datos introducidos por el usuario, registros automáticos del servidor, uso de *cookies* o tecnologías similares, etiquetados, monitorizaciones del uso del servicio, etc.), tratan (almacenamiento, procesamiento, tiempo de conservación de la información, realización de copias de seguridad, etc.) y eliminan los datos de carácter personal (borrado a través de sobreescritura, etc.), así como los lugares donde tiene lugar este tratamiento (Estados Unidos, Unión Europea, ubicaciones dispersas globalmente, etc.); c) con quien se comparte o puede compartirse la información obtenida (subproveedores, socios comerciales, filiales, nuevos adquirentes en casos de fusiones o venta de activos, otros usuarios del servicio, autoridades competentes, etc.); d) principios a los cuales se somete el tratamiento (transparencia, confidencialidad, protección de derechos de terceros, etc.) y marcos de regulación de la política de privacidad *(Privacy Shield*, Reglamento Europeo, certificaciones de privacidad, etc.); e) información general sobre seguridad (uso de herramientas de encriptado o autenticación, funciones de navegación segura, etc.), adopción de estándares técnicos, y protocolos de actuación y buenas prácticas ante la detección de vulnerabilidades (alertas, publicaciones o avisos en el sitio web del proveedor, etc,), f) se obtienen las autorizaciones del responsable del tratamiento, o directamente del titular si este es consumidor, para determinados usos y finalidades del tratamiento, también detallados, y se presentan mecanismos para modificar las preferencias de privacidad, acceder a los datos, actualizarlos, modificarlos, controlar con quien se comparten, y, en su caso, ejercer los

Recordemos que es obligación del responsable elegir un encargado o encargados que proporcionen las suficientes garantías (art. 28.1 RGPD). Por ello, puesto que el problema principal radica en la imposibilidad de negociar los contratos de adhesión, el pequeño empresario suscriptor de estos servicios deberá asegurarse, antes de contratar, de que el proveedor elegido le permite asegurar el cumplimiento de la normativa europea y española en materia de protección de datos. Por ello, deberá averiguar, de manera previa a la contratación, algunos extremos que reconozcan la legalidad de las transferencias internacionales, como por ejemplo la localización más o menos precisa de los centros de datos, la suscripción de cláusulas contractuales homólogas a las cláusulas tipo reglamentadas, y otros indicios que permitan asegurar el compromiso del proveedor con el cumplimiento del nuevo marco jurídico europeo. En caso de que el compromiso sobre privacidad no se adecúe a las exigencias legales, el empresario responsable del tratamiento deberá proponer los cambios necesarios al proveedor *cloud*, o sustituir sus servicios por los de otro proveedor más confiable. (tesi).

4.3 El precio real por el servicio *cloud*

En ocasiones, el precio se conforma como uno de los factores determinantes para que un pequeño empresario o profesional contrate un servicio de nube pública, optándose en muchos casos por los servicios más populares o "gratuitos", sin tenerse en cuenta posibles mermas en el rendimiento o en el cumplimiento de la normativa sobre privacidad, y sin que se efectúen una lectura previa y esmerada de las condiciones del servicio[35].

Es sabido que los servicios ofrecidos como "gratuitos", en realidad implican cesiones de datos o de derechos por parte del cliente[36]. Esta cuestión debe tenerse en cuenta por clientes responsables del tratamiento, con el fin de que no se vean mermadas las garantías que le son exigibles en cumplimiento de las normas de privacidad.

Asimismo, debe prestarse especial atención a aquellos contratos en los que aparecen cláusulas de limitación y exención de responsabilidad que puedan ser desproporcionadas. Estos contratos, la mayoría provenientes de proveedores establecidos fuera de las fronteras del EEE, implican en la práctica que el cliente está contratando servicios cuyo proveedor no responderá ante fallos en los sistemas de seguridad, incumplimiento de subproveedores, problemas de acceso al servicio y otros posibles factores que no solo le perjudiquen como cliente del servicio, sino también como responsable del tratamiento. Recordemos que, en principio, al pequeño empresario no se le aplica la normativa sobre cláusulas abusivas, sino que se le presupone un deber de diligencia profesional que incluye la lectura detallada de los contratos que suscribe. Estas limitaciones de responsabilidad del proveedor pueden derivar en problemas si el cliente responsable pretende ejercitar su derecho de repetición, especialmente cuando el proveedor esté establecido fuera del EEE.

---

derechos otorgados legalmente. A modo de ejemplo, las políticas de privacidad de Dropbox o Google (en línea). Disponibles respectivamente en: <https://www.dropbox.com/es_ES/privacy> y <http://www.google.es/intl/es/policies/privacy/>. (Fecha de consulta: 13 de marzo de 2019).

35 Al respecto, ver ROSSELLÓ RUBERT, Fca. M, "Las contraprestaciones no dinerarias en la Propuesta de Directiva sobre suministro de contenidos digitales", *Revista de Derecho Mercantil*, núm. 303, 2017, p. 163 a 190.

36 Para un estudio más detallado, nos remitimos a ROSSELLÓ RUBERT, *Cloud Computing. Régimen* …, op. cit., p. 113 a 116.

4.4 Subcontrataciones realizadas por proveedores de servicios *cloud*

La mayoría de contratos de nube pública implican subcontrataciones y, por tanto, mayor volumen de transferencias internacionales. Si bien la relación jurídica entre responsable y encargado del tratamiento se regirá mediante un contrato *ad hoc* (art. 28.3 RGPD), si existen subcontrataciones en las tareas del tratamiento, las garantías ofrecidas al responsable deberán mantenerse a lo largo de toda la cadena de subencargados, respondiendo ante el responsable el encargado originario (art. 28.4 RGPD).

El Grupo de Trabajo del Artículo 29, en el Dictamen 5/2012 sobre *Cloud Computing*, estableció cláusulas contractuales tipo para la transferencia internacional de datos personales a encargados del tratamiento establecidos en terceros países, introducidas por la Decisión de la Comisión de 5 de febrero de 2010. Mediante estas cláusulas, el subtratamiento se permitía únicamente si existía autorización previa y por escrito del responsable; y si mediaba un acuerdo escrito a través del cual el encargado responda plenamente frente al responsable por la ejecución de las obligaciones del subencargado. Con la actual redacción del Reglamento Europeo, se ha elevado a rango legal parte del contenido de las exigencias reconocidas por esas cláusulas tipo, garantizándose así que la cadena de subcontrataciones no dispersa las obligaciones y responsabilidades en materia de protección de datos.

Por nuestra parte, dudamos de la eficacia de estas garantías en la práctica, dada la dificultad de probar el cumplimiento normativo en cadenas de subcontrataciones que implican a diferentes países. Sería recomendable la entrada de mecanismos complementarios que permitieran al responsable comprobar que el cumplimiento normativo es real, por ejemplo, el sometimiento a certificaciones de cumplimiento, por ahora voluntarias (art. 42.3 RGPD), para darle, como responsable, mayores opciones de control sobre el tratamiento[37].

4.5 Responsabilidad por incumplimiento de obligaciones en materia de privacidad en entornos de nube pública

El grupo de expertos en contratación de la *Cloud Computing Strategy* plantea la posibilidad, por una parte, de habilitar acciones directas del empresario responsable del tratamiento contra el subproveedor *cloud* y, por otra, de que el proveedor *cloud* tuviera que responder por toda la cadena de subcontrataciones ante el cliente[38].

---

[37] Para un tratamiento más exhaustivo sobre las subcontrataciones en el *Cloud Computing*, nos remitimos a ROSSELLÓ RUBERT, *Cloud Computing. Régimen* …, op. cit., p. 300 y ss.

[38] La Comisión Europea, consciente de la problemática que planteaba en sus inicios el *Cloud Computing* en materia contractual y de privacidad, creó en 2012 y en el marco de la Estrategia para el Mercado Digital Europeo, la denominada *Cloud Computing Strategy*, que integraba tres grupos de trabajo: el primero, sobre términos contractuales equitativos; el segundo, sobre regulación de estándares técnicos, y el tercero, sobre colaboración entre industria del sector cloud e instituciones públicas europeas. CLOUD COMPUTING STRATEGY, *Discussion Paper on Subcontracting*, p. 3, (en línea). Disponible en: <https://ec.europa.eu/info/law/law-topic/consumers/consumer-contracts-law_en>. Para más información sobre esta Estrategia, nos remitimos a su sitio web oficial: <https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy>. (Fecha de consulta: 13 de marzo de 2019).

El responsable debe indemnizar cualesquiera daños y perjuicios ocasionados por infracciones en materia de privacidad (art. 82.1 RGPD), e indemnizar al interesado perjudicado, respondiendo el encargado únicamente cuando haya incumplido las instrucciones del responsable o las obligaciones que le impone directamente el Reglamento (art. 82.2 RGPD). Posteriormente, el responsable del tratamiento que haya abonado la indemnización podrá ejercer su derecho de repetición contra otros responsables o encargados que hayan participado en el tratamiento (art. 82.5 RGPD). De todos modos, se prevé que los encargados respondan por los incumplimientos de sus subencargados en materia de protección de datos (art. 28.4 RGPD). Todo lo anterior se aplicará también cuando tengan lugar transferencias internacionales de datos personales ilícitas o dañosas.

En cuanto a las reclamaciones que pretenda interponer el cliente *cloud* pequeño empresario por incumplimientos en materia de seguridad de los datos, será necesario acudir al contrato suscrito y comprobar las responsabilidades asumidas por responsable, encargado y, en su caso, subencargado. Para prever las consecuencias derivadas del eventual incumplimiento, es importante que el pequeño empresario averigüe con qué mecanismos de prueba cuenta, las posibles acciones que puede interponer contra el proveedor incumplidor en base al incumplimiento contractual, y qué autoridades son competentes para conocer del caso.

CONCLUSIONES

Los servicios de nube pública implican generalmente transferencias internacionales de datos personales, derivadas del almacenamiento y replicado remotos. A su vez, si el proveedor subcontrata parte del servicio, se genera un movimiento multinacional de datos digitales que dificulta el control de las garantías en materia de privacidad. En la práctica del *Cloud Computing*, el cumplimiento absoluto de obligaciones del pequeño empresario responsable del tratamiento que están relacionadas con la supervisión al encargado resultan complicadas, ya que aquel suele desconocer el funcionamiento interno del servicio *cloud*, y carece de posibilidades reales de auditar el cumplimiento normativo.

Sobre la nueva regulación europea, consideramos que incluye muchas mejoras respecto de la normativa anterior, y que supone un gran paso hacia una mejor protección de la privacidad digital. Es especialmente aplaudible la propuesta medidas proactivas como la protección de datos desde el diseño y por defecto o la concienciación de la necesidad de realizar evaluaciones de los riesgos que pueden derivarse de un tratamiento aparentemente sencillo de datos personales, incentivando a sectores específicos de actividad para que adopten medidas (como códigos de conducta y certificaciones adoptados por responsables, encargados y subencargados) y garantizando en última instancia los derechos exigibles y las acciones legales efectivas de los interesados (art. 46.1 RGPD).

Como conclusión, opinamos que la entrada en vigor del nuevo marco jurídico europeo facilitará el tráfico internacional y garante de datos personales que tengan lugar entre clientes *cloud* responsables del tratamiento y proveedores *cloud* encargados del tratamiento, o entre encargados y subencargados. Estas transferencias transfronterizas serán legitimadas mediante decisiones de la Comisión (como el acuerdo *Privacy Shield* y

la adscripción a este por parte de los proveedores *cloud* destinatarios de los datos), la suscripción de garantías contractuales (cláusulas tipo o autorizadas por las autoridades de control, normas corporativas vinculantes…), o voluntarias (códigos de conducta o mecanismos de certificación). No obstante, el pequeño empresario responsable del tratamiento debe constatar siempre la adecuación del proveedor elegido al cumplimiento legal del marco europeo. Es recomendable decantarse, preferentemente, por proveedores cuyos centros de datos se hallen ubicados en el EEE, o, en su defecto, que presenten las garantías reglamentadas.

Aun lo anterior, y siempre encaminados hacia la búsqueda de mejoras, nos adherimos a lo manifestado por GUASCH PORTAS y SOLER FUENSANTA: "hay que ser conscientes de que la existencia de estos instrumentos para garantizar la legalidad de las transferencias internacionales en el ámbito de la computación en nube no elimina las dificultades de su implantación en muchos casos reales. Deberán surgir nuevas herramientas en el futuro para facilitar todavía más el cumplimiento de las normas sobre protección de datos, tanto por parte del cliente como por parte del proveedor de servicios"[39].

BIBLIOGRAFÍA

ALAMILLO DOMINGO, Ignacio, "El control de localización de los datos e informaciones en el Cloud", en *Derecho y Cloud Computing* (Coord. Ricard Martínez Martínez), 2012, Navarra, p. 63 a 86.

ÁLVAREZ HERNANDO, Javier, "Acceso a datos por cuenta de terceros. El encargado del tratamiento y su régimen jurídico. Servicios de Cloud Computing", en *Grandes Tratados. Prácticum Protección de datos*, 1ª Edición, Navarra, 2018, p. 167-204.

ALVAREZ RIGAUDIAS, Cecilia, "Condiciones para las transferencias internacionales de datos personales en servicios Cloud", en *Derecho y Cloud Computing* (Coord. Ricard Martínez Martínez), 2012, Navarra.

APARICIO VAQUERO, Juan Pablo "Cuestiones de derecho aplicable y responsabilidad de los prestadores de servicios de red social y de sus usuarios", *En torno a la privacidad y la protección de datos en la sociedad de la información* (Coord. Juan Pablo Aparicio, Alfredo Batuecas), Granada, 2015, p. 187 a 231.

AREITIO BERTOLÍN, Javier, *Protección del Cloud Computing en Seguridad y privacidad,* Revista Española de Electrónica, nº 666, 2010, págs 42-48.

[39] GUASCH PORTAS, Vicente; SOLER FUENSANTA, Juan Ramón; "*Cloud Computing*, cláusulas contractuales y reglas corporativas vinculantes", Revista de Derecho UNED, núm. 14, 2014, p. 247 a 269.

ARMBRUST, Michael; FOX, Armando (et al); *Above the Clouds: a Berckeley View of Cloud Computing* (en línea), 2009. Disponible en: <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/ EECS-2009-28.html>. (Fecha de consulta: 14 de marzo de 2019).

BRADSHAW, Simon; MILLARD, Christopher; WALDEN, IAN, "Standard contracts for Cloud Computing Services", *Cloud Computing Law,* 1ª edición, Oxford, 2013, p. 37 a 72.

COTINO HUESO, Lorenzo, "Algunas cuestiones clave de protección de datos en la nube. Hacia una regulación nebulosa", *Revista catalana de dret públic*, núm. 51, 2015, p. 86 a 103.

FERNÁNDEZ ALLER, Cecilia, "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (*cloud computing*)". *Revista de derecho UNED,* núm. 10, 2012, p. 125 a 145.

GARCÍA SÁNCHEZ, Manuel, "Retos de la computación en la nube", en *Derecho y Cloud Computing*. (Coord.: Ricard Martínez Martínez), 1ª edición, Navarra, 2012, p. 37 a 60.

GORDON, Michael; MARCHESINI, Kathryn; *Examples of Cloud Computing Services* (en línea), 2010. Disponible en: <https://www.unc.edu/courses/2010spring/law/ 357c/001/cloudcomputing/exam ples.html>. (Fecha de consulta: 8 de julio de 2016).

GUASCH PORTAS, Vicente; SOLER FUENSANTA, Juan Ramón; "*Cloud Computing*, cláusulas contractuales y reglas corporativas vinculantes", Revista de Derecho UNED, núm. 14, 2014, p. 247 a 269.

GUASCH PORTAS, Vicente, *La transferencia internacional de datos en las normativas española y comunitaria,* 1ª edición, Madrid, 2014, 336 p.

GUASCH PORTAS, "La transferencia internacional de datos de carácter personal", *Revista de Derecho UNED*, núm. 11. 2012, p. 413 a 453.

MARCHINI, Renzo; *Cloud Computing: a practical introduction to the legal issues*, 1ª edición, Londres, 2010, 179 p.

MARZO PORTERA, Ana María, "Privacidad y Cloud Computing, hacia dónde camina Europa", *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*, Volumen I, Número 8, 2012, p. 202-229.

MIRALLES, Ramón, "Cloud Computing y protección de datos*"* (en línea), *Revista de Internet Derecho y Política de la Universitat Oberta de Catalunya*, núm. 11, 2010. Disponible en: <http://idp.uoc.edu/index.php/idp/issue/view/n11>. (Fecha de consulta: 19 de marzo de 2019).

NAVAS NAVARRO, Susana, "Computación en la nube: Big Data y Protección de Datos Personales" (en línea), *InDret Revista para el análisis del Derecho*, núm. 4/2015, 2015. Disponible en: <http://www.indret.com/pdf/1193_es.pdf>. (Fecha de consulta: 19 de marzo de 2019).

PUYOL MONTERO, Javier, *Algunas consideraciones sobre Cloud Computing*, 1ª edición, Madrid, 2013, 276 p.

ROSSELLÓ RUBERT, Francisca M., *Cloud Computing. Régimen jurídico para empresarios*, 1ª edición, Navarra, 2018, 444 p.

ROSSELLÓ RUBERT, Fca. M, "Las contraprestaciones no dinerarias en la Propuesta de Directiva sobre suministro de contenidos digitales", *Revista de Derecho Mercantil*, núm. 303, 2017, p. 163 a 190.

ROSSELLÓ RUBERT, Francisca Mª; "La transferencia de datos personales entre PYMEs españolas y proveedores norteamericanos de *Cloud Computing* tras la reciente anulación del Acuerdo *Safe Harbor* por el Tribunal de Justicia de la Unión Europea", *Diario La Ley*, núm. 8725, 2016.

RUBÍ NAVARRETE, Jesús, "El proveedor de *cloud* como encargado del tratamiento", *Derecho y Cloud Computing*, (coord. Ricard Martínez), Navarra, 2012, p. 87 a 108.

SAIZ PEÑA, Carlos A, "Medidas de seguridad en el Cloud Computing", *Derecho y Cloud Computing* (coord. Ricard Martínez), 2012, Navarra, p. 171.

TRONCOSO REIGADA, Antonio, "Las redes sociales a la luz de la propuesta de Reglamento General de Protección de Datos Personales. Parte dos", *Revista d'Internet, Dret i Política*, núm. 16. 2013, p. 27 a 39.

WINKLER, Matteo M, MOSCA, Jacopo, "Cloud Computing e Protezioni dei dati personali" (coord. M. Fumagalli Meraviglia), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica e scontro di civiltà?*, Nápoles, 2015.