LA COMPUTACIÓN EN NUBE Y LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN EL NUEVO REGLAMENTO DE LA UE[1]

CLOUD COMPUTING AND INTERNATIONAL DATA TRANSFERS IN THE NEW EU REGULATION

Vicente Guasch Portas

Profesor de la Escuela Universitaria de Turismo del Consell Insular de Ibiza

Resumen: La computación en nube supone una gran revolución tecnológica en la actualidad. El usuario de este servicio deja de tener los datos en sus equipos informáticos, pasando a almacenarlos el proveedor del servicio o alguien que ha subcontratado dicha labor. En ocasiones, la cadena de subcontrataciones es amplia. Los datos del cliente pueden estar moviéndose entre distintos países, algunos de ellos con protección adecuada de los datos personales, pero otros que no disponen de esta protección adecuada. Aparecen en este caso las transferencias internacionales de datos. Para que estas se puedan efectuar de forma legal, se deben cumplir una serie de obligaciones. Veremos que la normativa actual en materia de protección de datos padece de una rigidez que desincentiva su cumplimiento. Cuando entre en vigor el nuevo Reglamento europeo de protección de datos, se verán facilitadas todas las transferencias internacionales, incluidas las que se producen en los servicios de computación en nube.

[1] El presente trabajo se ha elaborado 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-R MINECO/FEDER), Investigadora Principal: Apol·lònia Martínez Nadal, financiado por la Dirección General de Investigación, del Ministerio de Economía y Competitividad del Gobierno de España.

Palabras clave: computación en nube, transferencia internacional, protección adecuada, cláusulas contractuales, normas corporativas vinculantes.

Abstract: Cloud computing is a major technological revolution today. The user of this service ceases to have the data in their computer equipment, to be stored by the service provider or someone who has subcontracted the work. Sometimes the subcontracting chain is wide. Customer data may be moving between different countries, some of them with adequate protection of personal data, but others that do not have this adequate protection. International data transfers appear in this case. In order for these to be legally enforceable, a number of obligations must be fulfilled. We will see that the current rules on data protection suffer from a rigidity that discourages compliance. When the new European Data Protection Regulation comes into force, all international transfers, including those occurring in cloud computing services, will be facilitated.

Keywords: cloud computing, international transfer, adequate protection, contractual clauses, binding corporate rules.

Recepción original: 09/02/2017
Aceptación original: 29/03/2017

I. LA COMPUTACIÓN EN NUBE

La computación en nube es una de las grandes revoluciones tecnológicas que se están produciendo en la actualidad. Consta de una serie de tecnologías y modelos de servicio que se centran en el uso de Internet y la prestación de aplicaciones informáticas, capacidad de tratamiento, espacio de memoria y almacenamiento.

La computación en nube puede generar importantes beneficios económicos, ya que los recursos a la carta pueden configurarse, ampliarse y ser accesibles fácilmente en Internet.

A pesar de las claras ventajas de la computación en nube, su despliegue a gran escala puede provocar diversos riesgos para la protección de datos, principalmente la falta de control sobre los datos personales, así como la insuficiente información en relación a cómo, dónde y por quién son tratados o subtratados los datos.

A la hora de contratar los servicios de computación en nube deberán evaluarse los riesgos que se asumen. Así por ejemplo, la falta de transparencia de una cadena de externalización compuesta por múltiples encargados del tratamiento y subcontratistas, y la incertidumbre con respecto a la admisibilidad de la transferencia de datos personales a los proveedores establecidos fuera del Espacio Económico Europeo.

El cliente que contrata servicios de computación en nube deberá verificar si el proveedor de tales servicios puede garantizar la legalidad de las transferencias internacionales de datos.

De las dos partes del contrato de servicios de computación en nube, cliente y proveedor de servicios, es el cliente quien es responsable y está sujeto a todas las obligaciones legales en materia de protección de datos. El GT 29 en su documento de trabajo WP 196[2] entiende que el cliente determina el objetivo último del tratamiento y decide sobre la externalización de este tratamiento y la delegación de la totalidad o de parte de las actividades de tratamiento a una organización externa. El cliente actúa por tanto como responsable del tratamiento.

El Reglamento General de Protección de Datos[3] (en adelante RGPD), en su art. 4.7 define al responsable del tratamiento como aquella persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

[2] Grupo de Protección de Datos del artículo 29 de la Directiva 95/46/CE, en su documento de trabajo WP 196, «Dictamen 05/2012 sobre la computación en nube», adoptado el uno de julio de 2012. Disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf.

[3] Reglamento (UE) 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). Será aplicable a partir del 25 de mayo de 2018. Publicado en el DOUE L 119, de cuatro de mayo de 2016.

El cliente, como responsable del tratamiento, debe aceptar la responsabilidad de respetar la legislación sobre protección de datos.

El proveedor del servicio es la entidad que presta los servicios de computación en nube. Cuando suministra los medios y la plataforma, actuando en nombre del cliente, se considera que es el encargado del tratamiento. Es decir, con arreglo al art. 4.8 del RGPD, la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

A pesar de que se asigna la responsabilidad al usuario que contrata los servicios, los clientes de estos servicios pueden no tener margen de maniobra a la hora de negociar las condiciones de uso de los mismos, ya que las ofertas normalizadas son una característica general en las ofertas de computación en nube.

No obstante, en última instancia, es el cliente quien decide sobre la asignación de parte o de la totalidad de las operaciones de tratamiento a los servicios en nube con fines específicos.

El proveedor de estos servicios actuará de contratista frente al cliente, que es el punto clave en este caso. Tal como se recoge en el Dictamen 1/2010 del GT 29[4], el desequilibrio en cuanto al poder contractual entre un pequeño responsable del tratamiento y un gran proveedor de servicios no debería considerarse una justificación para que el primero acepte cláusulas y condiciones de contratos que no se ajusten a la legislación en materia de protección de datos. Por esta razón, el responsable del tratamiento (el cliente) debe elegir un proveedor que garantice el cumplimiento de la legislación sobre protección de datos.

Pero el cumplimiento normativo no siempre es sencillo. La computación en nube se basa a menudo en la total falta de ubicación estable de los datos en la red del proveedor. Los datos pueden encontrarse ahora en un centro de datos y en el otro lado del mundo unas horas más tarde. El cliente rara vez se encuentra en posición de saber en cualquier momento en qué lugar están situados, almacenados o transferidos los datos. Y es aquí donde entran en juego los instrumentos jurídicos que regulan las transferencias de datos a terceros países, especialmente en el caso de que estos no ofrezcan una protección adecuada.

[4] Grupo de Protección de Datos del artículo 29 de la Directiva 95/46/CE, en su documento de trabajo WP 169, «Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»», adoptado el 16 de febrero de 2010. Disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_es.pdf

II. LAS TRANSFERENCIAS INTERNACIONALES EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Como señala el considerando 101 del RGPD, los flujos transfronterizos de datos personales a, y desde países no pertenecientes a la Unión, son necesarios para la expansión del comercio y la cooperación internacionales. Pero el aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. La transferencia de datos a destinatarios en terceros países no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión Europea.

Las transferencias internacionales se regulan en el capítulo V del RGPD, si bien no encontramos en esta norma una definición de lo que se entiende como transferencia internacional de datos. Podemos recurrir al todavía vigente RLOPD[5], en su art. 5.1.s, para entender dicho concepto: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo[6], 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.

Por lo tanto, la transmisión de datos entre países del Espacio Económico Europeo no tiene la consideración de transferencia internacional.

II.A Transferencias internacionales a países con nivel de protección adecuado

De acuerdo al art. 45 del RGPD, podrán realizarse transferencias de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado[7].

[5] Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal. Real Decreto 1720/2007, de 21 de diciembre. BOE de 19 de enero de 2008.

[6] Son miembros del Espacio Económico Europeo los 28 países integrantes de la Unión Europea y Noruega, Islandia y Liechtenstein. Estos tres países forman parte de la Asociación Europea de Libre Comercio (EFTA). Suiza, que también es miembro de la EFTA, rechazó entrar a formar parte del Espacio Económico Europeo.

[7] No se puede exigir a los países que no forman parte del Espacio Económico Europeo una normativa en materia de protección de datos idéntica a la europea. Como

El contenido del art. 45 se puede comparar con el que se recoge en el art. 2.1 del protocolo adicional al Convenio 108 del Consejo de Europa[8]: «Cada Parte dispondrá que la transferencia de datos de carácter personal hacia un destinatario sometido a la jurisdicción de un Estado u organización que no sea Parte en el Convenio sólo podrá efectuarse si dicho Estado u organización garantiza un nivel de protección adecuado a la transferencia de datos prevista».

La Comisión, tras haber evaluado la adecuación del nivel de protección en base a los criterios estipulados en el propio RGPD, puede decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado. Estas decisiones tendrán efecto para toda la Unión Europea[9].

Las decisiones adoptadas por la Comisión en virtud del art. 25.6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una nueva decisión de la Comisión. A día de hoy, han sido declarados como países con nivel adecuado de protección los siguientes[10]:

— Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000.

— Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.

— Argentina. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003.

---

señala el considerando 104 del RGPD, «el tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión».

[8] Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos, del Consejo de Europa. Ratificado por la mayor parte de los países de Europa, junto con algunos países no europeos. Texto disponible en la web http://conventions.coe.int/.

[9] Según el considerando 103 del RGPD, «La Comisión puede decidir, con efectos para toda la Unión, que un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional ofrece un nivel de protección de datos adecuado, aportando de esta forma en toda la Unión seguridad y uniformidad jurídicas en lo que se refiere al tercer país u organización internacional que se considera ofrece tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin que se requiera obtener otro tipo de autorización».

[10] El artículo 45.8 del RGPD dictamina que «La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado».

— Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.
— Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.
— Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008.
— Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010.
— Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010.
— Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011.
— Uruguay. Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012.
— Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.
— Estados Unidos. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE. UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016.

Como señala el art. 45.1 del RGPD, las transferencias basadas en una decisión de adecuación no requerirán ninguna autorización específica.

II.B Transferencias internacionales a países que no ofrecen un nivel equiparable de protección

Para el caso de transferencias a territorios que no han obtenido la declaración de nivel adecuado de protección por parte de la Comisión, el art. 46 del RGPD contempla la posibilidad de llevarlas a cabo en base a garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas[11].

Las garantías adecuadas permitirán las transferencias sin que se requiera ninguna autorización expresa de una autoridad de control. Podrán consistir en:

[11] Así lo señala también el considerando 108 del RGPD: «En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado».

a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) normas corporativas vinculantes;

c) cláusulas tipo de protección de datos adoptadas por la Comisión;

d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión;

e) un código de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados, o

f) un mecanismo de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados.

Además, siempre que exista autorización de la autoridad de control competente, podrán ser aportadas las garantías adecuadas siguientes:

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

II.B.1 Las normas corporativas vinculantes

En el art. 4 del RGPD se definen las normas corporativas vinculantes como aquellas políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

Todo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta debe tener la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo

empresarial o unión de empresas dedicadas a una actividad económica conjunta, siempre que tales normas corporativas incorporen todos los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal.

El RGPD quiere dar un gran impulso a las normas corporativas vinculantes (NCV), en inglés *binding corporate rules* (BCR). Las BCR no se encontraban recogidas en la Directiva 95/46/CE, y su regulación surgió en base a una serie de Documentos de Trabajo[12] elaborados por el GT 29:

a) En caso de NCV para responsables:

WP 155 - Preguntas más frecuentes sobre BCRs.

WP 154 - Cuadro que establece la estructura de las BCRs.

WP 153 - Cuadro que establece la relación de los elementos y principios que deben contener las BCRs.

WP 108 - Modelo de solicitud de autorización de transferencia internacional basada en BCRs en el ámbito del procedimiento coordinado.

WP 107 - Documento sobre la competencia de las Autoridades de Control europeas en el procedimiento coordinado de aprobación las BCRs.

WP- 74 - Documento sobre la aplicación del artículo 26.2 de la Directiva 95/46/CE a las BCRs.

b) En caso de NCV para encargados:

WP 204 - Documento explicativo sobre las BCRs para encargados.

WP 195a - Recomendación sobre el formulario de solicitud estándar para la aprobación de BCRs para la transferencia de datos personales para encargados.

WP 195 - Tabla con los elementos y principios que se encuentran en las BCRs para encargados.

De acuerdo al art. 47.1 del RGPD, la autoridad de control competente podrá aprobar normas corporativas vinculantes, siempre que estas:

[12] Pueden consultarse todos los Documentos de Trabajo del GT 29 en la siguiente dirección: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan la amplia relación de requisitos establecidos en el art. 47.2.

II.B.2 Las cláusulas contractuales tipo adoptadas por la comisión

Podrán llevarse a cabo transferencias internacionales de datos a territorios que no han obtenido la declaración de nivel adecuado de protección, en base a un contrato celebrado entre el exportador y el importador de datos. En dicho contrato deben constar las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales, además de garantizarse el ejercicio de los respectivos derechos.

Las cláusulas contractuales tipo adoptadas a día de hoy por la Comisión, regulan dos tipos de transferencias:

a) Transferencias Internacionales de datos entre responsables de tratamiento.

Para este tipo de transferencias se considera que reúnen las garantías adecuadas los contratos celebrados en los términos previstos en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de junio de 2001, y 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la anterior. Cada una de estas Decisiones contiene un conjunto de cláusulas contractuales tipo. Los responsables del tratamiento podrán optar por uno u otro conjunto de cláusulas, pero no podrán modificarlas ni combinar elementos de distintas cláusulas ni de los conjuntos.

b) Transferencias Internacionales de datos de responsable a encargado del tratamiento.

Cuando la transferencia de datos se realice entre un responsable y un encargado del tratamiento se considera que reúnen las garantías adecuadas los contratos que incluyan las cláusulas contractuales tipo establecidas en la Decisión de la Comisión Europea 2010/87/UE, de 5 de febrero de 2010.

La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos no debe obstar a que se incluyan las cláusulas tipo en un contrato más amplio, como un contrato entre dos encargados, o a que añadan otras cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo, ni mermen los derechos o las libertades fundamentales de los interesados[13].

II.B.3 Las cláusulas contractuales tipo adoptadas por una autoridad de control y aprobadas por la comisión

Si bien no han sido aprobadas por la Comisión, a día de hoy contamos en España con las cláusulas adoptadas por la AEPD para el caso de las transferencias internacionales de datos de encargado a subencargado del tratamiento. Es decir entre un encargado del tratamiento/exportador de datos, establecido en España, y un subencargado del tratamiento/importador de datos, ubicado en un país que no garantiza un nivel adecuado de protección.

Estas cláusulas tipo fueron adoptadas por la Agencia Española de Protección de Datos en su resolución de Autorización de Transferencia Internacional de Datos de 16 de octubre de 2012.

Además del contrato entre el encargado del tratamiento/exportador de los datos e importador/subencargado del tratamiento, se requiere otro contrato marco entre el responsable del tratamiento y el encargado del tratamiento/exportador de datos en el que aquél autorice la subcontratación y la transferencia internacional de datos.

II.B.4 Otras cláusulas contractuales

El art. 46.3.a) del RGPD hace referencia a «cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional». Se trata de cláusulas distintas a las adoptadas por la Comisión o por una autoridad de control.

Estas cláusulas podrán ser redactadas de acuerdo a la voluntad de las dos partes del contrato: exportador e importador de datos. Pero en este caso la autoridad de control competente deberá dar su autorización.

[13] Así lo manifiesta el considerando 109 del RGPD.

En la práctica, parece que será un instrumento minoritario. Las cláusulas contractuales tipo pueden ser usadas sin autorización expresa de ninguna autoridad de control. En cambio, el uso de otras cláusulas distintas requiere de su aceptación, con el trámite y coste que ello supone. Es previsible que solo en muy contadas ocasiones se optará por esta solución más cara y compleja.

II.B.5 Códigos de conducta y mecanismos de certificación

Desconocemos si las figuras contempladas en los apartados e) y f) del art. 46.2 podrán ocupar un espacio en las transferencias efectuadas mediante garantías adecuadas. Son los códigos de conducta y los mecanismos de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados.

Si en un futuro estas herramientas se desarrollasen, podrían aportar una nueva vía para poder efectuar transferencias internacionales de datos a aquellos países que no ofrecen un nivel equiparable de protección.

II.C Excepciones para situaciones específicas

En ausencia de una decisión de adecuación o de garantías adecuadas, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones del art. 49.1 del RGPD:

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;

d) la transferencia sea necesaria por razones importantes de interés público;

e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

En el caso de que no sea aplicable ninguna de las excepciones arriba indicadas, solo se podrá llevar a cabo la transferencia si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. Como señala el considerando 113 del RGPD, «dichas transferencias sólo deben ser posibles en casos aislados, cuando ninguno de los otros motivos para la transferencia sean aplicables».

Las exenciones previstas en el artículo 49.1 del RGPD permiten a los exportadores de datos transferir datos fuera del EEE sin proporcionar garantías adicionales. Sin embargo, es criterio reiterado del GT 29 que las excepciones sólo se aplicarán cuando las transferencias no sean recurrentes, voluminosas ni estructurales[14].

Sobre la base de esas interpretaciones, es casi imposible recurrir a las excepciones en el marco de la computación en nube.

[14] Véase por ejemplo el documento de trabajo WP 12 del GT 29, titulado «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE». Documento aprobado por el Grupo de Trabajo el 24 de julio de 1998. Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_es.pdf.

III. LAS TRANSFERENCIAS INTERNACIONALES EN LA NORMATIVA ACTUAL SOBRE PROTECCIÓN DE DATOS

La normativa española sobre protección de datos, que sigue vigente hasta que sea aplicable el nuevo RGPD a partir del 25 de mayo de 2018, contempla las transferencias internacionales de datos de una manera que, en principio, puede parecer muy similar a como lo hace el RGPD.

La regulación de las transferencias internacionales a países con nivel de protección adecuado no presenta cambios importantes. Pero sí los hay en las transferencias internacionales a países que no ofrecen un nivel equiparable de protección.

De acuerdo a los art. 66 y 70 del RLOPD, para que una transferencia internacional de datos pueda considerarse conforme a la Ley, será necesaria la autorización del Director de la Agencia Española de Protección de Datos (AEPD). Esta podrá ser otorgada en caso de que el responsable del tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos. A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, 2002/16/CE y 2004/915/CE, o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la legislación española.

En el capítulo V del título IX del RLOPD se regula el procedimiento para la obtención de la autorización para las transferencias internacionales de datos. Se iniciará siempre a solicitud del exportador que pretenda llevar a cabo la transferencia. Junto a la solicitud deberá aportarse la documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso.

Cuando la autorización se fundamente en la existencia de un contrato entre el exportador y el importador de los datos, deberá aportarse copia del mismo. Si se fundamenta en normas adoptadas en relación con el tratamiento de los datos en el seno del grupo, deberán aportarse estas, así como la documentación que acredite su carácter vinculante y su eficacia dentro del grupo.

El procedimiento es largo, siendo el plazo máximo para dictar y notificar la resolución de tres meses.

Resaltar que el contenido de la Directiva 95/46/CE y la normativa española que la transpone no son coincidentes en el sentido de que no solo se exige la formalización de un contrato o la aportación de normas corporativas vinculantes sino que, adicionalmente habrá que obtener la autorización del Director de la AEPD.

En la mayor parte de países del EEE, las transferencias realizadas al amparo de cláusulas contractuales tipo aprobadas por la Comisión, o normas corporativas vinculantes, disfrutan directamente de un nivel adecuado de protección. Y ello sin necesidad de procedimiento adicional alguno.

El procedimiento de autorización adoptado en España ha dificultado en muchos casos el cumplimiento de la legalidad. En el mundo de los negocios, en donde el tiempo es oro y la agilidad en las actuaciones es fundamental, un procedimiento administrativo que puede tardar tres meses en ser resuelto, ha desalentado a muchas empresas a cumplir con los trámites legales necesarios.

El número de autorizaciones anuales para realizar transferencias internacionales de datos es, para muchos expertos, ínfimo con respecto al movimiento internacional de datos que se produce en España. Las razones antes mencionadas pueden ser las causantes de ese incumplimiento masivo.

IV. CONCLUSIONES

Como hemos señalado anteriormente, el cliente de la computación en nube actúa como responsable del tratamiento, mientras que el proveedor del servicio es un mero encargado del tratamiento.

También se ha incidido en la falta de estabilidad en la ubicación de los datos. Es muy frecuente que los datos que se encuentran en un lugar determinado en un momento dado, pasen a estar localizados en

otro punto del planeta pocas horas después. Además, el cliente suele desconocer los lugares en que los datos van situándose en el tiempo.

Dependiendo del lugar donde se ubiquen los datos podemos encontrarnos con las siguientes situaciones:

— Si la transmisión de los datos derivada de la prestación de los servicios de computación en nube se realiza en el territorio del Espacio Económico Europeo, no tiene la consideración de transferencia internacional de datos.

— Cuando los datos se destinen a cualquiera de los países con un nivel de protección que se considera adecuado por Decisión de la Comisión Europea, la normativa de protección de datos del país en cuestión es considerada equiparable a la europea. Hay transferencia internacional de datos, pero no es necesario obtener garantías específicas del importador de datos.

— Cuando se trate de proveedores ubicados en los EEUU que se hayan certificado en el marco del Escudo de Privacidad UE-EEE, estaríamos en el mismo caso que en el punto anterior.

— Si se contratan los servicios de un proveedor de computación en nube que transfiera la información a un país que no ofrezca un nivel adecuado de protección, el responsable o el encargado del tratamiento solo podrá transmitir datos personales si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

En el último de los casos, las garantías adecuadas para la computación en nube se pueden obtener especialmente en base a la Decisión 2010/87/UE o de normas corporativas vinculantes.

La Decisión 2010/87/UE contempla los contratos en los que un responsable del tratamiento está establecido en el EEE, mientras que el encargado de tratamiento lo está fuera del territorio del EEE, caso muy común en las dos partes del contrato. Además, la Decisión 2010/87/UE contiene cláusulas contractuales tipo específicas para la subcontratación por un encargado del tratamiento de datos establecido en un tercer país (el importador de datos) de sus servicios de tratamiento a otros encargados (subencargados del tratamiento de datos) establecidos en terceros países, circunstancia muy frecuente en la computación en nube.

En el caso de que las garantías adecuadas se obtengan en base a NCV (ya sean para responsables o para encargados), los grupos multi-

nacionales con sucursales y filiales en países dentro y fuera del EEE, podrán efectuar transferencias desde las entidades en el EEE con destino a las entidades radicadas fuera. Significan una alternativa a las cláusulas tipo, y al contrario que estas, no se trata de estándares generales sino de soluciones particulares para cada grupo multinacional.

La normativa española todavía vigente exige que, además de la firma de las cláusulas tipo o de la aprobación de NCV, se solicite la autorización a la transferencia internacional de datos. Hemos visto que esa solicitud inicia un largo procedimiento administrativo, que posiblemente desincentiva el cumplimiento de la legalidad.

Con la entrada en vigor del nuevo RGPD, la firma de las cláusulas tipo o de la aprobación de NCV, permitirá la transferencia internacional sin más requisitos. A efecto de que no puedan surgir interpretaciones en sentido contrario, el art. 46.2 del RGPD lo deja bien claro: no se requiere ninguna autorización expresa de una autoridad de control.

Este cambio normativo facilitará enormemente el cumplimiento de la ley en todas las transferencias internacionales de datos, incluyendo claro está, las que se produzcan en el marco de la computación en nube.

Aún así, es necesario que surjan nuevas herramientas para simplificar todavía más las transferencias internacionales, a la vez que se garantice la protección de datos personales. En caso contrario, la UE quedará rezagada en el campo de la computación en la nube y en la aplicación de las nuevas aplicaciones tecnológicas.