

CLOUD COMPUTING, CLÁUSULAS CONTRACTUALES Y REGLAS CORPORATIVAS VINCULANTES

CLOUD COMPUTING, STANDARD CONTRACTUAL CLAUSES
AND BINDING CORPORATE RULES

VICENTE GUASCH PORTAS

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

JOSÉ RAMÓN SOLER FUENSANTA

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

Resumen: Los artículos 25 y 26 de la Directiva 95/46/CE prevén la libre circulación de datos personales a países situados fuera del EEE sólo si el país en cuestión garantiza un nivel adecuado de protección de datos. De otro modo, el responsable del tratamiento y sus correspondientes o encargados deberán establecer garantías específicas. En el caso de la computación en nube es muy frecuente que los datos se ubiquen en países que no garantizan un nivel adecuado. Para poder efectuar estas transferencias de datos a terceros países se requieren salvaguardias específicas mediante el uso de disposiciones de puerto seguro, cláusulas contractuales tipo o normas corporativas vinculantes, según proceda. En este trabajo se analizan las diferentes herramientas que se pueden emplear para que la computación en nube se realice de acuerdo a la normativa de protección de datos.

Palabras clave: Computación en nube, transferencia internacional, protección adecuada, cláusulas contractuales, reglas corporativas vinculantes.

Abstract: Articles 25 and 26 of Directive 95/46/EC provides the free movement of personal data to countries outside the EEA only if the country in question ensures an adequate level of data protection. Otherwise, the controller and the stewards or processors should establish specific safeguards. In the case of cloud computing is very common that the data are located in countries that do not ensure an adequate level. To make these transfers of data to third countries, specific safeguards are required using safe harbor provisions, contractual clauses or binding corporate rules. In this paper the different tools that can be used for cloud computing is carried out in compliance with the rules of data protection are studied.

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

Recepción original: 19/02/2014

Aceptación original: 20/03/2014

Sumario: I. Introducción. II. Partes que intervienen en la computación en nube. III. Localización de los datos. IV. La función de las disposiciones contractuales. V. Las cláusulas contractuales tipo de la Unión Europea. VI. Las cláusulas contractuales de la AEPD: Encargado a Subencargado. VII. Las reglas corporativas vinculantes. VIII. Conclusiones.

I. INTRODUCCIÓN

El cloud computing o computación en nube es una forma nueva de prestación de los servicios de tratamiento de la información. Consita 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 es un negocio en auge que probablemente cambiará de forma radical la concepción que tenemos sobre la informática. Los ingresos mundiales de los servicios de computación en nube crecen a una tasa que quintuplica a la de los productos tradicionales de tecnología de la información¹.

¹ Véase por ejemplo el documento *Worldwide and Regional Public IT Cloud Services 2010-2014 Forecast*. Junio de 2010. IDC Corporate USA. Disponible en: <http://www.idc.com/research>

Podríamos clasificar los servicios de computación en nube en diferentes categorías²:

- a) Nube pública. Hablamos de un servicio de Nube Pública cuando el proveedor de servicios de cloud proporciona sus recursos de forma abierta a entidades heterogéneas, sin más relación entre sí que haber cerrado un contrato con el mismo proveedor de servicio.
- b) Nube privada. Encontramos un servicio de Nube Privada, cuando una entidad realiza la gestión y administración de sus servicios en la nube para las partes que la forman, sin que en la misma puedan participar entidades externas y manteniendo el control sobre ella. Una Nube Privada no necesariamente se implementa por la misma entidad que la utiliza, sino que puede contratarse a un tercero que actuará bajo su supervisión y en función de sus necesidades.
- c) Otros modelos. Entre ambos modelos se encuentran soluciones intermedias que tomarán distintos nombres, como pueden ser las Nubes Híbridas, en las que determinados servicios se ofrecen de forma pública y otros de forma privada, o las Nubes Comunitarias, cuando dichos servicios son compartidos en una comunidad cerrada.

Los proveedores de la nube proporcionan acceso a recursos informáticos a través de la red, y ofrecen una serie de servicios adicionales de valor añadido que acercarán la oferta del proveedor a las necesidades de su cliente. En función de lo completo que sea ese valor añadido podemos diferenciar³:

- a) Software como servicio. Podemos hablar de una Nube de Software (modelo de servicio Software as a Service o SaaS), cuando el usuario encuentra en la nube las herramientas finales con las que puede implementar directamente los procesos de su empresa.
- b) Infraestructura como servicio. Si el valor añadido es nulo, se puede hablar de una Nube de infraestructura (IaaS). En ese caso el proveedor proporciona capacidades de almacenamiento y proceso en bruto, sobre las que el usuario ha de construir

² Clasificación obtenida de la «GUÍA para clientes que contraten servicios de Cloud Computing», elaborada por la AEPD. Disponible en: <http://www.agpd.es>.

³ Clasificación obtenida también de la «GUÍA para clientes que contraten servicios de Cloud Computing», citada anteriormente.

las aplicaciones que necesita su empresa prácticamente desde cero.

- c) Plataforma como servicio. Entre estas dos aproximaciones se pueden encontrar otras intermedias llamadas PaaS (Plataforma como Servicio), en las que se proporcionan utilidades para construir aplicaciones, como bases de datos o entornos de programación sobre las que el usuario puede desarrollar sus propias soluciones.

La computación en nube tiene las siguientes cinco características esenciales⁴:

- Autoservicio bajo demanda. El usuario puede acceder a capacidades de computación «en la nube» de forma automática conforme las necesita sin necesidad de una interacción humana con su proveedor o sus proveedores de servicios Cloud.
- Múltiples formas de acceder a la red. Los recursos son accesibles a través de la red y por medio de mecanismos estándar que son utilizados por una amplia variedad de dispositivos de usuario, desde teléfonos móviles a ordenadores portátiles o PDAs.
- Compartición de recursos. Los recursos (almacenamiento, memoria, ancho de banda, capacidad de procesamiento, máquinas virtuales, etc.) de los proveedores son compartidos por múltiples usuarios, a los que se van asignando capacidades de forma dinámica según sus peticiones. Los usuarios pueden ignorar el origen y la ubicación de los recursos a los que acceden, aunque sí es posible que sean conscientes de su situación a determinado nivel, como el de CPD o el de país.
- Elasticidad. Los recursos se asignan y liberan rápidamente, muchas veces de forma automática, lo que da al usuario la impresión de que los recursos a su alcance son ilimitados y están siempre disponibles.
- Servicio medido. El proveedor es capaz de medir, a determinado nivel, el servicio efectivamente entregado a cada usuario, de forma que tanto proveedor como usuario tienen acceso transparente al consumo real de los recursos, lo que posibilita el pago por el uso efectivo de los servicios.

⁴ Clasificación obtenida de la página electrónica de la Agencia Española de Protección de Datos en su apartado de «preguntas frecuentes». Disponible en: <http://www.agpd.es>.

Como se indica en el informe «Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal⁵», las ventajas técnicas y económicas del modelo son inmediatas para los usuarios. No es necesario que los pequeños negocios cuenten con personal informático propio dedicado al mantenimiento de los servidores y las aplicaciones. Por otra parte, los servicios tecnológicos pasan a ser un gasto operativo, obviándose la necesidad de inversiones en infraestructuras de breves ciclos de vida y rápida obsolescencia. El acceso a los servicios está garantizado desde cualquier lugar del mundo en el que se disponga de una conexión a Internet, y el proveedor de servicios asegura la disponibilidad del servicio y la actualización permanente de aplicaciones y sistemas.

II. PARTES QUE INTERVIENEN EN LA COMPUTACIÓN EN NUBE

En el ámbito de la protección de datos es muy importante evaluar el papel de las partes que intervienen en la computación en nube. Para efectuar este estudio es muy importante el análisis del documento elaborado por el Grupo de Protección de Datos del Artículo 29 (G-29 a partir de ahora) sobre los conceptos de responsable del tratamiento y encargado del tratamiento⁶, si bien encontramos las definiciones generales de ambas figuras en el artículo 2 de la Directiva:

- Responsable del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario.
- Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento.

⁵ Informe *Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal*. Presentado a 18 de junio de 2012 por la AEPD y el Consejo General de la Abogacía Española. Documento disponible en: <http://www.agpd.es>.

⁶ Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», WP 169, adoptado el 16 de febrero de 2010.

Según el documento antes indicado del G-29, «el papel primero y primordial del concepto de responsable del tratamiento es determinar quién debe asumir la responsabilidad del cumplimiento de las normas sobre protección de datos y de qué manera los interesados pueden ejercer sus derechos en la práctica. En otras palabras, debe asignar la responsabilidad». Por otra parte, el encargado del tratamiento deberá cumplir dos condiciones básicas:

- Ser una entidad jurídica independiente del responsable.
- Realizar el tratamiento de datos personales por cuenta de éste.

En el Dictamen 05/2012 del G-29⁷, se estudia la posición que ocupan clientes y proveedores de servicios de computación en nube. Para el G-29, 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, y por lo tanto debe aceptar la responsabilidad de respetar la legislación sobre protección de datos, y es responsable y está sujeto a todas las obligaciones legales que figuran en la Directiva 95/46/CE.

El proveedor es la entidad que presta los servicios de computación en nube de las distintas formas que se han mencionado. Cuando el proveedor suministra los medios y la plataforma, actuando en nombre del cliente, se considera que es el encargado del tratamiento es decir, será como antes ya hemos definido, «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento».

En la computación en nube es frecuente que los encargados de tratamiento (proveedores del servicio) subcontraten subencargados del tratamiento adicionales. Esta subcontratación se ha estudiado por el G-29 en el Dictamen 1/2010 antes mencionado, llegando a la conclusión de que «no hay nada en la Directiva que impida que, por exigencias organizativas, se pueda designar a varias entidades como encargadas (o subencargadas) del tratamiento de datos, incluso subdividiendo los cometidos en cuestión. Ahora bien, todas ellas tienen que ajustarse a las instrucciones dadas por el responsable del tratamiento de los datos al llevar a cabo el tratamiento».

⁷ Dictamen 05/2012 sobre la computación en nube, WP 196, adoptado el 1 de julio de 2012.

III. LOCALIZACIÓN DE LOS DATOS

La computación en nube se basa en muchas ocasiones 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. Por otra parte, el cliente suele desconocer los lugares en que los datos van situándose en el tiempo.

Ante la posibilidad de que los datos no se encuentren ubicados en territorio español, deberemos ver las consecuencias que esto comporta. Para ello podemos partir del contenido del artículo 25.1 de la Directiva 95/46/CE: «Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado». Sin embargo, el artículo 26.2 regula que «los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas».

Debemos aclarar, como ya se indica en el art. 25.1 señalado anteriormente, que existirá una transferencia internacional cuando los datos sean ubicados en un país tercero. El RLPOD lo deja mucho más nítido cuando en su artículo 5 nos define la transferencia internacional de datos como aquel «tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo⁸, 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».

Entonces solamente existirá una transferencia internacional cuando los datos sean transmitidos a otro país que no forme parte del Espacio Económico Europeo. Sin embargo, y ya dentro de lo que son

⁸ El Espacio Económico Europeo está formado por los 28 países de la Unión Europea más Islandia, Liechtenstein y Noruega.

transferencias internacionales, deberemos distinguir entre países que garanticen un nivel de protección adecuado y países que no lo garanticen. La lista de países que han obtenido el reconocimiento, por parte de la Comisión Europea, de nivel adecuado de protección, es muy reducida: Suiza, Canadá (respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos), Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda⁹. Además se considera que ofrecen garantías adecuadas las entidades estadounidenses adheridas a los principios de «Puerto Seguro» (Safe Harbor)¹⁰. No se espera que esta lista tenga mucho crecimiento en el medio plazo, con lo cual la gran inmensidad de países del planeta quedan fuera del libre tránsito de datos personales¹¹.

Siguiendo la clasificación del informe «Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal», más arriba citado, 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 tienen la consideración de transferencia internacional de datos, por lo que no resulta necesaria la autorización de la AEPD.
- 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, por lo que tampoco resulta necesaria la autorización de la AEPD.

⁹ Las decisiones de la Comisión sobre nivel de protección adecuado han sido las siguientes:

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

¹⁰ Decisión 2000/520/CE de la Comisión de 26 de julio de 2000.

¹¹ Véase sobre esta materia el artículo de GUASCH PORTAS, V: «La transferencia internacional de datos de carácter personal». Revista de Derecho Uned, n.º 11 de 2012.

- Cuando se trate de proveedores ubicados en los EEUU que se hayan adherido voluntariamente para la prestación de esos servicios al acuerdo de «puerto seguro», en virtud del cual se obligan a cumplir requisitos equivalentes a los europeos en materia de protección de datos, estaríamos en el mismo caso que en el punto anterior. Deberá suscribirse un contrato de prestación de servicios conforme a la LOPD entre las dos partes y si el proveedor radicado en EEUU va a transferir los datos personales a un tercer país deberá aportar garantías por escrito para ofrecer, como mínimo, el mismo nivel de protección que se le haya requerido¹².
- Si se contratan los servicios de un proveedor de Cloud Computing que transfiera la información a un país que no ofrezca un nivel adecuado de protección habrá de obtenerse la autorización previa del Director de la AEPD, según el procedimiento previsto en los artículos 137 a 140 del RLOPD.

IV. LA FUNCIÓN DE LAS DISPOSICIONES CONTRACTUALES

Habíamos visto que el artículo 26.2 de la Directiva 95/46/CE permite a un Estado miembro autorizar una transferencia o un conjunto de transferencias a un tercer país que no garantice una protección adecuada «cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos». Esta disposición especifica, asimismo, que «dichas garantías podrán derivarse, en particular, de cláusulas contractuales».

Además, el artículo 26.4 faculta a la Comisión para declarar que determinadas cláusulas contractuales tipo ofrecen garantías suficientes a efectos de lo dispuesto en el artículo 26.2.

El documento WP 12¹³ del G-29 analiza cual debe ser el objetivo de una solución contractual. En el contexto de las transferencias a terceros países el contrato es un medio que permite al responsable del

¹² Véase la Decisión de la Comisión sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, en el DOCE L 215, de 25 de agosto de 2000.

¹³ WP 12 «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 adoptado por el Grupo de trabajo el 24 de julio de 1998. Este documento no es el

tratamiento ofrecer garantías adecuadas al transmitir datos fuera de la Unión Europea a un país en el que el nivel general de protección no sea suficiente. Para que una cláusula contractual pueda cumplir esta función, debe compensar de manera satisfactoria la ausencia de una protección general adecuada mediante inclusión de los elementos esenciales de la misma que no existen en una situación determinada.

El punto de partida para analizar el significado de la expresión «garantías suficientes» utilizada en el artículo 26.2 es el concepto de «protección adecuada». Éste consiste en una serie de principios básicos para la protección de datos, junto con ciertas condiciones necesarias para asegurar su eficacia.

El primer requisito de una solución contractual es que obligue a las partes de la transferencia a garantizar que se aplique íntegramente el conjunto de principios básicos de protección de datos al tratamiento de los datos transferidos al país no comunitario.

Dichos principios básicos son los siguientes:

- Principio de limitación de objetivos.
- Principio de proporcionalidad y de calidad de los datos.
- Principio de transparencia.
- Principio de seguridad.
- Derecho de acceso, rectificación y oposición.
- Restricciones respecto a transferencias sucesivas a personas ajena al contrato.

Además, en determinados casos deben aplicarse los principios complementarios relativos a los datos sensibles, a la mercadotecnia directa y a las decisiones automatizadas.

El contrato debe estipular minuciosamente la forma en que el receptor de los datos transferidos ha de aplicar los anteriores principios

primero en que el G-29 estudia el tema, ya que antes lo había realizado en los siguientes informes:

- WP 4 «Primeras orientaciones sobre la transferencia de datos personales a terceros países. Posibles formas de evaluar la adecuación», documento adoptado por el Grupo de trabajo el 26 de junio de 1997.

- WP 7 «Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un tercer país?», documento adoptado por el Grupo de trabajo el 14 de enero de 1998.

- WP 9 «Conclusiones preliminares sobre la utilización de disposiciones contractuales en caso de transferencia de datos personales a terceros países», documento adoptado por el Grupo de trabajo el 22 de abril de 1998.

(es decir, deben especificarse los fines de la transferencia, las categorías de los datos, el plazo límite de conservación, las medidas de seguridad, etc.). En circunstancias distintas, por ejemplo cuando exista en el tercer país considerado una ley general de protección de datos similar a la Directiva, es probable que existan otros mecanismos por los que se precise la forma en la que se aplican, en la práctica, las normas sobre protección de datos (códigos de conducta, notificación, función consultiva de la autoridad supervisora). En el caso de un contrato esto no es así. Por tanto, en el supuesto de que la transferencia se base en un contrato, los detalles son imprescindibles.

Por otra parte, para evaluar la efectividad del contrato en un sistema de protección de datos, el G-29 fija tres criterios que son la capacidad del sistema para:

- Ofrecer un nivel satisfactorio de cumplimiento de las normas.
- Facilitar apoyo y asistencia a los interesados en el ejercicio de sus derechos.
- Proporcionar vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas.

V. LAS CLÁUSULAS CONTRACTUALES TIPO DE LA UNIÓN EUROPEA

Las cláusulas contractuales tipo adoptadas por la Comisión Europea han contemplado dos posibles supuestos: transferencias internacionales de datos entre responsables del tratamiento o entre un responsable y un encargado del tratamiento. En el apartado 2 de este trabajo ya habíamos delimitado el concepto de ambas figuras tal como aparecen definidas en el documento WP 169 del G-29.

Las cláusulas contractuales tipo entre responsables de tratamiento cubren la transferencia de datos personales por responsables del tratamiento establecidos en la UE a destinatarios establecidos fuera del territorio de la Unión que actúen también como responsables del tratamiento:

- Decisión 2001/497/CE¹⁴.
- Decisión 2004/915/CE¹⁵ (por la que se modifica la Decisión 2001/497/CE).

¹⁴ DOCE L 181 de 4 de julio de 2001.

¹⁵ DOUE L 385 de 29 de diciembre de 2004.

Las cláusulas contractuales tipo entre un responsable y un encargado del tratamiento cubren la transferencia de datos personales por responsables del tratamiento establecidos en la UE a destinatarios establecidos fuera del territorio de la Unión que actúen solamente como encargados del tratamiento, ya que estas transferencias no exigen las mismas garantías, porque el encargado del tratamiento actúa exclusivamente en nombre del responsable:

- Decisión 2002/16/CE¹⁶ (derogada a partir de 15 de mayo de 2010).
- Decisión 2010/87/UE¹⁷.

Como ya se había indicado anteriormente, en la computación en nube el cliente actúa como responsable del tratamiento, y por lo tanto debe aceptar la responsabilidad de respetar la legislación sobre protección de datos, y es responsable y está sujeto a todas las obligaciones legales que figuran en la Directiva 95/46/CE. El proveedor es la entidad que presta los servicios de computación en nube y por regla general se considera que es el encargado del tratamiento.

Si la relación se produce entre un responsable y un encargado de tratamiento, las cláusulas tipo de conformidad con la Decisión 2010/87/CE de la Comisión son un instrumento que puede ser utilizado como base para que la computación en nube ofrezca garantías adecuadas en el contexto de las transferencias internacionales.

La Decisión 2010/87/UE debe entenderse sin perjuicio de las autorizaciones nacionales que puedan conceder los Estados miembros de conformidad con las disposiciones nacionales de aplicación del artículo 26.2 de la Directiva 95/46/CE. La Decisión tendrá como efecto únicamente exigir a los Estados miembros que no se nieguen a reconocer que las cláusulas contractuales tipo establecidas en ella proporcionan las garantías adecuadas, por lo que no afectará de ninguna manera a otras cláusulas contractuales.

Anteriormente a la Decisión 2010/87/UE ya existía la Decisión 2002/16/CE de la Comisión. La anterior Decisión se adoptó para facilitar la transferencia de datos personales de un responsable del tratamiento de datos establecido en la Unión Europea a un encargado del tratamiento de datos establecido en un tercer país que no ofrezca el nivel adecuado de protección. Sin embargo, la Decisión 2002/16/CE

¹⁶ DOCE L 51 de 22 de febrero de 2002.

¹⁷ DOUE L 39 de 12 de febrero de 2010.

necesitaba una actualización que abordase entre otros temas, algunos problemas que no fueron regulados por dicha Decisión.

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. Además establece las condiciones que ha de cumplir el subtratamiento para garantizar que los datos personales que se están transfiriendo sigan protegidos con independencia de la sucesiva transferencia a un subencargado del tratamiento.

El subtratamiento no podrá exceder de las operaciones acordadas en el contrato entre el exportador de datos y el importador de datos. No se referirá a operaciones de tratamiento o finalidades diferentes para respetar así el principio de limitación de la finalidad establecido en la Directiva 95/46/CE. Además, si el subencargado del tratamiento de datos no cumple sus propias obligaciones de tratamiento de datos, el importador de datos seguirá siendo responsable frente al exportador de datos. La transferencia de datos personales a encargados del tratamiento establecidos fuera de la Unión Europea se hará sin perjuicio de que las actividades de tratamiento se rijan por la legislación de protección de datos aplicable.

Las cláusulas contractuales tipo serán exigibles no solamente por las organizaciones que sean parte en el contrato, sino también por los interesados, en particular cuando estos sufran un daño como consecuencia del incumplimiento del contrato. El interesado tendrá derecho a emprender acciones y, en su caso, percibir una indemnización del exportador de datos que sea el responsable del tratamiento de los datos personales transferidos. Excepcionalmente, bajo ciertas condiciones, también tendrá derecho a emprender una acción y, en su caso, percibir una indemnización del importador de datos o del subencargado del tratamiento de datos. El contrato se regirá por la legislación del Estado miembro de establecimiento del exportador de datos.

La Decisión 2010/87/UE solo se aplica a la subcontratación por un encargado del tratamiento establecido en un tercer país, de sus servicios de tratamiento a un subencargado establecido en un tercer país, por lo que no se aplicará a la situación en la que un encargado del tratamiento establecido en la Unión Europea y que realice el tratamiento de datos personales en nombre de un responsable del tratamiento establecido en la Unión Europea subconfrage sus operaciones

de tratamiento a un subencargado del tratamiento establecido en un tercer país¹⁸.

Aparece entonces el problema de cómo encuadrar jurídicamente las transferencias de datos de un responsable del tratamiento establecido en el EEE hacia un encargado del tratamiento establecido en el EEE y luego a un subencargado del tratamiento establecido fuera del EEE. Mientras no se adopte ningún instrumento específico para este caso, el G-29 encuentra tres posibles soluciones¹⁹:

- a) Un contrato directo entre el responsable del tratamiento y el subencargado del tratamiento establecido fuera del EEE, conforme a la Decisión 2010/87/UE.
- b) Un mandato expreso por el cual el responsable da al encargado del tratamiento establecido en el EEE el poder de utilizar las cláusulas tipo de la Decisión 2010/87/UE por su cuenta.
- c) Un contrato ad hoc. Tal como se indica en el Considerando 23 de la Decisión 2010/87/UE, «en tales situaciones, los Estados miembros son libres de tener en cuenta el hecho de que los principios y las garantías de las cláusulas contractuales tipo establecidas en la presente Decisión se hayan utilizado para subcontratar a un subencargado establecido en un tercer país con la intención de prestar la adecuada protección de los derechos de aquellos interesados cuyos datos personales se estén transfiriendo para operaciones de subtratamiento».

La Decisión 2010/87/UE se aplica desde el 15 de mayo de 2010, quedando derogada la Decisión 2002/16/CE con efectos a partir de la misma fecha.

¹⁸ Así lo confirma el G-29 en su documento WP 176, adoptado el 12 de julio de 2010, sobre preguntas frecuentes por la entrada en vigor de la Decisión 2010/87/UE, en su primera cuestión: «*Les clauses types de la décision 2010/87/UE s'appliquent-elles en cas de transfert de données à caractère personnel d'un responsable du traitement établi dans l'EEE vers un sous-traitant établi dans l'EEE, puis vers un sous-traitant ultérieur établi hors de l'EEE? Non. Comme l'indique le considérant 23, la décision de la Commission s'applique exclusivement à la sous-traitance, par un sous-traitant établi dans un pays tiers, de ses services de traitement à un sous-traitant ultérieur établi dans un pays tiers.*

¹⁹ Así lo formula en la tercera cuestión del documento WP 176 antes citado.

VI. LAS CLÁUSULAS CONTRACTUALES DE LA AEPD: ENCARGADO A SUBENCARGADO

La postura que venía manteniendo la AEPD en el caso de la subcontratación de un encargado establecido en España a un subencargado radicado en un tercer país que no ofrece un nivel adecuado de protección, la encontramos en el Informe de la Agencia 582/2004²⁰. En dicho Informe se señala que los supuestos planteados en la Instrucción 1/2000²¹ únicamente se refieren a aquellos casos en que la transferencia sea realizada por un responsable del tratamiento, bien a otro responsable, bien a un encargado. Del mismo modo, la Comisión Europea únicamente ha adoptado Decisiones en las que una parte del contrato sea el responsable del tratamiento, efectuándose la transferencia bien a un responsable (Decisiones 2001/497/CE y 2004/915/CE), bien a un encargado del tratamiento (Decisión 2002/16/CE). Si nos centramos en este caso, «la transferencia amparada en las cláusulas contenidas en la Decisión 2002/16/CE únicamente es posible en caso de que el contrato sea celebrado entre el responsable del tratamiento y el encargado ubicado en el tercer estado que no ofrezca un nivel adecuado de protección, de modo que no será posible en ningún caso que el mismo sea suscrito por dos encargados del tratamiento, ya que el encargado exportador no podría asumir las obligaciones estipuladas en el contrato sin convertirse en responsable, lo que implicaría la existencia de una previa cesión de datos al mismo, que habría de resultar conforme a lo dispuesto en el artículo 11 de la Ley Orgánica 15/1999 y desnaturalizaría la posición del propio encargado». Para que la transferencia pueda considerarse conforme a lo dispuesto en la LOPD, es necesario que, en las cláusulas contractuales que se firmen, el responsable del tratamiento tenga la condición de exportador, a los efectos previstos en la Decisión 2002/16/CE.

Esta postura ha cambiado en fecha reciente. La AEPD ha elaborado a primeros de 2012 un nuevo conjunto de cláusulas contractuales²² aplicables a contratos de subcontratación de servicios entre encargados establecidos en España y subencargados radicados en terceros

²⁰ «Subcontratación de un encargado del tratamiento en tercer país que no ofrece nivel adecuado de protección. Necesidad de intervención del responsable. Informe 582/2004». Disponible en la web de la AEPD.

²¹ Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos (BOE de 16-12-2000).

²² Estas cláusulas contractuales (encargados a subencargados de tratamiento) están disponibles en la página electrónica de la AEPD.

países²³. Estas cláusulas contractuales se basan en el contenido del Considerando 23²⁴ de la Decisión 2010/87/UE, que otorga a las autoridades nacionales en materia de protección de datos, la posibilidad de dar mayor flexibilidad en la subcontratación que puedan llevar a cabo encargados nacionales con subencargados que operan en terceros países.

El nuevo conjunto de cláusulas contractuales prevé que el solicitante de la autorización de la transferencia internacional sea el encargado del tratamiento (y no el responsable del tratamiento, como se venía exigiendo hasta la fecha). Dicha solicitud de transferencia se inspira en la Cláusula 11²⁵ de la Decisión 2010/87/UE, sobre subtratamiento de datos.

Bajo el nuevo modelo de cláusulas contractuales, el responsable deberá autorizar previamente al encargado la posterior subcontratación a un subencargado importador y, si es el caso, a posteriores subencargados. El contrato marco responsable-encargado (regulado en el artículo 12 de la LOPD y en los artículos 20 a 22 del RLOPD), debe-

²³ Véase el documento «El régimen de transferencias internacionales de datos a encargados de tratamiento» elaborado por la señora María José Blanco Antón, Subdirectora General del Registro General de Protección de Datos, para la «Cuarto sesión anual abierta de la AEPD», celebrada en Madrid el 27 de enero de 2012. Disponible en la página electrónica de la AEPD.

²⁴ Según el Considerando 23 de la Decisión 2010/87/UE, dicha Decisión solo se aplica a la subcontratación por un encargado del tratamiento establecido en un tercer país de sus servicios de tratamiento a un subencargado establecido en un tercer país, por lo que no se aplicará a la situación en la que un encargado del tratamiento establecido en la Unión Europea y que realice el tratamiento de datos personales en nombre de un responsable del tratamiento establecido en la Unión Europea subcontrate sus operaciones de tratamiento a un subencargado del tratamiento establecido en un tercer país. En tales situaciones, los Estados miembros son libres de tener en cuenta el hecho de que los principios y las garantías de las cláusulas contractuales tipo establecidas en la Decisión 2010/87/UE se hayan utilizado para subcontratar a un subencargado establecido en un tercer país con la intención de prestar la adecuada protección de los derechos de aquellos interesados cuyos datos personales se estén transfiriendo para operaciones de subtratamiento.

²⁵ Según el punto 1 de la Cláusula 11 de la Decisión, el importador de datos no subcontratará ninguna de sus operaciones de procesamiento llevadas a cabo en nombre del exportador de datos con arreglo a las cláusulas sin previo consentimiento por escrito del exportador de datos. Si el importador de datos subcontrata sus obligaciones con arreglo a las cláusulas, con el consentimiento del exportador de datos, lo hará exclusivamente mediante un acuerdo escrito con el subencargado del tratamiento de datos, en el que se le impongan a éste las mismas obligaciones impuestas al importador de datos con arreglo a las cláusulas. En los casos en que el subencargado del tratamiento de datos no pueda cumplir sus obligaciones de protección de los datos con arreglo a dicho acuerdo escrito, el importador de datos seguirá siendo plenamente responsable frente al exportador de datos del cumplimiento de las obligaciones del subencargado del tratamiento de datos con arreglo a dicho acuerdo.

rá dar garantías por parte del responsable y del encargado de que los tratamientos de datos han sido efectuados y seguirán efectuándose de conformidad con la LOPD. En el contrato deberán constar las autorizaciones a la subcontratación y a las transferencias internacionales de datos, debiendo identificarse los ficheros y la notificación al Registro General de Protección de Datos.

El encargado de tratamiento en todo momento deberá tener a disposición de la AEPD, por una parte, la relación de responsables a los que presta servicios, y por otra, la relación de importadores y de subencargados ulteriores que intervengan en el tratamiento. En el contrato se describirán los servicios prestados por el subencargado, la descripción de finalidades y categorías de datos objeto de tratamiento así como la descripción de las medidas de seguridad que va a aplicar el subencargado.

En un primer momento el modelo de cláusulas contractuales se mantuvo en secreto por parte de la AEPD. Solo se facilitaría por parte de la Agencia a aquellas entidades que tuvieran un interés real en emplearlas para sus transferencias internacionales de datos. Esta postura cambió completamente a partir de la solicitud de autorización para la transferencia internacional de datos efectuada a 16 de julio de 2012 por una empresa en calidad de encargada del tratamiento²⁶. En la Resolución de Autorización de transferencias internacionales de datos correspondiente a esta solicitud de autorización, la AEPD añadió como anexo el nuevo conjunto de cláusulas contractuales. El punto de partida del nuevo modelo contractual se encuentra, como ya se había indicado anteriormente, en la Decisión 2010/87/UE. Es decir, el contrato viene a estipular un clausulado similar al de la citada Decisión. No obstante, como no puede ser de otro modo, dicho clausulado no puede ser idéntico, tanto por la naturaleza de las partes intervenientes como por la necesaria relación que el contrato de transferencia internacional debe guardar con el contrato marco firmado por el exportador con el responsable del tratamiento. Así por ejemplo, se incluyen una serie de obligaciones del exportador de datos, adicionales a las establecidas en la Decisión 2010/87/UE. Se contienen en las letras i) a n) de la cláusula 4.2, de forma que el exportador:

«i) mantendrá una lista actualizada de los responsables del tratamiento y ficheros a cuyos datos se refiera la transferencia, que pondrá a disposición de la Agencia Española de Protección de Datos y notificará cualquier modificación en la misma;

²⁶ Véase el número de Expediente TI/00126/2012 en la página de la AEPD, así como la publicación oficial del «Acuerdo de Apertura del Período de Información Pública» en el BOE de 20-09-2012.

- j) comunicará al responsable del tratamiento cualquier acuerdo que el importador de datos pretenda concluir al amparo de la cláusula 11 para obtener su autorización;*
- k) enviará, sin demora, al responsable del tratamiento una copia de cualquier acuerdo del importador de datos con el subencargado ulterior del tratamiento que concluya con arreglo a las cláusulas;*
- l) comunicará, sin demora, al responsable del tratamiento cualquier notificación del importador de datos conforme a la letra d) de la cláusula 5 del presente contrato;*
- m) promoverá las medidas de auditoría previstas en la letra f) de la cláusula 5 cuando así lo solicite el responsable del tratamiento, dándole traslado en todo caso de los resultados de dichas medidas, así como, en su caso, la identificación del organismo que las hubiera llevado a cabo;*
- n) comunicará al responsable del tratamiento las medidas que se adopten conforme a la cláusula 12 en relación con el destino final de los datos».*

Para concluir, podemos afirmar que cualquier transferencia que se efectúe dentro del marco de una autorización obtenida en base a las nuevas cláusulas contractuales no precisará de una posterior autorización singular del Director de la Agencia Española de Protección de Datos, siempre y cuando:

- Las transferencias internacionales de datos se ajusten a lo establecido en las cláusulas del contrato presentado entre el exportador e importador de los datos, es decir, no afecten nada más que a los colectivos establecidos en el apéndice 1 del contrato de transferencia, y se refieran a las categorías de datos y a las operaciones de tratamiento establecidas en dicho apéndice.
- Se haya suscrito, y pueda ponerse en cualquier momento a disposición de la AEPD el denominado contrato marco entre el responsable del tratamiento y el exportador de datos, incluyendo el contenido y las garantías derivados del marco objeto de la autorización.
- Con anterioridad al comienzo de una transferencia internacional de datos se haya notificado la misma por el responsable del tratamiento, a fin de que se proceda a su inscripción en el RGPD, quedando identificados el fichero o ficheros a cuyos datos se refiera la transferencia internacional, con referencia a la resolución en que se había autorizado la transferencia internacional.

VII. LAS REGLAS CORPORATIVAS VINCULANTES

La transferencia internacional de datos a países terceros que no proporcionan un nivel adecuado de protección en materia de protección de datos ha sido un problema para las empresas multinacionales desde la aprobación de la Directiva 95/46/CE. Como señala Valverde López, «el marco legislativo de la protección de datos de carácter personal ha causado importantes quebraderos de cabeza a las empresas privadas, principalmente multinacionales con representación en diferentes países dentro y fuera de la Unión Europea, para encontrar soluciones innovadoras que pudieran conjugar el correcto cumplimiento de la normativa en materia de protección de datos con sus necesidades comerciales»²⁷. Una de esas soluciones innovadoras ha sido la aparición de las reglas corporativas vinculantes (RCV o en inglés BCR). La Comisión Europea las entiende como «los códigos de buenas prácticas basados en las normas de protección de datos europeas y aprobados al menos por una autoridad de control de la protección de datos, que las entidades elaboran de manera voluntaria y suscriben a fin de asegurar las salvaguardias necesarias para determinadas categorías de transferencias de datos personales entre empresas que forman parte del mismo grupo de sociedades y están vinculadas por esas normas»²⁸.

Como se señala en la página electrónica de la AEPD, se podrán autorizar transferencias internacionales de datos entre sociedades de un mismo grupo multinacional de empresas, cuando hubieran sido adoptadas normas o reglas internas vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español. Los artículos 70.4 y el Título IX, Capítulo V del RLOPD establecen el régimen jurídico aplicable a las transferencias internacionales en el seno de una multinacional. Esta regulación se completa con los siguientes Documentos de Trabajo elaborados por el Grupo del Artículo 29 de la Directiva 95/46/CE relativos al contenido de las normas corporativas vinculantes y al procedimiento previo, que se desarrolla entre los di-

²⁷ VALVERDE LÓPEZ, M: *Las Reglas Corporativas Vinculantes (Binding Corporate Rules) en materia de protección de datos*. 2009, pág. 3. Documento disponible en varias direcciones electrónicas, entre las cuales está la siguiente:

http://www.scribd.com/full/52311596?access_key=key-1i6r2esa8i5og7zl0ta9

²⁸ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI*. Bruselas, 25.01.2012, COM(2012) 9 final. Pág. 12.

ferentes Estados Miembros implicados para la aprobación de dichas normas²⁹:

- 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.

Toda esta regulación de las reglas corporativas vinculantes se ha centrado en las transferencias de datos personales inicialmente tratados por la organización en cuanto que responsable del tratamiento, y realizadas dentro de la misma organización.

Durante los últimos años las RCV para los responsables del tratamiento han demostrado tener cada vez más éxito, aumentando rápidamente el número de grupos multinacionales que las han adoptado.

Sin embargo las RCV para los responsables del tratamiento no dan respuesta a nuevos modelos de negocio para el tratamiento internacional de datos personales como puede ser la computación en nube. Para resolver este problema el G-29 ha elaborado unas nuevas RCV diseñadas para encargados de tratamiento.

Como indica el documento WP 204³⁰ del G-29, las RCV «para los encargados del tratamiento se conciben originariamente como un instrumento de ayuda para estructurar las transferencias internacionales de datos personales inicialmente tratados por un encargado del tratamiento, en nombre de un responsable del tratamiento de la UE y según sus instrucciones, y subtratados dentro de la organización del

²⁹ Puede consultarse el contenido de todos estos documentos en la siguiente dirección electrónica:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

³⁰ WP 204 «Documento explicativo sobre las normas corporativas vinculantes para los encargados del tratamiento». Aprobado el 19 de abril de 2013.

encargado del tratamiento. Por lo tanto, se adjuntarán las RCV para los encargados del tratamiento al contrato de los mismos (denominado en este informe «acuerdo de nivel de servicios») exigido por el artículo 17 de la Directiva 95/46 de la UE y que recoge especialmente las instrucciones del responsable del tratamiento firmadas entre el responsable externo del tratamiento y el encargado del tratamiento. Las RCV para los encargados del tratamiento deben considerarse como garantías adecuadas que el encargado del tratamiento ofrece al responsable del tratamiento (artículo 26, apartado 2, de la Directiva 95/46 de la UE), permitiendo a este último cumplir la legislación sobre protección de datos aplicable de la UE. Las entidades del grupo del encargado del tratamiento se comprometerán a respetar los principios recogidos en las RCV para los encargados del tratamiento, y responderán ante el responsable del tratamiento en caso de incumplimiento de las mismas».

El contenido básico de las RCV para los encargados de tratamiento se encuentra definido en el documento WP 195 elaborado por el G-29³¹. El WP195 dispone que el subtratamiento de los datos podrán realizarlo otros miembros del grupo del encargado del tratamiento únicamente cuando se haya informado previamente al responsable del tratamiento y se haya recibido su consentimiento escrito. Las RCV para los encargados del tratamiento garantizan la transparencia con el responsable del tratamiento y otorgan a este último el control de los datos tratados en su nombre y bajo sus instrucciones por entidades del grupo del encargado del tratamiento. Ambas partes del acuerdo de servicios son libres de decidir, dependiendo de sus necesidades particulares, si únicamente necesitarán un consentimiento general previo del responsable del tratamiento al comienzo del servicio, o si se requerirá un consentimiento específico del responsable del tratamiento para cada subtratamiento.

La organización de un encargado del tratamiento que haya ejecutado las RCV para los encargados del tratamiento no tendrá que firmar contratos para estructurar las transferencias con cada subencargado del tratamiento que forme parte de su organización, puesto que las RCV para los encargados del tratamiento ofrecen garantías para

³¹ Documento WP 195 «Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules». Adoptado el 6 de junio de 2012. En combinación con este documento, se elaboró el WP 195a «Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities». Adoptado el 17 de septiembre de 2012.

los datos transferidos y tratados en nombre de un responsable del tratamiento y bajo sus instrucciones.

Además de las normas anteriormente fijadas para las transferencias dentro del grupo del encargado del tratamiento, los miembros del grupo del encargado del tratamiento únicamente pueden subcontratar sus obligaciones previstas en el acuerdo de servicios (artículo 17 de la Directiva) a un subencargado del tratamiento externo al grupo mediante un acuerdo escrito con este último que garantice la protección adecuada, de conformidad con los artículos 16 y 17 de la Directiva 95/46/CE, y que asegure que el subencargado del tratamiento externo tendrá que respetar las mismas obligaciones impuestas al miembro del grupo del encargado del tratamiento en virtud del acuerdo de servicios y de las secciones 1.3, 1.4, 3 y 6 del documento de trabajo 195. Además, puesto que las RCV para los encargados del tratamiento no son aplicables para las transferencias a subencargados del tratamiento externos (fuera del grupo), se garantizará en estos casos una protección adecuada de conformidad con los artículos 25 y 26 de la Directiva 95/46/CE.

Para el G-29, el establecimiento de RCV facilitará la aplicación del artículo 26.2 de la Directiva en el caso de los encargados del tratamiento. También debería conllevar un cierto grado de simplificación para las organizaciones multinacionales que, en nombre de los responsables del tratamiento, tratan e intercambian datos personales de forma rutinaria en todo el mundo.

VIII. CONCLUSIONES

A pesar de las claras ventajas de la computación en nube, tanto en términos económicos como sociales, el despliegue a gran escala de los servicios de computación en nube puede provocar diversos riesgos para la protección de datos. El cliente de servicios computación en nube deberá verificar, entre otros elementos, si el proveedor de tales servicios puede garantizar la legalidad de las transferencias internacionales de datos. Para garantizar el cumplimiento de esa legalidad se han estudiado las tres herramientas que se encuentran disponibles a día de hoy: las cláusulas contractuales tipo de la Unión Europea de la Decisión 2010/87/UE, las cláusulas contractuales de la AEPD (encargado a subencargado) y las reglas corporativas vinculantes para los encargados del tratamiento. Pero 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.

