COMPUTACIÓN EN LA NUBE Y PUERTO SEGURO

CLOUD COMPUTING AND SAFE HARBOR

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: La computación en la nube se trata de un negocio en auge que cambiará radicalmente la concepción que tenemos sobre la informática. Es una nueva modalidad de servicio tecnológico que permite su uso desde cualquier lugar del mundo que disponga una conexión a internet. Las ventajas para el usuario son muy claras, ya que los ahorros en equipos, software y personal informático pueden llegar a ser muy cuantiosos.

A pesar de esas grandes ventajas, deberá prestarse una atención especial a la hora de evaluar los riesgos jurídicos en materia de protección de datos, que afectan principalmente a las transferencias internacionales de datos. Si este problema ya existía con anterioridad, se ha agravado con la sentencia del Tribunal de Justicia de la Unión Europea de seis de octubre de 2015, en la que se han invalidado los acuerdos de Puerto Seguro con los Estados Unidos.

Abstract: Cloud computing is a booming business that will radically change the conception we have about the informatics. It is a new form of technological service that allows its use from anywhere in the world that has an Internet connection. The user benefits are clear, because the savings in hardware, software and IT staff can become very substantial.

Despite these advantages, special attention must be made when evaluating the legal risks in terms of data protection, which mainly affect the international transfer of data. If this problem already existed, it has been exacerbated by the Court of Justice of the European Union ruling of 6 October 2015, in that have been invalidated the Safe Harbor agreements with the United States.

Palabras clave: Computación en la nube, transferencia internacional de datos, puerto seguro, protección de datos, protección adecuada.

Keywords: Cloud computing, international data transfers, safe harbor, data protection, adequate protection.

Recepción original: 28/12/2015
Aceptación original: 6/04/2016

Sumario: I. La computación en la nube. II. La normativa sobre protección de datos. III. Computación en la nube y normativa de protección de datos. IV. Prestadores de servicios en la nube radicados en EE.UU. V. Conclusiones.

I. LA COMPUTACIÓN EN LA NUBE

La computación en la nube se trata de un negocio en auge que probablemente cambiará de forma radical la concepción que tenemos sobre la informática. Consiste en un modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda y a través de la red a un conjunto de recursos compartidos y configurables que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor de servicios.

Como indica la Agencia Española de Protección de Datos (AEPD) en su Informe «*Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal*»[1], 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 que disponga de una conexión a Internet, y el proveedor de servi-

[1] Informe disponible en la página web de la Agencia: www.agpd.es

cios asegura la disponibilidad del servicio y la actualización permanente de aplicaciones y sistemas.

Para la Comisión Europea la computación en la nube abarca una amplia gama de ámbitos estratégicos. En su documento «*Liberar el potencial de la computación en la nube en Europa*»[2] urge a la adopción de iniciativas políticas que reduzcan los obstáculos a su implantación en la Unión Europea. Para la Comisión es esencial que se sienten las bases para que Europa se convierta en una potencia mundial de la computación en la nube.

La computación en la nube permite a sus usuarios el acceso a una serie de servicios muy variado: correo electrónico, almacenamiento documental, herramientas ofimáticas, aplicaciones de gestión o de contabilidad, etc. Y todo ello sin precisar de servidores o de software propios. Las aplicaciones y los datos se encuentran en algún lugar de Internet representado de forma habitual por una nube.

Las ventajas para el usuario son muy claras, ya que los ahorros en equipos, software y personal informático pueden llegar a ser muy cuantiosos.

Según un reciente informe (15.10.2015) elaborado por el comparador de software «Buscoelmejor», la mayor parte de las empresas españolas está planteándose la sustitución de sus herramientas tecnológicas tradicionales por nuevas soluciones en la nube. Y es en las empresas de menor tamaño en donde existe mayor interés en llevar a cabo ese cambio. Dentro del grupo de las empresas que facturan menos de un millón de euros, más de un 80% estudiaron soluciones CRM (*Customer Relationship Management*) y ERP (*Enterprise Resource Planning*) en la nube. En empresas de mayor tamaño ese porcentaje baja ligeramente, pero sigue siendo muy elevado. Si en lugar de analizar las empresas por su facturación, lo hacemos por la actividad que realizan, encontramos que el 93% de las empresas de servicios está estudiando soluciones en la nube. En la industria y en la distribución ese porcentaje no es tan elevado, pero sigue siendo mayoritario (65% y 72% respectivamente).

Sin embargo, con la contratación de estos servicios en la nube suele desaparecer el conocimiento por parte del usuario de la ubicación física de la información, así como de las condiciones de procesa-

[2] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 27 de septiembre de 2012, titulada «Liberar el potencial de la computación en nube en Europa» (COM(2012)0529). Disponible en: http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20120529.do

miento. En general los datos pasan a situarse en algún lugar indeterminado y variable, en un servidor radicado en una ubicación física desconocida.

De esta manera pueden quedar afectadas las garantías de confidencialidad y de seguridad de la información situada en la nube.

Y es aquí donde aparece el conflicto entre este nuevo modelo de prestación de servicios tecnológicos y la normativa española y europea sobre protección de datos personales.

II. LA NORMATIVA SOBRE PROTECCIÓN DE DATOS

La protección de datos de carácter personal es un campo del derecho de nacimiento muy reciente. Su desarrollo ha estado muy ligado a la evolución de la informática. La posibilidad de almacenar cantidades masivas de datos y de gestionarlos de forma automatizada ha obligado a que surgiese un nuevo derecho para la protección de los datos de carácter personal. Además este campo del derecho se ha consolidado en un periodo de tiempo muy breve.

En nuestro país ya se recoge esta preocupación en el artículo 18.4 de la Constitución Española de 1978: «La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

Pocos años más tarde España firmó y ratificó el Convenio n.º 108, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, del Consejo de Europa. Convenio que entró en vigor para España el uno de octubre de 1985[3].

Pero la norma básica sobre protección de datos a nivel de la UE es la Directiva 95/46/CE[4]. Al igual que todas las directivas, en principio no tiene efecto directo. Son los países de la UE quienes han desarrollado normativa interna que la transpone. En España se efectuó dicha transposición por medio de la Ley Orgánica de Protección de Datos de Carácter Personal[5] (LOPD).

Además de las normas jurídicas antes expuestas, es necesario mencionar que la protección de datos personales ha logrado el estatus

[3] Véase en el BOE de 15 de noviembre de 1985 el texto completo del Convenio n.º 108, así como el Instrumento de Ratificación por parte de España.

[4] DOCE L 281 de 23 de noviembre de 1995.

[5] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Publicada en BOE de 14 de diciembre de 1999.

de derecho fundamental en Europa a través de la Carta de los Derechos Fundamentales de la Unión Europea[6].

La estructura jurídica implantada en la Unión Europea ha llevado a unos resultados relativamente satisfactorios en el mercado interior en materia de protección de datos. Sin embargo el sistema carecería de eficacia si no se hubieran establecido mecanismos que contemplen el movimiento internacional de datos con terceros países. La normativa europea en el campo de la protección de datos es la más exigente del planeta. En cambio hay países con una regulación poco exigente, o incluso sin regulación alguna. Estas diferencias podrían haber conducido a que la protección conseguida en el seno de la Unión se perdiera en el momento en que los datos se localizaran en naciones con un nivel inferior o completamente nulo de protección.

Por las razones mencionadas, la Directiva 95/46/CE y las leyes de transposición de los países de la UE han tenido que afrontar el movimiento internacional de datos hacia países terceros. Como bien señala el artículo 25.1 de la Directiva, únicamente podrá efectuarse una transferencia internacional de datos cuando «el país tercero de que se trate garantice un nivel de protección adecuado». Esta prohibición es mucho más dura de lo que podría parecer, ya que el grupo de países que han conseguido un nivel de protección reconocido como adecuado, es muy reducido: Suiza[7], Canadá[8] respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos, Argentina[9], Guernesey[10], Isla de Man[11], Jersey[12], Islas Feroe[13], Andorra[14], Israel[15], Uruguay[16] y Nueva Zelanda[17]. Tampoco se espera que esta lista tenga mucho crecimiento en el medio plazo.

---

[6] DOUE C 83 de 30 de marzo de 2010.

[7] Suiza: Decisión 2000/518/CE publicada en el DOCE L 215 de 25 de agosto de 2000.

[8] Canadá: Decisión 2002/2/CE publicada en el DOCE L 2 de 4 de enero de 2002.

[9] Argentina: Decisión 2003/490/CE publicada en el DOUE L 168 de 5 de julio de 2003.

[10] Guernesey: Decisión 2003/821/CE publicada en el DOUE L 308 de 25 de noviembre de 2003.

[11] Isla de Man: Decisión 2004/411/CE publicada en el DOUE L 151 de 30 de abril de 2004.

[12] Jersey: Decisión 2008/393/CE publicada en el DOUE L 138 de 28 de mayo de 2008.

[13] Islas Feroe: Decisión 2010/146/UE publicada en el DOUE L 58 de 9 de marzo de 2010.

[14] Andorra: Decisión 2010/625/UE publicada en el DOUE L 277 de 21 de octubre de 2010.

[15] Israel: Decisión 2011/61/UE publicada en el DOUE L 27 de 1 de febrero de 2011.

[16] Uruguay: Decisión 2012/484/UE publicada en el DOUE L 227 de 23 de agosto de 2012.

[17] Nueva Zelanda: Decisión 2013/65/UE publicada en el DOUE L 28 de 30 de enero de 2013.

Si no existiesen soluciones alternativas, el movimiento de datos hacia el exterior de la Unión sería extremadamente limitado, ya que la mayor parte de los países, entre los que se encuentran las nuevas potencias emergentes como China, India, Brasil o Rusia, y desde fecha muy reciente también EEUU, quedan fuera de la relación antes citada de países.

Pero el artículo 26.2 de la Directiva aporta una nueva vía para poder efectuar una transferencia internacional de datos personales a un país que no garantice un nivel de protección adecuado: 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. En particular estas garantías podrán derivarse de cláusulas contractuales apropiadas.

Además de ofrecer esas garantías suficientes, el artículo 33 de la LOPD añade otro requisito adicional: la autorización previa a la transferencia del Director de la Agencia Española de Protección de Datos.

Aquí deberemos recurrir a algunas de las definiciones que nos ofrece el artículo 5 del Reglamento de desarrollo de la Ley Orgánica de protección de datos de carácter personal[18] (RLOPD). En particular nos interesa dejar claro el concepto de lo que es un responsable del tratamiento y lo que es un encargado del tratamiento:

a) Responsable del tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

b) Encargado del tratamiento es la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

[18] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Publicado en el BOE de 19 de enero de 2008.

Las transferencias internacionales las podemos dividir en dos tipos:

— Las que representan una cesión de datos, es decir, de un responsable a otro responsable de tratamiento.

— Las que suponen un acceso a los datos por parte de un encargado del tratamiento.

a) Cuando la transferencia de datos se realice entre responsables de tratamiento se considerará que reúnen las garantías adecuadas los contratos celebrados en los términos previstos en la Decisión de la Comisión Europea 2001/497/CE[19] y en la 2004/915/CE[20], por la que se modifica la anterior.

Cada una de estas dos 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) Cuando la transferencia de datos se realice entre un responsable y un encargado del tratamiento se considerará que reúnen las garantías adecuadas los contratos que incluyan las cláusulas contractuales tipo establecidas en la Decisión de la Comisión Europea 2010/87/UE[21].

c) Cuando la transferencia se realice entre un encargado del tratamiento, establecido en España, y un subencargado del tratamiento, ubicado en un país que no garantiza un nivel adecuado de protección, se considerará que reúnen las garantías adecuadas los contratos que incluyan las cláusulas contractuales tipo 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[22]. Además de este contrato entre el encargado del tratamiento y el subencargado del tratamiento, se requiere otro contrato marco entre el responsable del tratamiento y el encargado del tratamiento en el que aquél autorice la subcontratación y la transferencia internacional de datos.

[19] DOCE L 181 de 4 de julio de 2001.
[20] DOUE L 385 de 29 de diciembre de 2004.
[21] DOUE L 39 de 12 de febrero de 2010.
[22] Disponible en la página web de la AEPD: www.agpd.es

En base a estos contratos se podrá iniciar el procedimiento de autorización de una transferencia internacional de datos. Éste se encuentra regulado en los artículos 137 y siguientes del RLOPD. El plazo de tramitación es largo: tres meses.

Además del procedimiento en base a los contratos tipo, también hay otra vía mucho más compleja y larga en su tramitación: las Reglas Corporativas Vinculantes. Se trata de la autorización de 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. Su regulación se encuentra básicamente en varios Documentos de Trabajo elaborados por el Grupo del Artículo 29 de la Directiva 95/46/CE[23].

III. COMPUTACIÓN EN LA NUBE Y NORMATIVA DE PROTECCIÓN DE DATOS

La expansión de internet ha supuesto la ruptura de los esquemas tradicionales sobre los que se había diseñado la normativa de protección de datos.

La Directiva 95/46/CE y las normas nacionales de transposición han regulado sobre una concepción de la informática que no es la actual. Internet ha hecho aparecer nuevos tratamientos de datos que antes no existían: redes sociales, buscadores, computación en la nube.

Ha habido que examinar cómo se aplican los conceptos clásicos a estas nuevas realidades. Así lo ha hecho el Grupo de Trabajo del art. 29 de la Directiva en su Dictamen 05/2012[24], sobre la computación en la nube, al analizar el papel que juegan el cliente y el proveedor de servicios.

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.

[23] La regulación de las Reglas Corporativas Vinculantes se encuentra esencialmente en los documentos de trabajo siguientes: WP 74, WP 107, WP 108, WP 153, WP 154 y WP 155. Todos ellos están disponibles en la página web del Grupo de Trabajo del artículo 29 de la Directiva: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

[24] Documento de trabajo WP 196, adoptado el uno de julio de 212. Disponible en la página web del Grupo de Trabajo.

En base a este papel, el cliente debe aceptar la responsabilidad de respetar la legislación sobre protección de datos, 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 la nube. Cuando el proveedor suministra los medios y la plataforma, actuando en nombre del cliente, se considera que es el encargado del tratamiento, pues su labor es tratar datos personales por cuenta del responsable.

En el marco de la prestación de servicios de tratamiento de datos personales por cuenta de terceros, recogido en el artículo 12 de la LOPD, el usuario de los servicios de computación en la nube, es decir el responsable, deberá velar para que el prestador de servicios, que actúa como encargado, cumpla la normativa española de protección de datos personales. Las partes no pueden pactar la aplicación de una normativa distinta ni excluir la competencia de la AEPD.

El riesgo para el cliente de la computación en la nube es la falta de transparencia sobre las condiciones en las que prestan el servicio los proveedores.

El prestador del servicio es quien conoce todos los detalles del tratamiento que ofrece. Pero el cliente generalmente se enfrenta a la ausencia de una información clara, precisa y completa sobre todos los elementos inherentes a la prestación.

A la hora de contratar un servicio de computación en la nube, el cliente suele tener una dimensión económica mucho más reducida que el proveedor. El cliente normalmente no podrá negociar con los proveedores las cláusulas del contrato, ya que estos ofrecen contratos de adhesión con cláusulas contractuales cerradas. De esta forma desaparece la posibilidad de modificar las condiciones de contratación.

Aún así, el cliente es el responsable de acuerdo a la Ley, aunque sea el proveedor el que incumpla su parte.

Por pura cuestión de prudencia, si un proveedor no deja claros los términos en que procesará los datos, habría que renunciar a la contratación de sus servicios.

Por otra parte, es muy probable que los datos no se almacenen en territorio español, lo que nos obliga a tener en cuenta que, de acuerdo al artículo 25 de la Directiva, la transferencia a un país tercero de datos personales únicamente puede efectuarse cuando el país tercero de que se trate garantice un nivel de protección adecuado. En caso

contrario solo se podría realizar la transferencia si se obtiene la autorización del Director de la AEPD, previa la aportación de garantías adecuadas.

Cuando el negocio se haya establecido entre el responsable establecido en España y un encargado de tratamiento no establecido, la transferencia de datos se considerará que reúne las garantías adecuadas si se basa en un contrato celebrado en los términos previstos en la Decisión de la Comisión Europea 2010/87/UE.

Cuando el negocio se haya establecido entre el responsable y un encargado establecidos en España, y sea este último quien subcontrata con un subencargado del tratamiento, ubicado en un país que no garantiza un nivel adecuado de protección, se considerará que reúnen las garantías adecuadas los contratos que incluyan las cláusulas contractuales tipo 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.

El artículo 44 de la LOPD califica como infracción muy grave la transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos. Las infracciones muy graves están sancionadas con una multa muy cuantiosa, de 300.001 a 600.000 euros.

Entonces un aspecto esencial es conocer el lugar al que se ha efectuado la transferencia de datos:

— Si la transferencia se ha efectuado a otro país que forma parte del Espacio Económico Europeo[25] no tendrá la consideración de transferencia internacional de datos. Por la misma razón no es necesaria la autorización de la AEPD.

— Cuando la transferencia se efectúa a alguno de los países con un nivel de protección que se considera adecuado por Decisión de la Comisión Europea, sí tendrá la calificación de transferencia internacional de datos, pero tampoco se necesita autorización de la AEPD.

[25] El Espacio Económico Europeo está formado por los 28 países integrantes de la UE más Islandia, Liechtenstein y Noruega. Se formó en 1994 para ampliar las disposiciones de la Unión Europea sobre el mercado interior a los países de la Asociación Europea de Libre Comercio (AELC). La legislación de la UE relativa al mercado interior pasa a formar parte del ordenamiento jurídico de los países del EEE cuando estos aceptan su incorporación.

— Si la transferencia de datos se efectúa a un país que no ofrece un nivel adecuado de protección será necesaria la autorización previa del Director de la AEPD. Dicha autorización deberá seguir el procedimiento previsto en el RLOPD.

Aquí es importante resaltar que, en relación al prestador de servicios en la nube, una cosa es la localización de la sede central de dicha empresa, y otra distinta es dónde se almacenan los datos. Así ocurre en el caso de las empresas multinacionales que tienen centros de proceso de datos repartidos por diferentes naciones del mundo, algunos dentro del Espacio Económico Europeo, otros en países con nivel adecuado de protección, y otros en terceros países sin las suficientes garantías.

Como antes ya se había mencionado, el problema con la contratación de estos servicios en la nube es que, habitualmente de manera automática, desaparece el conocimiento por parte del usuario sobre la ubicación física exacta de la información, así como de las condiciones de procesamiento. Pero legalmente corresponde al responsable del tratamiento dar cumplimiento a aquellos aspectos de la normativa de protección de datos que le sean exigibles conforme a la legislación española y, en particular, el cumplimiento de las reglas que rigen las transferencias internacionales de datos, si las hay. Ello exigiría que en todo caso se conociera con exactitud la ubicación de los servidores que contendrán la información. Y una vez se tuviese dicha información, si van a existir transferencias internacionales, proceder a la tramitación de su autorización.

A pesar de las duras sanciones fijadas en la LOPD a las transferencias internacionales de datos efectuadas sin autorización a países con un nivel de protección no adecuado, lo cierto es que el número de transferencias internacionales solicitadas por los interesados, y autorizadas por la AEPD, es muy reducido[26].

Y todavía es mucho más reducido el número de transferencias autorizadas para servicios de computación en la nube.

Todo parece indicar que hay un gran incumplimiento a la hora de declarar como transferencia internacional los servicios de computación en la nube en los que los datos son almacenados en países de protección no equiparable.

[26] Véanse en la página web de la Agencia Española de Protección de Datos las transferencias internacionales autorizadas hasta la fecha: www.agpd.es

Ese incumplimiento no siempre es voluntario. A veces se entiende que el tratamiento se está realizando en la UE o en un país con protección adecuada, cuando en realidad no es así. Otras veces se incumple la ley por desconocimiento de la obligación por parte del responsable del tratamiento. Pero estas razones no servirían para eximir de responsabilidad al cliente del servicio en la nube.

Es necesario que se aborden cambios legislativos a corto y medio plazo para mejorar las salvaguardias existentes y para ayudar al sector de la computación en la nube a resolver los problemas planteados, garantizando al mismo tiempo el respeto de los derechos fundamentales a la intimidad y a la protección de datos.

Algunos de los cambios normativos que deben hacer más fáciles los servicios en la nube se recogen en la propuesta de Reglamento de protección de datos de la UE, que con toda probabilidad se convertirá en la nueva normativa de la Unión en un próximo futuro.

IV. PRESTADORES DE SERVICIOS EN LA NUBE RADICADOS EN EEUU

Es una realidad que la mayoría de empresas prestadoras de servicios de computación en la nube son estadounidenses (Amazon, Microsoft, IBM, Google, Salesforce, Dropbox, Mailchimp), lo que nos lleva a analizar la situación jurídica actual en cuanto a las transferencias internacionales de datos.

En el momento en que entró en vigor en la Unión Europea la Directiva relativa a la protección de datos, surgió un problema muy importante con los Estados Unidos.

La Directiva sólo permite la transferencia de datos personales a aquellos países que ofrezcan un nivel adecuado de protección de la vida privada. Pero Estados Unidos no tiene una regulación completa de carácter general sobre la materia. Ello implica que no se puede considerar que Estados Unidos ofrezca un nivel adecuado de protección de la vida privada. Mientras que para la UE la protección de datos personales es un derecho fundamental de los ciudadanos, en Estados Unidos la protección de datos se considera un elemento disponible por parte de los ciudadanos, regulado parcialmente en una multitud de normas específicas y sectoriales sin conexión entre ellas, poniéndose casi todo el énfasis en la autorregulación y sin que exista una autoridad o autoridades de control encargadas de garantizar efi-

cazmente el cumplimiento de las reglas y la aplicación de unos estándares universalmente aceptados.

La Unión Europea y los Estados Unidos iniciaron en 1999 las negociaciones para encontrar un sistema que permitiese la declaración de adecuación del nivel de protección de datos personales en este último país.

El Departamento de Comercio de los Estados Unidos presentó una propuesta en la que se establecían los *Principios de Puerto Seguro*. En base a esta propuesta, los operadores que se adhiriesen a dichos *Principios* tendrían una presunción de adecuación a las exigencias de la Directiva 95/46/CE. Se obtendría así un mecanismo que permitiría la libre transferencia de datos personales.

Esos operadores deberían manifestar ante la Oficina Federal de Comercio, u otro organismo que ella hubiera designado, la adhesión a los Principios de Puerto Seguro y su compromiso de llevarlos a la práctica.

El Grupo de Trabajo sobre protección de datos del artículo 29, en su Dictamen 4/2000[27] sobre el nivel de protección que proporcionan los *Principios de Puerto Seguro*, expresó su posición crítica al acuerdo con Estados Unidos. Opinaba el Grupo de Trabajo que habría sido posible conseguir un mayor nivel de protección de los datos y que creía conveniente que se introdujeran mejoras.

A pesar de las críticas del Grupo de Trabajo, la Decisión 2000/520/CE[28] de la Comisión, considera que los *Principios de Puerto Seguro*, aplicados de conformidad con la orientación que proporcionan las preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos, garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a entidades establecidas en Estados Unidos de América.

Las modificaciones del régimen jurídico del tratamiento de datos personales incorporadas tras los atentados del 11 de septiembre no hicieron otra cosa que empeorar la situación de partida. A pesar de

[27] Documento de Trabajo WP 32, aprobado el 16 de mayo de 2000. Disponible en la página web del Grupo de Trabajo.

[28] Decisión 2000/520/CE, de 26 de julio de 2000, 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. Publicada en el DOCE L 215 de 25 de agosto de 2000.

ello Estados Unidos siguió estando en la lista blanca de países a los que Europa podía transmitir datos personales.

Este régimen ha durado 15 años ya que, el 6 de octubre de 2015, una Sentencia del Tribunal de Justicia de la Unión Europea (asunto C-362/14[29]) ha invalidado la Decisión 2000/520/CE y, en consecuencia, los acuerdos de Puerto Seguro.

La sentencia proclama que la Decisión de Puerto Seguro es inválida, entre otras razones, porque entiende que en EEUU prevalece incondicionalmente y sin ninguna limitación «la seguridad nacional, el interés público o el cumplimiento de la ley» sobre los derechos fundamentales a la intimidad y la protección de datos, sin otorgar a los ciudadanos europeos ningún medio para obtener la tutela efectiva de esos derechos.

Las consecuencias prácticas de la sentencia del Tribunal de Justicia de la Unión Europea son muy duras. El Grupo de Trabajo del art. 29 de la Directiva considera que está claro que las transferencias procedentes de la Unión Europea a EEUU ya no se pueden enmarcar en la Decisión de Adecuación de la Comisión Europea 2000/520/CE. Además, las transferencias que aún se estén llevando a cabo bajo la Decisión de Puerto Seguro, tras la sentencia del Tribunal de Justicia de la Unión Europea son ilegales.

El Grupo de Trabajo ha hecho un llamamiento urgente a los Estados miembros y a las Instituciones europeas para iniciar conversaciones con las autoridades de EEUU a fin de encontrar soluciones políticas, jurídicas y técnicas que permitan transferencias de datos al territorio de EEUU respetando los derechos fundamentales.

Si a finales de enero de 2016 no se ha encontrado una solución adecuada con las autoridades estadounidenses, y en función de la evaluación de las herramientas de transferencia por parte del Grupo de Trabajo, las autoridades de protección de datos de la UE se han comprometido a adoptar todas las medidas necesarias y apropiadas, que pueden incluir acciones coordinadas de aplicación de la ley[30].

En el hipotético caso de que las autoridades de protección de datos decidieran prohibir las transferencias a los Estados Unidos, las repercusiones económicas serían muy importantes ya que hay mu-

[29] Sentencia disponible en: http://curia.europa.eu/juris/liste.jsf?num=C-362/14

[30] Véanse la «nota de prensa» y la posterior «Nueva comunicación sobre la aplicación de la sentencia de Puerto Seguro» emitidas por la AEPD para aclarar su postura a partir de la sentencia del Tribunal de Justicia de la Unión Europea. Disponibles en su página web: www.agpd.es

chos servicios que no son ofrecidos por ningún proveedor establecido en el Espacio Económico Europeo, o que son ofrecidos con un nivel de calidad o prestaciones inferior.

V. CONCLUSIONES

Tal como se ha reiterado, la computación en nube permite al usuario optimizar la asignación y el coste de los recursos asociados a sus necesidades de tratamiento de información. El usuario no tiene necesidad de realizar inversiones en infraestructura sino que utiliza la que pone a su disposición el prestador del servicio, garantizando que no se generan situaciones de falta o exceso de recursos, así como el sobrecoste asociado a dichas situaciones. En este sentido, la computación en nube es una oportunidad para la mejora en la competitividad de las empresas.

A pesar de sus evidentes ventajas, deberá prestarse una atención especial a la hora de evaluar los riesgos jurídicos en materia de protección de datos, que afectan principalmente a las transferencias internacionales de datos. Tal como indica el Grupo de Trabajo de Protección de Datos del artículo 29, en su Dictamen 05/2012 sobre la computación en la nube, el cliente que quiera contratar servicios de computación en nube deberá verificar si el proveedor puede garantizar la legalidad de las transferencias de datos transfronterizas y limitar las transferencias a los países elegidos por el propio cliente. Las transferencias de datos a terceros países que no ofrezcan garantías, requerirán salvaguardias específicas mediante el uso de cláusulas contractuales tipo o normas corporativas vinculantes, según proceda. En modelos en la nube propietarios esto será más fácil de realizar, no así en los públicos en los que deberá prestarse especial atención a las condiciones en que se almacenan y tratan estos datos.

Además el problema se agrava por el hecho de que los clientes normalmente no podrán negociar con los proveedores las cláusulas del contrato, ya que estos ofrecen contratos de adhesión con cláusulas contractuales cerradas. En vista de la asimetría de la situación jurídica de los usuarios que sean pequeñas empresas frente a los grandes proveedores de computación en la nube, se necesitan cambios legales que permitan la negociación de unas condiciones generales más equilibradas con los proveedores. No podemos olvidar que el cliente que contrata los servicios en la nube sigue siendo responsable del tratamiento de los datos personales. Aunque los contrate con una gran compañía multinacional la responsabilidad no se desplaza al presta-

dor del servicio, ni siquiera incorporando una cláusula en el contrato con esta finalidad.

Todas estas razones obligan a que deban explorarse nuevas vías más sencillas que permitan una adecuada ponderación entre la protección de la intimidad y los legítimos intereses empresariales en un contexto multinacional.

Si a pesar de las dificultades regulatorias, el cliente que contrata servicios de computación en la nube puede garantizar el cumplimiento de la normativa en el campo de la protección de datos, tendrá una herramienta muy poderosa para el desarrollo de su negocio a un coste más reducido que las tecnologías de la información tradicionales.

En el caso de que no se pueda garantizar el cumplimiento de la legalidad, lo más prudente es buscar otro proveedor del servicio que sí permita dicho cumplimiento. Es recomendable no efectuar el «salto» a la nube si no se obtienen todas las garantías necesarias.