IMPLICACIONES LEGALES DE LA PRESTACIÓN DE SERVICIOS DE CLOUD COMPUTING. ESPECIAL REFERENCIA A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL[1]

LEGAL IMPLICATIONS REGARDING THE PROVISION OF CLOUD COMPUTING SERVICES. SPECIAL REFERENCE TO THE PROTECTION OF PERSONAL DATA

Sor Arteaga
Investigadora. Universidad Ceu San Pablo de Madrid

RESUMEN: La necesidad de las empresas de modernizar sus procesos, y prestar servicios de forma más eficiente y rentable, ha motivado incluir las tecnologías de la información y la comunicación (TICs) en sus actividades, utilizando nuevas formulas y modelos más rentables como el cloud computing, para el almacenamiento de ingente cantidad de datos e información, utilizando modernas técnicas de virtualización, que permiten además del ahorro de costes y tiempo, una gestión más eficaz, eficiente y flexible de sus recursos, la compartición de servicios e interoperabilidad de los datos, siendo uno de los principales retos a los que se enfrenta el cloud computing "la seguridad y la privacidad de los datos de carácter personal". En consecuencia, el presente trabajo pretende aproximarnos al análisis del marco normativo español aplicable a la prestación de servicios en la nube, identificando sus ventajas y desventajas; la responsabilidad del intermediario o del proveedor de servicios cloud, así como las garantías o mecanismos de protección de los usuarios, ofreciendo algunas recomendaciones a tomar en cuenta a la hora de contratar la prestación de servicios de computación en la nube.

PALABRAS CLAVE: cloud computing; protección de datos; legal; España.

ABSTRACT: *The need for companies to streamline their processes and deliver services in a more efficient and profitable*

[1] Este trabajo ha sido publicado en FODERTICS II: Hacia una justicia 2.0. Coordinado por Federico Bueno de Mata (2014). Ratio Legis Ediciones, Salamanca, ISBN: 9788494202803, en el marco del Proyecto I+D del Ministerio de Ciencia e Innovación. Ref. DER 2012-35948 sobre "Protección de Datos y Aplicación extraterritorial de las normas. La reforma de la Directiva sobre protección de datos" del que es investigador principal el Prof. José Luis PIÑAR MAÑAS.

way, has led to include Information and Communication Technology (ICT) into their regular activities, using new formulas and more profitable models such as Cloud Computing to store large amounts of data and information, using modern virtualization techniques which allow time and cost savings, a more effective, efficient and flexible management of resources, the sharing of services and interoperability of data; being the "security and privacy of personal data" one of the major challenges that Cloud Computing faces nowadays. Consequently, this paper aims to approach the reader to the analysis of the Spanish regulatory framework for the provision of Cloud Computing Services, identifying its advantages and disadvantages; the liabilities of intermediaries and Cloud Computing service providers, as well as guarantees or mechanisms of protections for users, offering some recommendations to consider when arranging the provision of Cloud Computing services.

KEYWORDS: *cloud computing; data protection; legal; Spain.*

SUMMARY: *Introduction; 1 Cloud Computing Services: definition and characteristics; 2 Cloud computing and the fundamental right to the protection of personal data; 3 Applicable Law, territoriality and international movement of data; Conclusions and recommendations; References.*

INTRODUCCIÓN

La aparición del modelo de "cloud computing", permite que determinados recursos de computación e infraestructura de comunicaciones, que normalmente se encontraban alojados en servidores locales, sean alojados por un tercero que, empleando dichos recursos e infraestructuras, ofrezcan servicios a medida de las necesidades de múltiples usuarios que acceden a aquellos a través de una red pública de comunicaciones como Internet, ofreciendo una gran flexibilidad tanto para los clientes de este tipo de servicios como para quienes los prestan.

El cloud computing ofrece mucho beneficios: para *el cliente* representa un coste de inversión en tecnología mucho menor que en el caso de mantener una estructura informática tradicional, pudiendo acceder a la información desde prácticamente cualquier lugar sin tener que preocuparse de los detalles técnicos, y para *el proveedor,* supone el poder prestar servicios a una multiplicidad de usuarios localizados en cualquier lugar del mundo y realizar una gestión más

eficaz, eficiente y flexible de sus recursos; activando o desactivando servicios en función de la demanda de sus clientes gracias entre otras cosas, a las modernas técnicas de virtualización.

Pese a ello, uno de los mayores riesgos del cloud computing es *la seguridad y la privacidad de datos*, por lo cual resulta importante conocer desde un punto de vista jurídico, la responsabilidad del intermediario o del proveedor de servicios cloud y las garantías o mecanismos de protección de los usuarios. Así las cosas, el presente trabajo abordará a través de diferentes herramientas de recogida y análisis de datos, basado en técnicas de investigación esencialmente cualitativas dos objetivos: por un lado, realizar un análisis descriptivo de las características que definen los servicios de computación en la nube, identificando en el capítulo I sus ventajas y desventajas; y por el otro, aproximarnos al marco normativo aplicable a los servicios de cloud computing a través del análisis del marco normativo español aplicable a la prestación de servicios en la nube (capítulos II y III), donde se identifican las medidas de seguridad que el prestador de servicios en la nube está obligado a implementar, ofreciendo en el capítulo IV algunas conclusiones preliminares y recomendaciones, interesantes para el debate de la protección del cloud computing, que deberán tomarse en consideración a la hora de contratar servicios en la nube.

1 SERVICIOS DE CLOUD COMPUTING: DEFINICIÓN Y CARACTERÍSTICAS

La popularización del acceso a Internet, el aumento de contenidos y servicios ofrecidos a través de una amplia variedad de dispositivos que permiten la información de manera deslocalizada por parte de los prestadores de servicios de acceso a Internet, han permitido el desarrollo del cloud computing, o computación en la nube[2], concepto que nace como una evolución de la prestación de servicios a través de Internet, que permite concentrar miles de máquinas virtuales flexibles "a medida" en grandes CPD[3].

[2] Pérez Arribas, David (2011). "*Análisis de los aspectos legales de la prestación de servicios de computación en la nube: la protección de datos de carácter personal y otras referencias legales*". Xª edición Máster en Auditoría Informática.

[3] Colom, José Luis (2012) "*Aspectos profesionales: Protección de datos, Cloud Computing y Sistemas de Gestión*". Disponible en: http://joseluiscolom.blogspot.com.es/2012/05/cloud-computing-y-proteccion-de-datos.html?goback=.gmr_3388897.gde_3388897_member_111969450 Fecha de acceso: 03.04.2013.

Así, si nos centramos en la "*nube*" propiamente dicha, se hace referencia a los servicios y al modelo de entrega de éstos, es decir, estaríamos ante una interpretación amplia del concepto de computación en la nube. En cambio, si nos referimos al concepto de "*computación*", se trataría de un concepto mucho más específico y ceñido a aquellas tecnologías que hacen posible esos servicios, principalmente la infraestructura y la virtualización.

Ante las abundantes y variadas definiciones presentes en la literatura, una de las más completas e integrales la ofrece el National Institute of Standards and Technology (en adelante, NIST)[4] del Departamento de Comercio de Estados Unidos, que define por computación en la nube como: "*un modelo que permite el acceso ubicuo a red bajo demanda a un conjunto de recursos de computación configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un esfuerzo mínimo de gestión o interacción por parte del prestador de servicios*".

En consecuencia, de la definición antes expuesta, se puede identificar *características* esenciales de la computación en la nube como lo son:

(i) Autoservicio bajo demanda, donde el usuario puede acceder a capacidades de computación "en la nube" de forma automática conforme a sus necesidades.

(ii) Compartición de recursos, (almacenamiento, memoria, ancho de banda, capacidad de procesamiento, máquinas virtuales, etc.) de los proveedores, que son compartidos por múltiples usuarios, a los que se van asignando capacidades de forma dinámica según sus peticiones.

(iii) Rápida Elasticidad, en el cual 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.

(iv) Servicio medido, donde 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] El NIST es el organismo encargado del desarrollo de estándares, guías y recomendaciones sobre requisitos mínimos para la adecuada provisión de seguridad de la información para todas las operaciones de agencias gubernamentales de los EE.UU. y sus activos, excepto para los sistemas de seguridad nacional.

1.1 MODELOS DE SERVICIOS DE CLOUD COMPUTING

Existen diversos modelos de servicio de cloud computing, siendo unas de las clasificaciones mas utilizadas la del NIST, que detallamos a continuación:

(i) *Software como Servicio (SaaS):* los servicios del cliente corren sobre una infraestructura de tipo nube, accesible desde varios dispositivos del cliente, donde el cliente paga un importe equivalente a un alquiler por el uso efectivo de los servicios.

(ii) *Plataforma como Servicio (PaaS):* se ofrece al cliente aplicaciones adquiridas o desarrolladas por el usuario empleando lenguajes de programación, librerías, servicios y herramientas soportadas por el prestador de servicios.

(iii) *Infraestructura como Servicio (IaaS):* La capacidad ofrecida al cliente consiste en proporcionar capacidad de procesamiento, almacenamiento (software virtual en la nube, donde el cliente instala lo que desea) funciones de red y otros recursos de computación fundamentales con los que el usuario es capaz de desplegar y ejecutar software arbitrario que puede incluir sistemas operativos y aplicaciones.

Por otra parte, en relación a la *distribución de la infraestructura* que da soporte a la prestación de servicios de computación en la nube y atendiendo a la titularidad de la misma, pueden diferenciarse los siguientes modelos de despliegue:

(i) *Nube Privada:* La infraestructura de nube es provisionada para su utilización por una única organización (empresa) que comprende múltiples usuarios.

(ii) *Nube Comunitaria:* es del uso exclusivo de una comunidad de usuarios específica. Su propiedad, gestión y operación puede corresponder a una o más de las organizaciones existentes en la comunidad, a un tercero o a una combinación de ambos, y puede existir dentro o fuera de las instalaciones de dichas organizaciones.

(iii) *Nube Pública:* es ofrecida al público general y su propiedad, gestión y operación puede corresponder a una organización gubernamental, académica, industrial o administrativa de carácter público, o a una combinación de las mismas.

(iv) *Nube Híbrida:* La infraestructura de nube está compuesta de dos o

más infraestructuras de nube (privadas, comunitarias o públicas) que permanecen como entidades únicas pero están unidas entre si mediante tecnología estándar o propietaria que permite la portabilidad de aplicaciones y de los datos como, por ejemplo, el "*cloud bursting*" para el balanceo de carga entre nubes. (Perez Arribas, D. 2011)

1.2 VENTAJAS Y DESVENTAJAS DEL CLOUD COMPUTING

Las *ventajas o beneficios* de la computación en la nube está condicionada por el tipo de modelo de servicio. Así podemos citar, entre otras las siguientes:

(i) Económico financieras: Reduce costes de inversión en tecnología y maximiza el retorno de la inversión con la eliminación de gastos en CPDs, servidores, instalaciones, personal, etc. Si se apuesta por un modelo de nube pública o privada financiada y operada por un tercero, los costes a afrontar por los clientes serán, básicamente, operacionales.

(ii) Ubicuidad en el acceso a los datos y disponibilidad: Permite el acceso a los datos desde cualquier lugar y en cualquier momento.

(iii) Escalabilidad: Se adapta tanto a las necesidades de las grandes empresas como a las de una pyme.

(iv) Fiabilidad: Los servicios son más fiables y robustos que los sistemas de computación tradicionales, ofreciendo una mayor flexibilidad y capacidad de respuesta en caso de que se produzca una interrupción del servicio.

Por otra parte, como contrapartida entre las *desventajas* propias del modelo de cloud computing se pueden citar:

(i) Dependencia del acceso a Internet y de una conexión y ancho de banda adecuado.

(ii) Dependencia del proveedor de los servicios tecnológicos y pérdida de control por parte de clientes: dependiendo de la modalidad de cloud seleccionada y contratada.

(iii) Gran desconocimiento en el mercado de lo que es y las ventajas que ofrece.

(iv) Existencia de interfaces y proveedores poco seguros, problemas de cumplimiento normativo derivados de la localización de los datos,

problemas derivados de la compartición de infraestructuras, etc. [5]

(v) Casos de abuso y mal uso de los servicios (SLA), ataques internos de los usuarios del servicio y del personal del proveedor, el secuestro de sesiones de usuarios o del servicio.[6]

(vi) Y finalmente una de las principales desventajas que enfrenta el cloud computing es la garantía de la "*Confidencialidad y Seguridad de los datos*". Al respecto, el informe de la ONTSI[7] destaca que la preocupación más recurrente para las pymes no usuarias del cloud es la seguridad y confidencialidad de los datos corporativos (60,1%), seguida de la disponibilidad de los servicios y datos por parte del proveedor (32,7%), la pérdida de control sobre los procesos (27,4%) y la dependencia adquirida hacia el proveedor (26,1%).

2 EL CLOUD COMPUTING Y EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

El derecho a la protección de los datos de carácter personal se establece en el artículo 8 de la Carta de los Derechos Fundamentales, en el artículo 16 del Tratado de Funcionamiento de la Unión Europea y en el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las libertades fundamentales (CEDH). En el ordenamiento jurídico español, está desarrollado en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y su Reglamento de desarrollo (Real Decreto 1720/2007, de 21 de diciembre, RLOPD) cuyas disposiciones resultan aplicables a la contratación de servicios en la nube, cuando se almacenen datos de carácter personal.

2.1 RESPONSABILIDAD DE LOS ACTORES EN EL SERVICIO DE CLOUD COMPUTING

2.1.1 En Cloud Computing, el Cliente que contrate los servicios tendrá la condición de Responsable del tratamiento (art. 3.d) de la LOPD y art. 5.1.q) del RLOPD), pues a él le corresponde la decisión sobre la finalidad, el contenido y uso del tratamiento, así como la decisión sobre optar por la computación en la nube y sobre su modalidad

[5] INTECO-CERT (2011). "Riesgos y Amenazas en Cloud Computing", marzo 2011.

[6] Idem.

[7] ONTSI (2012) Cloud computing. Retos y oportunidades. Resumen ejecutivo. p. 8-9.

Para ello, tiene la obligación legal de *transparencia y diligencia en la contratación*. Deberá conocer dónde, cuándo y quién procesa los datos, y velará porque el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en la normativa de protección de datos (art. 20.2 RLOPD).

Al respecto, la Agencia Española de Protección de Datos (AEPD, 2013)[8] ha publicado una "*Guía para clientes que contraten servicios de cloud computing*", en el que incluye una lista de control, con 12 preguntas a tener en cuenta por el cliente, sobre las garantías exigibles al proveedor, resaltando entre los aspectos a tomar en cuenta antes de la contratación: la evaluación de la tipología de datos y los niveles de seguridad incluyendo la información sobre los tipos de nube y de servicios; la responsabilidad de las partes; la legislación aplicable; las obligaciones como cliente; la ubicación de los datos personales; las garantías adecuadas para las transferencias internacionales de datos; las medidas de seguridad exigibles y garantías sobre las mismas; los compromisos de confidencialidad; la garantía de la portabilidad de los datos; la destrucción de los datos una vez finalizado el contrato, y la garantía de los derechos ARCO.

Estas garantías también han de proporcionarlas aquellas compañías que actúan como *partners* de otros proveedores de cloud computing, en cualquiera de las figuras de *reseller*, agregadores de servicios de *cloud*, *cloud builders*, proveedores de aplicaciones, etc., y que proporcionan servicios contratando directamente con los clientes.

Asimismo, el cliente que contrate servicios de cloud computing, al seguir siendo el responsable del tratamiento de los datos personales, está obligado a facilitar el ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición) de los interesados en los plazos previstos en la ley.

2.1.2 Por su parte, el intermediario o prestador de servicios de Cloud Computing tendrá la naturaleza de Encargado del tratamiento (art. 3.g) de la LOPD y (art. 5.1.i) del RLOPD, pues en definitiva tratará los datos personales por cuenta y orden del responsable

Entre sus obligaciones, deberá respetar los principios de protección de datos, garantizar los derechos ARCO, y cumplir con las previsiones de los artículos 20 a 22 del Reglamento, referidas al encargado del tratamiento.

[8] AEPD (2013). *Guía para clientes que contraten servicios de cloud computing*. Agencia Española de Protección de Datos. disponible en www.agpd.es (Fecha de acceso: 01.05.2013).

Asimismo, tendrá que firmar con el cliente un *contrato de prestación de servicios de tratamiento de datos personales* por cuenta de terceros, que deberá formalizarse por escrito (art. 12 LOPD) e incluir las medidas de seguridadprevistas en el art. 9 de la LOPD, definiendo las condiciones de seguridad concretas, e informando al cliente de forma detallada sobre las medidas de seguridad a cumplir.

Aunado a ello, ha de *garantizar la conservación de los datos*, mediante la realización de copias de seguridad periódicas y dotando su infraestructura de los mayores niveles de seguridad. Deberá establecer *mecanismos seguros de autenticación* para el acceso a la información por parte del cliente, e información sobre las técnicas de cifrado de la información que aplique en sus sistemas.

Por otra parte, será fundamental que acuerde un *procedimiento de recuperación y migración de los datos* a la terminación de la relación contractual; así como el mecanismo de borrado de los datos una vez que estos han sido transferidos al cliente o al nuevo proveedor designado por éste.

En definitiva, los *aspectos a incluir en los contratos de cloud computing*, y destacados en el estudio elaborado por el Consejo General de la Abogacía Española (CGAE)[9] y la AEPD, son:

(i) Objeto, tipo de servicio cloud, características, obligaciones de las partes, SLA, etc.

(ii) Régimen de los datos, que especifique que el proveedor no puede disponer de los datos personales ni hacer uso de los mismos para ningún fin que no esté autorizado.

(iii) Consecuencias de la extralimitación por parte del proveedor de Cloud en su calidad de encargado del tratamiento, en virtud de la cual pasará a asumir la condición de responsable del fichero (art. 12.4 LOPD).

(iv) Disponibilidad. El proveedor ha de garantizar una elevada disponibilidad del servicio.

(v) Portabilidad. Entendida como la posibilidad efectiva de transferir datos y aplicaciones de un proveedor a otro. Para ello, es necesario que los datos personales puedan ser devueltos al cliente o que éste pueda indicar que se transfieran a un nuevo proveedor de servicios

[9] CGAE (2012). Informe "*Utilización del 'cloud computing' por los despachos de abogados y protección de datos de carácter personal*" Elaborado por el CGAE y la AEPD. Publicado en julio del 2012 y disponible en www.agpd.es (Fecha de acceso: 12.08.2012).

que haya seleccionado, en el momento en que finalice la prestación del mismo, es una garantía que ha de tenerse especialmente en cuenta.

(vi) Consecuencias en caso de incumplimiento del proveedor de sus obligaciones.

(vii) Regulación en caso de subbcontratación de servicios por parte del proveedor, etc.

3 LEY APLICABLE, TERRITORIALIDAD Y TRANSFERENCIA INTERNACIONAL DE DATOS

La *ley aplicable* en los servicios de cloud computing será la del domicilio *del cliente,* independientemente del país donde se ubiquen los ficheros con datos de carácter personal en la nube. Por tanto, si los clientes y responsables del tratamiento están sujetos a la normativa española, la relación jurídica con el prestador de servicios estará sujeta a la LOPD y su reglamento de desarrollo, y no será una cuestión negociable o disponible para las partes.

En relación a la *territorialidad*, por la propia naturaleza del modelo Cloud Computing los datos almacenados en la nube se podrán encontrar en un servidor ubicado en cualquier lugar del mundo, con una ubicación por lo general desconocida por el usuario.

Si los datos están en España, aplicará la normativa vigente en protección de datos. Pero si por el contrario, están en un tercer país, aplica la normativa referida a *transferencias internacionales de datos*, regulada en los artículos 33 y 34 de la LOPD, el Título VI del RLOPD, y en los artículos 26 y 25 de la Directiva 95/46/CE.

En estos casos es preciso tener en cuenta que no se pueden realizar transferencias internacionales de datos a países que no dispongan de un nivel adecuado de protección, salvo que se obtenga, previa la aportación de garantías adecuadas y la autorización del Director de la AEPD. El incumplimiento de esta autorización, será considera una infracción muy grave sancionable con multa entre 300.001 – 600.000 euros.

A estos efectos, hay que distinguir:

(i) Si la transmisión de los datos derivada de la prestación de los servicios de Cloud se realiza en el territorio de la UE, no tienen la consideración de transferencia internacional de datos, según el artículo 5.1.s) del RLOPD, por lo que no resulta necesaria la autorización de la AEPD.

(ii) 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*.

(iii) Igualmente los proveedores radicados en los EEUU que se hayan adherido voluntariamente para la prestación de estos servicios al acuerdo de "puerto seguro" (safeharbor), en virtud del cual se obligan a cumplir requisitos equivalentes a los europeos en materia de protección de datos.

(iv) Otra alternativa es que el proveedor de Cloud haya obtenido una autorización previa del Director de la AEPD para realizar transferencias internacionales de datos a subencargados establecidos en terceros países basada en cláusulas contractuales en las que el cliente autorice los servicios susceptibles de subcontratación (CGAE, 2012), como lo son las BCR.

En caso de *subcontratación de servicios de cloud*, es especialmente importante, dadas las características propias de los servicios de cloud computing, establecer mecanismos para permitir que las subcontrataciones que se realicen en este contexto de transferencias internacionales se gestionen con fluidez, asegurando al mismo tiempo que el cliente responsable tiene información suficiente sobre los subcontratistas, o potenciales subcontratistas, y mantiene la capacidad de tomar decisiones. Al respecto, la Guía para clientes que contraten servicios de cloud computing de la AEPD (2013) señala que el cliente *debe dar su conformidad* (al menos delimitando genéricamente los servicios), asimismo, tiene que poder identificar a los subcontratistas y su ubicación (a través de una página web, actualizable), regular la posibilidad de finalizar el contrato de tratamiento, y obtener la autorización de la AEPD al margen de las garantías aportadas por las cláusulas tipo (arts. 26.2 Directiva 95/46, 33 LOPD, 66 y 70 RLOPD, Decisión 2010/87, considerando 5).

Asimismo, es importante resaltar que la AEPD dispone en su web de un modelo de contrato entre (encargado y subencargado) y ha puesto en marcha desde el 2012, clausulas elaboradas cuando el contrato se celebra entre encargado, exportador, y subencargado importador de los datos. La autorización de la AEPD se trata de una autorización marco, que habilita al encargado-exportador para realizar tantas transferencias como clientes tenga sin necesidad

de solicitar una autorización por cada uno de los clientes. Es Obligatorio tener suscrito el contrato tipo con el responsable del tratamiento (a disposición de la AEPD). Asimismo, será necesario notificar al RGPD los ficheros a los que afecta la transferencia a realizar al amparo de la resolución con carácter previo.

CONCLUSIONES Y RECOMENDACIONES

El uso del cloud computing fomenta el desarrollo industrial y digital, y es una herramienta clave para garantizar la competitividad de las empresas españolas, especialmente de las pymes (AEPD, 2013). No obstante, en la práctica las empresas europeas prestadoras de servicios de cloud computing, se encuentran en una posición de desventaja competitiva, al tener que garantizar el cumplimiento de la normativa europea en materia de protección de datos, frente a otras empresas procedentes de países no miembros de la unión.

Por ello, uno de los retos pendientes en Europa debe ser mejorar las condiciones de los proveedores de servicios de cloud computing, manteniendo la protección y garantía de los clientes, donde la "*Seguridad, transparencia y seguridad jurídica*" deben ser los factores claves que deben estar presentes en las ofertas de servicios en la nube (GT29, 2012)[10].

El cliente como Responsable del Fichero, deberá seleccionar un proveedor de cloud que garantice contractualmente el cumplimiento de la normativa de protección de datos, la legitimidad de las transferencias de datos internacionales y las garantías suficientes en términos de medidas técnicas y organizativas. Asimismo, tendrá que tomar en consideración las recomendaciones expuestas por la AEPD identificadas en el presente trabajo, y en especial deberá contar con un *contrato de Encargado de Tratamiento,* y en caso de subcontratación, con un *contrato de acceso a los datos*, que establezca las condiciones y garantías necesarias para garantizar el nivel de protección de datos personales (Decisión de la Comisión Europea 2010/87/UE)[11].

Asimismo, en caso de tratarse de prestadores de servicios no establecidos en la UE, se recomienda solicitar estándares reconocidos en materia de

[10] GT29 (2012). Grupo Europeo de Protección de Datos del Artículo 29. Opinión sobre cloud computing. 2012.

[11] Colom, José Luis (2012) "*Aspectos profesionales: Protección de datos, Cloud Computing y Sistemas de Gestión*". Disponible en:http://joseluiscolom.blogspot.com.es/2012/05/cloud-computing-y-proteccion-de-datos.html?goback=.gmr_3388897.gde_3388897_member_111969450 (Fecha de acceso: 03.04.2013).

seguridad[12], certificaciones como ISO/IEC 27001, disponer un buen acuerdos de nivel de servicio (SLA) y establecer la posibilidad de realizar auditorias por un personal especializado.

Por último, es importante destacar que en la actualidad se está discutiendo en Europa la Reforma del marco normativo europeo de protección de datos, con la propuesta de un nuevo Reglamento Europeo que sentará las bases de la regulación de la protección de datos y unificará la normativa en los países de la UE. Entre los aspectos novedosos del Reglamento, que afectan a los servicios de cloud computing destaca la aplicación de la nueva regulación de las empresas no europeas que ofrezcan sus servicios y productos en la unión, quienes deberán designar un representante. Asimismo, se establecen algunas disposiciones en cuanto a la seguridad de los datos, y obligaciones para los encargados de tratamiento. Aspectos, que junto a otras novedades como la regulación de la figura del DPO, las evaluaciones de impacto para la privacidad, la protección de los menores, y la creación del Consejo Europeo de Protección de Datos, representan nuevos retos y cambios significativos en la regulación, interesantes de abordar, que serán objeto de estudio y profundización en futuros trabajos de investigación.

REFERENCIAS

AEPD (2013). *Guía para clientes que contraten servicios de cloud computing*. Agencia Española de Protección de Datos. disponible en www.agpd.es (Fecha de acceso:01.05.2013)

CGAE (2012).Informe "*Utilización del 'cloud computing' por los despachos de abogados y protección de datos de carácter personal*" Elaborado por el CGAE y la AEPD. Publicado en julio del 2012 y disponible en www.agpd.es (Fecha de acceso: 12.08.2012)

COLOM, José Luis (2012) "*Aspectos profesionales: Protección de datos, CIoud Computing y Sistemas de Gestión*". Disponible en: http://joseluiscolom.blogspot.com.es/2012/05/cloud-computing-y-proteccion-de-datos.html?goback=.gmr_3388897.gde_3388897_member_111969450 Fecha de acceso: 03.04.2013.

GT29 (2012). Grupo Europeo de Protección de Datos del Artículo 29. Opinión sobre cloud computing. 2012

[12] Al respecto, destacan informes sobre la estructura de control interno del proveedor como: Statement on Auditing Standards nº 70 Type I y II, Statement on Standards for Attestation Engagements 16 Distribuido por AICPA (American Institute of Certified Public Accountants), o el International Standard on Assurance Engagements 3402 Estándar internacional desarrollado por IAASB (International Auditing and Assurance Standards Board).

INTECO-CERT (2011). "Riesgos y Amenazas en Cloud Computing", marzo 2011.

ONTSI (2012) Cloud computing. Retos y oportunidades. Resumen ejecutivo. p 8-9.

PÉREZ ARRIBAS, David (2011). "*Análisis de los aspectos legales de la prestación de servicios de computación en la nube: la protección de datos de carácter personal y otras referencias legales*". Xª edición Máster en Auditoría Informática.

PIÑAR MAÑAS, en "Seguridad, transparencia y protección de datos: el futuro de un necesario equilibrio", Documento de Trabajo 147/2009, Fundación Alternativas, 2009.