INICIACIÓN A LA INVESTIGACIÓN
REVISTA ELECTRÓNICA
UNIVERSIDAD DE JAÉN

"DERECHO Y NUEVAS TECNOLOGÍAS: LUCES Y SOMBRAS DEL CLOUD COMPUTING"

David Marrero Blanco
Escuela de Doctorado – Universidad de Jaén
david.marrero@icajaen.es

ABSTRACT

Parece ya innegable que el Cloud Computing, aunque todavía no ha alcanzado su pleno potencial, ha supuesto un punto de inflexión -un "nuevo paradigma"-, que está cambiando radicalmente la forma en que usamos los servicios TIC (Tecnologías de la Información y la Comunicación). No obstante, aún hay algunas sombras en torno a esta nueva manera de entender y utilizar las tremendas posibilidades que nos ofrece Internet, sobre todo en lo referente a calidad del servicio y protección de datos personales.

En este breve artículo definiremos sucintamente cuáles son los pros y contras que conlleva utilizar servicios de Cloud Computing, fundamentalmente desde una perspectiva de privacidad y protección de datos personales.

Comenzando por las ventajas, podemos señalar la simplicidad de uso y el considerable ahorro de costes que aportan las soluciones *Cloud Computing*, permitiendo que el usuario pueda optimizar la asignación y el precio de los recursos asociados a sus necesidades de tratamiento de información. Así, los servicios tecnológicos pasan a ser un gasto operativo, obviándose la necesidad de inversiones en infraestructuras de breves ciclos de vida y rápida obsolescencia[1].

De hecho, la principal diferencia que aporta el Cloud Computing con respecto a los modelos tradicionales de negocio radica en la posibilidad de aumentar de forma gradual y escalable, a petición del cliente, el número de servicios prestados a través de Internet. Esto genera beneficios tanto para los proveedores –que pueden ofrecer de forma más rápida y eficiente un mayor número de servicios- como para los usuarios o clientes –quienes tienen la posibilidad de

[1] "Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal". Informe elaborado por la AEPD y el CGAE, 2012.
[http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/junio/informe_CLOUD.pdf]

acceder a dichos servicios disfrutando de la sencillez e inmediatez del sistema y, potencialmente, de un modelo de pago por consumo[2].

Otro punto a favor del Cloud Computing es que el cliente tiene asegurado –al menos en teoría- el acceso a los servicios desde cualquier lugar del mundo en el que se disponga de una conexión a Internet, así como el hecho de que el proveedor de Cloud Computing normalmente asegura la disponibilidad del servicio y la actualización permanente de aplicaciones y sistemas.

Ahora bien, es importante señalar que sin calidad de servicio no se puede tener Cloud Computing. En este sentido, el experto en Internet Andrew Blum, en su obra Tubes[3], destaca cómo los defensores del Cloud Computing desdeñan la importancia de la infraestructura en el entorno digital, cuando lo cierto es que –al menos hoy por hoy- sin los cables que transportan la señal, ninguna Internet es posible, ni en *la nube* ni en nuestro servidor doméstico o empresarial. Es más, si carecemos del ancho de banda suficiente, no tendremos ni la capacidad ni la velocidad que el Cloud requiere, y por lo tanto será inoperativo a efectos prácticos.

En lo referente a la privacidad, el Grupo de Trabajo del artículo 29, en su Opinión 05/2012, ha advertido acerca de los riesgos que el Cloud Computing puede generar en lo relativo a la confidencialidad, disponibilidad, integridad, y portabilidad de los datos, ya que este tipo de servicios TIC pueden llegar a poner en peligro la libertad de disposición que sobre su propia información pueden tener las empresas, un aspecto en absoluto baladí, pues en la actualidad probablemente el activo más valioso de una compañía sea su información. Estos son los principales riesgos del Cloud Computing descritos en dicho informe[4]:

- **Disminución de la disponibilidad de información** debido a la merma en la interoperabilidad, lo que acaba provocando clientes "cautivos" de un sólo proveedor. Es el caso de clientes que contratan exclusivamente con un solo proveedor de *Cloud*, ya que éste les garantiza un servicio completo, pero que posteriormente tienen problemas a la hora de transferir sus datos y documentos entre sistemas de distintos proveedores de nubes (disminución del *data portability*) o de intercambiar información con otras entidades que utilizan un sistema diferente de *nubes* (interoperabilidad)

- **Disminución de la integridad de los sistemas**, ya que los servicios Cloud se realizan normalmente a través de sistemas y recursos compartidos. De esta forma, los datos personales de personas físicas u organizaciones están dentro de infraestructuras de seguridad mucho más complicadas.

- **Disminución de confidencialidad:** El proveedor del servicio Cloud puede encontrarse prácticamente en cualquier lugar del mundo, y su objetivo último será proporcionar los servicios citados optimizando sus propios recursos –a través de, por ejemplo, prácticas de deslocalización, compartición de recursos y movilidad o realizando subcontrataciones adicionales-, lo que puede implicar un riesgo para el cliente, ya que los servidores donde se aloje la información de la nube podrían no encontrarse dentro del ámbito territorial de la UE, ni de alguno de los países que la UE determine como "seguros" en materia de protección de

[2] GARCÍA DEL POYO, Rafael. "Cloud Computing: aspectos jurídicos clave para la contratación de estos servicios", *Revista Española de Relaciones Internacionales.* Núm. 4, 2012. ISSN 1989-6565

[3] BLUM, Andrew. *Tubes: A Journey to the Center of the Internet*, Edit. Viking/Penguin, U.K., 2012

[4] Opinión 5/2012 emitida el 1 de Julio de 2012 por el grupo de trabajo del artículo 29

datos, y por lo tanto no cumplirían con la normativa de seguridad que exige la UE en esta materia.

- **Disminución de la capacidad de control** por parte del cliente, debido a la frecuente externalización de los servicios que realizan los proveedores, quienes suelen utilizar a su vez otros proveedores (subencargados) que pueden cambiar a lo largo del contrato, dificultando el control del cliente sobre los mismos y pudiendo provocar cambios durante la prestación del servicio. Así, en función del modelo utilizado, los datos pueden no estar realmente en manos del contratista, toda vez que la propiedad, el mantenimiento y gestión del soporte físico de la información, los procesos y las comunicaciones pueden encontrarse en manos de terceros no autorizados.

Es de destacar también que los clientes que utilizan servicios Cloud entregan a un tercero valiosa información de su negocio y los datos personales de los que disponen, y esta información recorre diferentes nodos para llegar a su destino, y lo cierto es que cada uno de ellos –así como sus respectivos canales de acceso- pueden convertirse en un foco permanente de inseguridad. Precisamente por esto se deben utilizar protocolos seguros[5].

En este sentido, un reciente informe[6] de la Asociación de Expertos Nacionales en Abogacía TIC (ENATIC), en colaboración con el Instituto Nacional de Tecnologías de la Información (INTECO), destaca que sólo en el plano empresarial venimos siendo testigos de ciberataques y fugas de información cada vez más habituales y graves, que no sólo causan grandes daños económicos y de reputación a las entidades que los sufren, sino también de confianza por parte de los ciudadanos, hechos que ponen en peligro los usos innovadores de las Nuevas Tecnologías y el normal desarrollo de la Economía Digital.

Otra de las cuestiones que más riesgos conlleva a la hora de contratar servicios Cloud es la relativa al **"data residency"**, es decir, saber en qué país –y por tanto bajo qué jurisdicción- están los datos en cada momento. La situación se complica aún más cuando el proveedor subcontrata a terceros, normalmente socios o *partners*, algunos elementos necesarios para implementar el servicio Cloud que dicho proveedor ofrece al cliente –hardware, almacenamiento, etc.-, y todo puede complicarse aún más porque los subcontratistas –que en materia de protección de datos asumirían el rol de "subencargado de tratamiento"- pueden a su vez subcontratar de nuevo parte del servicio que proporcionan al prestador final –el proveedor que realmente ha firmado el contrato con el cliente- a terceras y sucesivas compañías.

Esta cadena de subcontrataciones, cuyo objeto es redimensionar continuamente los recursos de la *nube* de forma dinámica y en función de las condiciones del mercado, en teoría podría no tener fin, y los riesgos en lo relativo a la protección de datos personales pueden aumentar considerablemente.

Palabras clave: Nuevas tecnologías / Servicios TIC / Protección de datos / Privacidad / Derecho contractual / Derechos fundamentales / Cloud Computing / Contratos TIC

---

[5] GARCÍA DEL POYO, Rafael. Op. Cit.

[6] SAIZ, Carlos y PÉREZ BES, Francisco (coordinadores). "La responsabilidad legal de las empresas frente a un ciberataque", ISMS Forum Spain - ENATIC, Madrid 2014

BIBLIOGRAFÍA BÁSICA

BLUM, Andrew. *Tubes: A Journey to the Center of the Internet*, Edit. Viking/Penguin, U.K., 2012

GARCÍA DEL POYO, Rafael. "Cloud Computing: aspectos jurídicos clave para la contratación de estos servicios", *Revista Española de Relaciones Internacionales.* Núm. 4, 2012. ISSN 1989-6565

MARTÍNEZ MARTÍNEZ, Ricard. *Derecho y Cloud Computing.* Editorial Aranzadi, Madrid, 1ª edición, 2012

ROSSBACH, Carsten y WELZ, Bernd. "Survival of the fittest. How Europe can assume a leading role in the cloud". Roland Berger Strategy Consultants, SAP. 2011

SAIZ, Carlos y PÉREZ BES, Francisco (coordinadores). "La responsabilidad legal de las empresas frente a un ciberataque", ISMS Forum Spain - ENATIC, Madrid 2014

OTRAS FUENTES

Opinión 5/2012 emitida el 1 de Julio de 2012 por el grupo de trabajo del artículo 29

"Guía para clientes que contraten servicios de Cloud Computing", Agencia Española de Protección de Datos, 2013
[http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf]

"Orientaciones para prestadores de servicios de Cloud Computing", Agencia Española de Protección de Datos, 2013
[http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIENTACIONES_Cloud.pdf]

"Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal". Informe elaborado por la AEPD y el CGAE, 2012.
[http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/junio/informe_CLOUD.pdf]