Fecha de recepción: 31 de enero de 2013 / Fecha de aprobación: 18 de abril de 2013

Revista de Derecho Comunicaciones y Nuevas Tecnologías

Jurisdicción aplicable en materia de datos personales en los contratos de cloud computing:análisis bajo la legislación colombiana

Gonzalo Andrés Moreno Gómez

Universidad de los Andes
Facultad de Derecho
Revista de Derecho, comunicaciones y Nuevas Tecnologías
N.º 9, Junio de 2013. ISSN 1909-7786

Jurisdicción aplicable en materia de datos personales en los contratos de cloud computing: análisis bajo la legislación colombiana*

Gonzalo Andrés Moreno Gómez**

Resumen

El Cloud Computing representa una forma de almacenamiento y administración de información en servidores que en la mayoría de los casos se encuentran en jurisdicciones diferentes a la del contratante. Al tratarse de un reciente fenómeno tecnológico donde los ordenamientos jurídicos se encuentran un paso atrás es necesario hacer un análisis de las relaciones contractuales y obligaciones que surgen de esta novedad a la luz de la jurisdicción aplicable a los contratos, concentrándonos en la protección de datos personales.

Palabras clave: Cloud computing, computación en la nube, software como servicio, plataforma

Abstract

Cloud computing represents a way of storing and managing information on servers which, in most cases, are in different jurisdictions than the contractors; being a new technological phenomenon the legal systems are a step back, needing to do an analysis of the contractual relationships and obligations arising from this technology. At the same time address the issue of jurisdiction for the contracts, focusing on the specific aspects of data protection.

Keywords: Cloud computing, software as a service, platform as a service, infrastructure as a

---

* Este documento es una parte de la investigación que se realizó para obtener el título de Magister en Derecho Privado de la Universidad de los Andes, dicha investigación se centró en analizar los efectos jurídicos de los servicios denominados cloud computing, que tienen como característica particular la posibilidad de prestarse en demanda a través de internet, sin importar las jurisdicciones en las cuales se encuentre el ofertante y contratante, al tener los mismos efectos jurídicos para las partes que si se tratara de una contratación física y no virtual. En este documento se analizará la naturaleza jurídica de los servicios cloud, los efectos de la contratación en la nube para los datos personales y sus implicaciones bajo la legislación colombiana, efectos a los que se aplican las normas jurídicas vigentes en el Estado colombiano aunque se generan en un espacio inmaterial.

** Abogado, Pontificia Universidad Javeriana de Bogotá, Colombia y Universidad del País Vasco de San Sebastián, España. Especialista en derecho comercial, tributación y Magister en derecho privado de la Universidad de los Andes. Actualmente es Gerente de Nuevos Negocios & Apoyo Estratégico de la Organización Staffing de Colombia, profesor de Cátedra de Derecho Comercial en la Universidad de los Andes y miembro del Grupo de Estudios en internet Comercio electrónico, Telecomunicaciones e Informática GECTI de la Universidad de los Andes. Correo electrónico: gonzalomorenogomez@gmail.com

como servicio, infraestructura como servicio, jurisdicción, contratos, responsabilidad civil, protección de datos personales, transferencia internacional de datos.

service, jurisdiction, contracts, liability, data protection, international data transfers.

Sumario

Introducción

El Cloud Computing (computación en la nube) representa una forma de prestar servicios a través de internet utilizando data centers que, en la mayoría de los casos, se encuentran en jurisdicciones diferentes a la del contratante, lo cual genera como consecuencia un dilema de aplicación espacial del derecho. Se trata de un fenómeno que revolucionó la forma de consumo de almacenamiento de datos, el desarrollo de aplicativos, el acceso a software en internet con un costo menor al reducir la capacidad instalada de las empresas[1].

Las relaciones jurídicas que se originan a causa de este fenómeno están quedando en un limbo pues no se tiene claridad sobre el lugar donde tiene efectos el contrato, ya que no se conoce la ubicación física de los data centers, la sede del proveedor del servicio y/o la ubicación del usuario. Dado que la contratación se da en la web en la mayoría de los casos y los pagos se realizan por medios electrónicos, las partes no llegan a interactuar físicamente, razón por la cual la ubicación, para efectos legales, podría ser definida por el lugar donde se encuentren los data centers e, incluso, donde estén los consumidores finales.

Dentro de la problemática descrita anteriormente aparece el el objetivo fundamental del presente escrito que es analizar el vínculo contractual que surge de un contrato de computación en la nube y los problemas de jurisdicción que surgen de la relación contractual en la nube. Ahora bien, los problemas de jurisdicción en materia de cloud computing tendrán un tratamiento diferente dependiendo de la naturaleza del fenómeno jurídico que se estudie, pudiéndose presentar discrepancias en materia de: ley aplicable por actuaciones criminales, responsabilidad civil, relaciones contractuales, impuestos y protección de datos. El presente escrito pretende hacer un análisis particular de este último aspecto.

Para tal efecto analizaremos el concepto técnico de cloud computing, sus antecedentes, los tipos de computación en la nube y los esquemas comerciales utilizados en la actualidad, para luego estudiar la figura contractual, los problemas de ley y de jurisdicción en materia de protección de datos.

I. MARCO CONCEPTUAL DEL CLOUD COMPUTING

El análisis del computing debe partir del estudio del concepto como tal y para ello, partiremos en el presente escrito, de la definición para luego adentrarnos en sus particularidades.

A. Definición Cloud Computing

Aunque normalmente la definición de cloud computing es de origen doctrinal y empresarial, la regulación extranjera reciente ha incursionado en esta cuestión. Este es el caso de los Estados Uni-

1 Sobre este tema se puede consultar: Marston, S., Zhi Li, Bandyopadhyay, S. & Ghalsasi, A. (2011). Cloud Computing - The Business Perspective. En System Sciences *(HICSS), 2011 44th Hawaii International Conference*. 4, (*7),* 1-11.. doi: 10.1109/HICSS.2011.102; Petcu, D. (2010). Identifying Cloud computing usage patterns. *Cluster Computing Workshops and Posters (CLUSTER WORKSHOPS), 2010 IEEE International Conference*. 20, *(24)*, 1-8. doi: 10.1109/CLUSTERWKSP.2010.5613106; Chunye Gong, Jie Liu,; Qiang Zhang, Haitao Chen, & Zhenghu Gong. (2010). The Characteristics of Cloud Computing, Parallel Processing Workshops (ICPPW). *2010 39th International Conference*. 13, *(16)*, 275-279doi: 10.1109/ICPPW.2010.45.

dos Mexicanos en donde la computación en la nube o cómputo en la nube es definido como el:

> *modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente*(Estados Unidos Mexicanos, Presidencia de la República, 2011, *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* Cursivas mías.).

Esta es la primera definición legal sobre la materia, la cual se encuentra consagrada en el artículo 52 del *Reglamento de la Ley Federal de protección de datos personales en posesión de particulares* publicada en diciembre de 2011 por el Estado Mexicano.

De las diversas acepciones[2] sobre Cloud Computing puede concluirse, entre otras, que se trata de un servicio mediante el cual el usuario (una persona, una empresa, una entidad pública o cualquier organización) terceriza la provisión de ciertos recursos tecnológicos, como puede ser la infraestructura para el desarrollo de un software, una plataforma para el desarrollo de aplicaciones web o simplemente una solución de software en una central de cómputo (denominado cloud service provider –CSP-) quien, a través de internet, permite que se utilicen sus data centers para guardar la información, albergar programas de computador que corran en sus servidores o permitir la utilización de su capacidad instalada para suplir necesidades de cómputo. Este servicio opera por demanda o solicitud del usuario, es flexible y se obtiene pagando sólo por el espacio efectivamente utilizado.

Una vez introducido el concepto de computación en la nube, entraremos a analizar las diversas clases de entornos que en la actualidad se están ofreciendo en internet.

B. Tipos de Cloud Computing

La particularidad del cómputo en la nube permite que se ofrezcan diversas posibilidades a los usuarios del servicio, creándose formas de acceso público, privado o mixto, las cuales tienen un tratamiento diferente en materia de seguridad y costos, como se evidencia a continuación:

1. Nube pública

Es aquel modelo que permite a los usuarios el acceso a recursos de cómputo compartidos, a través de internet, utilizando cualquier navegador del común no especializado (Mozilla Firefox, Internet Explorer, Safari, Google Chrome, entre

2 Varios autores y grupos de trabajo se han referido al concepto de cloud computing en los siguientes términos: La mesa sectorial de cloud computing, una perspectiva para Colombia, del 10 de abril de 2010 la definió como *"un modelo para habilitar el acceso a un conjunto de servicios computacionales (E.G. Redes, Servidores, almacenamiento, aplicaciones y servicios) de manera conveniente y por demanda, que puede ser rápidamente aprovisionados y liberados con un esfuerzo administrativo y una interacción con el proveedor del servicio mínimos*" (Castro, J. et al Abril de 2010, *Cloud Computing: Una Perspectiva Para Colombia, Mesa Sectorial Cloud Computing.* Versión 1.0.0).. Sectores tecnológicos especializados la definen como *"a collection of net-centric, service oriented concepts, methodologies, best practices and technologies, It promises scaled economic benefits by provisioning computing resources and application as services to customers while costumers base their needs to subscribe related services"* (Zhixiong C, & Yoon, J., 2010, IT Auditing to Assure a Secure Cloud Computing, Services*, (SERVICES-1), 2010 6th World Congress.*). Otros textos han manifestado que *"Cloud Computing delivers on-demand services with flexibility and scalability on a simple pay-per-use basis. For small- and medium sized enterprises (SMEs), Cloud Computing enables them to avoid over-provisioning of IT infrastructure and training personal"* (Doelitzscher, F, Reich, C. & Sulistio, A., 2010, p. 930-935) Como se evidencia de estas definiciones la constante es el servicio por demanda y la flexibilidad de los recursos informáticos prestados a través de internet.

otros). Está basado en un negocio de pago por utilización del servicio, similar a servicios públicos como la electricidad, lo cual posibilita la suficiente flexibilidad para ofrecer una asistencia adecuada en los momentos de alta demanda que permitie a los consumidores utilizar los recursos de acuerdo a los requerimientos de su propia demanda. Este servicio es menos seguro que otros modelos en la nube que consideraremos más adelante ya que, al permitir acceso al público en general, existe la posibilidad de que se presenten mayores de ataques maliciosos que en otros escenarios (Ramgovind, S, Eloff, M.M. & Smith, E., 2010, The management of security in Cloud computing, *Information Security for South Africa (ISSA)*).

En la nube pública varios consumidores comparten los data centers, sin tener una asignación específica de equipos físicos, no obstante, el acceso a la información es exclusivo por parte de su titular y no pueden acceder otros a ésta. Un ejemplo es el sistema *Amazon Simple Storage Service (Amazon S3),* el cual proporciona una interfaz de servicios web sencilla que se puede utilizar para almacenar y recuperar datos sin importar el momento o el lugar en la web, con la particularidad que todos los archivos almacenados en línea se codifican y guardan en *Amazon Simple Storage Service* -S3- en varios centros de datos ubicados en los Estados Unidos (Where are my files stored?). Si bien esta información se encuentra codificada, se compartirán los recursos informáticos con otros usuarios del servicio al estar sujetos a los controles de seguridad de la información que imponga la proveedora del Data Center, en este caso, Amazon.

2. Nube privada

Es aquel servicio atado al centro de información interno de una organización o empresa, es decir, una compañía utiliza de forma exclusiva una infraestructura cloud; siendo mucho más fácil alinear la seguridad y el cumplimiento de los requerimientos regulatorios permitiendo un mayor control en su despliegue y utilización. En la nube privada los recursos son escalables y las aplicaciones virtuales ofrecidas por el proveedor cloud son utilizadas y compartidas de forma conjunta por los usuarios. Se diferencia de la nube pública en que todos los recursos web y aplicaciones son administrados única y exclusivamente por el organizador, asimilándose a un funcionamiento como el de una intranet[3].

Un ejemplo de esta es el utilizado por las compañías para compartir archivos en carpetas comunes (que diferentes usuarios puedan acceder y modificar utilizando un log in). Estos se encuentran almacenados en servidores físicos, custodiados por la empresa, que pueden ser accedidos desde una página web. Esto permite mayores niveles de seguridad que cualquier otro tipo de Cloud Computing.

3. Nube híbrida

Es una nube privada atada a uno o más servicios cloud externos manejados centralizada-

3 Sobre este tema se puede ver: Breckinridge, C. (February 27, 2012). *From the Experts: Cloud Computing's Hidden Export Regulation Risks How to avoid violating U.S. trade controls when storing data in the cloud. Ed.* Corporate Counsel -ALM Media, Inc-. Recuperado de http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202543464867&thepage=1 y Robison, W., J. (2010) Free at What Cost?: Cloud Computing Privacy Under The Storage Communications Act. En *The Georgetown Journal*. . 98, *(1195).* Washington: USA.

mente, provisionados como una sola unidad en conjunto y circunscritos por una red segura. Provee soluciones de tecnología virtual a partir de una mezcla de nubes públicas y privadas y, de esta forma, garantiza mecanismos de control más eficaces sobre la información y las aplicaciones permitiendo que varias partes accedan a la información por medio de internet. Este tipo de nube tiene como particularidad una arquitectura abierta que permite interfaces con otros sistemas de administración[4] y habilita a varias empresas, con diferentes programas, para acceder y estructurar el software o la información de acuerdo con la necesidad particular; en este sentido se presenta como una posibilidad para que dos o más nubes (públicas o privadas) estén unidas, facilitando el intercambio de datos y/o aplicaciones entre ellas de una manera controlada.

Un ejemplo que implementa el modelo de nube híbrida es Domino's Pizza. Esta compañía recibe 50% más de pedidos en el domingo del *Super Bowl* que en una noche típica de viernes. En vez de comprar hardware adicional de TI para atender la demanda inusual de llamadas en el Super Bowl —capacidad que no usaría en el resto del año- Domino's Pizza ha utilizado la nube para manejar el incremento de sus necesidades en TI para ese día (Microsoft Corporation, Junio 28 de 2011, *Microsoft Office 365: Identify For Enterprises, Service Description*). De este modo, aumentan su capacidad para recibir llamadas y procesar los pedidos al permitir la interacción entre la nube privada de la compañía y la nube pública.

C. Esquemas comerciales de ofertas de servicios de Cloud Computing

Los servicios varían dependiendo de las necesidades de los usuarios del servicio, no obstante, dichos requerimientos quedan comprendidos dentro de alguna de las siguientes categorías:

1. Software como servicio (software-as-a-service –SaaS-)

Con este tipo de servicio se busca reemplazar la práctica habitual de descargar las aplicaciones de software en cada computador de escritorio o la de instalar aplicaciones en servidores para ofrecer servicios a los diferentes usuarios de una organización. De este modo, el usuario evita tener que instalar y correr el software específico ya que accede a una página web desde la cual puede utilizar el programa (Dillon, T., Chen Wu. & Chang, E., 2010, p.27-33, 20-23).

Un ejemplo de este servicio es Office 365. Éste permite que a partir del acceso a internet una persona pueda utilizar aplicativos como Word, Outlook, Excel y PowerPoint, aplicaciones de colaboración (Sharepoint) y de comunicaciones unificadas (Lync) sin necesidad de descargar un programa específico en su computador (éstas corren directamente en la plataforma de Microsoft), permitiéndose incluso en una versión más sofisticada correr directamente el paquete Office en el PC, sólo pagando por el tiempo que efectivamente se utilice. El usuario cuenta con

4 Sobre esto se puede consultar a: Ramgovind, S, Eloff, M., M. & Smith, E. (2010). *The management of security in Cloud computing. Information Security for South Africa (ISSA)*. Recuperado de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5588290&isnumber=5588257 y Natsui, T. (s.f.). *Cloud Computing Service And Legal Issues*. Recuperado de http// cyberlaw.la.coocan.jp/Documents/Cloud%20Computing%20Service%20and%20Legal%20Issues%20x.pdf.

la posibilidad de guardar y modificar los archivos en la web pagando por el servicio efectivamente utilizado (Microsoft Corporation, Enero de 2011, *Privacy and Data Access in a World of Online Computing: A Call To Action*).

2. Plataforma como servicio (platform-as-a-service –PaaS-)

Es un escenario que soporta íntegramente el ciclo del software al permitir que los consumidores desarrollen servicios y aplicaciones en la web. La diferencia principal con el SaaS es que éste sólo hospeda software ya terminado. El PaaS ofrece la posibilidad de acoger software finalizados y en proceso, de este modo, el usuario puede acceder a herramientas, ambientes y direcciones de configuración del proceso (Minqi Z, et al, 2010, p.105-112). Así se permite que diferentes personas puedan trabajar en el mismo proyecto sin tener que estar en el mismo lugar.

3. Infraestructura como servicio (infrastructure-as-a-service –IaaS-)

Este esquema contempla la traslación de la operación completa de procesadores, dispositivos de almacenamiento, redes y otros componentes del proceso de sistemas hacia un esquema virtual. De este modo se promueve la desaparición de los equipos físicos, permitiendo que en el momento de crecimiento se amplíen los servicios, mientras que en la etapa de declinación se puede reducir la capacidad instalada posibilitando la disminución de los costos involucrados en el proceso[5].

Esto se configura como un negocio de almacenamiento de datos con una economía de escala, por el cual, una organización (Cloud Service Provider) invierte en servidores permitiendo a los usuarios acceso remoto[6]. En esta propuesta se debe aclarar el tipo de servicio que se quiera implementar con el vendedor –ofertante de la infraestructura Cloud-.

Para puntualizar la importancia de la tecnología cloud computing en la actualidad, en Colombia se han presentado casos de éxito con respecto a esta tecnología por parte de entidades como el ICFES, el cual utiliza la infraestructura de software como servicio Windows Azure, desde Octubre de 2010, para entregar los resultados de los exámenes de Estado Saber 11; y teniendo en cuenta que más de 600 mil estudiantes que presentaron el examen accedieron al portal web en busca de sus resultados, al usar la tecnología cloud computing evitaron que se saturara la plataforma y se cayera el portal web (Instituto Colombiano para la Evaluación de la Educación –ICFES, 2011, *Comunicado de prensa 5 de Abril de 2011: ICFES Utiliza soluciones tecnológicas de vanguardia para la consulta de resultados*).

5 Sobre este tema se puede ver: Ramgovind, S, Eloff, M., M. & Smith, E. (2010). *The management of security in Cloud computing. Information Security for South Africa (ISSA)*. Recuperado de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5588290&isnumber=5588257 y Dillon, T., Chen W. & Chang, E. (2010). Cloud Computing: Issues and Challenges. *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference*. 27-33. Recuperado de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5474674&isnumber=5474664.

6 Sobre este tema se puede consultar: Zhixiong C. & Yoon, J. (2010). IT Auditing to Assure a Secure Cloud Computing, Services. *(SERVICES-1), 2010 6th World Congress*. Recuperado de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5575840&isnumber=5575460. y Chunye G., Jie L, Qiang Z., Haitao C, & Zhenghu G. (2010). The Characteristics of Cloud Computing, Parallel Processing Workshops (ICPPW). *2010 39th International Conference*. 13, *(16)*, 275-279doi: 10.1109/ICPPW.2010.45.

Otro servicio en la nube utilizado en Colombia ha sido el *"Google Apps Premier Edition",* utilizada por compañías como Avantel, la Superintendencia de Servicios Públicos (SSP) y Fedepalma. Dicha herramienta permite acceso remoto a los correos y mensajería instantánea solucionando problemas y limitaciones en materia de capacidad instalada de servidores, los costos de administración y el soporte técnico; presentándose en el caso de la SSP reducciones de soporte técnico de hasta un 98% (Más Publicidad y Marketing. 7 de Abril de 2010, *Cloud Computing ya tiene casos de éxito en Colombia*).

II. ANÁLISIS LEGAL DEL CLOUD COMPUTING

La descripción teórica del Cloud Computing, sus características, esquemas comerciales de ofertas de servicio y tipos de nube evidencian que se trata de una nueva forma de aproximación a la manera en que las personas naturales y jurídicas almacenan información y la comparten. Así, nos encontramos frente a un fenómeno en el cual los ordenamientos jurídicos deben ser interpretados y actualizados con el fin de identificar y anticipar los posibles cuestionamientos o incertidumbres legales que puedan surgir.

Es por esto que el estudio de la computación en la nube debe empezar en la naturaleza legal del servicio y los retos jurídicos que se presentan sobre este tipo de contratos[7]. De esta forma se evidencia el marco sobre el cual se debe analizar el servicio específico en la nube.

Los retos jurídicos de este tipo de contratación, que según la doctrina surgen desde diferentes vertientes del derecho como: la protección de datos[8], la transferencia internacional de datos[9], la propiedad intelectual[10], la seguridad de la in-

7 Cada tipo de esquema comercial de ofertas de servicios genera una relación jurídica contractual entre el contratante del servicio y el oferente del servicio cloud, vínculos contractuales que en su mayoría son contratos de adhesión.

8 Sobre este tema se pueden consultar los siguientes autores: Marchimi R. (2010) *A Practical Introduction To The Legal Issues.* London: Ed. British Standards Istitution., Robison, W., J.. (2010). Free at What Cost?: Cloud Computing Privacy Under The Storage Communicatios Act. En *The Georgetown Journal*. 98, *(1195)*. Washington: USA., Doelitzscher, F, Reich, C. & Sulistio, A. (2010). Designing Cloud Services Adhering to Government Privacy Laws, Computer and Information Technology (CIT). *2010 IEEE 10th International Conference on.* 930-935.doi: 10.1109/CIT.2010.172, Gellman, R. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. *World Privacy Forum*. Recuperado de www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf., Hon, W. K., Millard C. & Walden I. (2010). The Problem of "Personal Data" in Cloud Computing – What information is Regulated? The Cloud of Unknowing, Part 1. *School of Law, Legal Studies Research Paper*. 75. London: Queen Mary University of London. Recuperado de http://ssrn.com/abstract=1783577., Hon, W. K., Millard, C, Walden, I. (2011). Who is Responsible for "Personal Data" in Cloud Computin? The Cloud of Unknowing, Part 2. *University of London, School of Law, Legal Studies Research Paper*. 77. London: Queen Mary Recuperado de http://ssrn.com/abstract=1794130.

, Natsui.(s.f.,

9 Sobre este tema se pueden consultar los siguientes autores: Marchimi R. (2010) *A Practical Introduction To The Legal Issues.* London: Ed. British Standards Istitution., Walden, I. (s.f.). *Accesing Data in the Cloud: The Long Arm of the Law Enforcement Agent.* London: Queen Mary University Of London. Recuperado de http://ssrn.com/abstract=1781067. Hon, W., K. Hornle, J. & Millard, C. (2011). Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3. *School of Law, Legal Studies Research Paper No. 84/2011*. London: Queen Mary University of London. , Recuperado de http://ssrn.com/abstract=1924240.,

Hon, W. K., Millard C. & Walden I. (2010*).* The Problem of "Personal Data" in Cloud Computing – What information is Regulated? The Cloud of Unknowing, Part 1. *School of Law, Legal Studies Research Paper*. 75. London: Queen Mary University of London. Recuperado de http://ssrn.com/abstract=1783577.

y Robison Breckinridge, C. (Febrero 27 2012). *From the Experts: Cloud Computing's Hidden Export Regulation Risks How to avoid violating U.S. trade controls when storing data in the cloud. Ed.* Corporate Counsel -ALM Media, Inc.-. Recuperado de http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202543464867&thepage=1

10 Sobre este tema se pueden consultar los siguientes autores: Mowbray, M. (April 2009) The Fog over the Grimp: Cloud Computing and the Law. *SCRIPTed Journal of Law, Technology and Society.* 6, *(1),*

formación almacenada en la nube[11], las actuaciones criminales[12], la responsabilidad civil[13], el derecho de la competencia[14] y los impuestos[15] tienen como eje común el problema de la ley aplicable a los contratos y bajo qué jurisdicción se realizaron los actos jurídicos.

No obstante la multiplicidad de materias que podrían ser estudiadas, en el presente escrito nos centraremos en analizar dos puntos; el primero es el marco conceptual del contrato de computación en la nube -análisis que sirve para todos los cuestionamientos anteriormente mencionados-, para tratar posteriormente las generalidades de los servicios de Cloud Computing. Como segundo punto se realizará un análisis de los problemas de jurisdicción a la luz de la protección de datos en el caso colombiano.

A. Definición contractual

El gran conflicto que surge frente a la relación jurídica entre el contratante del servicio en la nube y los Cloud Service Providers CSP es que el consumidor no necesariamente sabe dónde se encuentra su información. A su vez, al tratarse de una contratación excesivamente elástica, los términos y condiciones del contrato son im-

132-146. DOI:10.2966/scrip.060109.132. Marchimi R. (2010) *A Practical Introduction To The Legal Issues.* London: Ed. British Standards Istitution.,
Reed, C. (2010). Information Ownership" in the Cloud. *School of Law, Legal Studies Research Paper.* 45. London: Queen Mary University of London. Recuperado de http://ssrn.com/abstract=1562461.

11 Sobre este tema se pueden consultar los siguientes autores: ISACA. (2009). *Computación en la nube: Beneficios de negocio con perspectivas de seguridad, gobierno y Aseguramiento.* IL, USA: Ed. Isaca, Rolling Meadows., Minqi Z., Rong, Z., Wei X.e, Weining, Q. & Aoying, Z. (2010). Security and Privacy in Cloud Computing: A Survey, Semantics Knowledge and Grid (SKG). *2010 Sixth International Conference on*. 1, *(3)*, 105-112 doi: 10.1109/SKG.2010.19, Pearson, S. & Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on.* 93-702. doi: 10.1109/CloudCom.2010.66, Zhixiong C. & Yoon, J. (2010). IT Auditing to Assure a Secure Cloud Computing, Services. *(SERVICES-1), 2010 6th World Congress*. Recuperado de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5575840&isnumber=5575460.,

Timmermans, J, Ikonen, V. & Stahl, B.,C. & Bozdag, E. (2010). The Ethics of Cloud Computing: A Conceptual Review, Cloud Computing Technology and Science (CloudCom). *2010 IEEE Second International Conference, Nov. 30 2010-Dec. 3 2010.* Recuperado de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5708509&isnumber=5708426.

12 Sobre las actuaciones criminales en cloud computing se pueden consultar los siguientes autores: Pearson, S. & Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on.* 93-702. doi: 10.1109/CloudCom.2010.66, Zhixiong C. & Yoon, J. (2010). IT Auditing to Assure a Secure Cloud Computing, Services. *(SERVICES-1), 2010 6th World Congress*. Recuperado de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5575840&isnumber=5575460, Velasco San Martin, C. (Febrero 28, 2009) *Jurisdictional Aspects Of Cloud Computing* Recuperado de http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf ., ISACA. (2009). *Computación en la nube: Beneficios de negocio con perspectivas de seguridad, gobierno y Aseguramiento.* IL, USA: Ed. Isaca, Rolling Meadows.,

Corrales, M., Barnitzke, B, & Forgó Nikolaus. (2011). *Aspectos Legales de la computación en la Nube: protección de datos y marco general sobre propiedad intelectual en la legislación Europea*. Trad. María Clara Bouchoux. Buenos Aires: Editorial Allbremática. (1ª Edición).

y Walden, I. (s.f.). *Accesing Data in the Cloud: The Long Arm of the Law Enforcement Agent.* London: Queen Mary University Of London. Recuperado de http://ssrn.com/abstract=1781067.

13 Sobre la responsabilidad extracontractual en los servicios cloud computing se pueden consultar: Silver, G. (1 de Enero de 2012). *5 Key Considerations When Litigating Cloud Computing Disputes* Recuperado de http://www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202538844687&slreturn=1., Marchimi R. (2010) *A Practical Introduction To The Legal Issues.* London: Ed. British Standards Istitution, ISACA. (2009). *Computación en la nube: Beneficios de negocio con perspectivas de seguridad, gobierno y Aseguramiento.* IL, USA: Ed. Isaca, Rolling Meadows..

14 Sobre este tema se pueden consultar a: Corregio L., Laíse, D. & Walden, I. (s.f.). *Ensuring competition in the Clouds: The role of competition law?* Recuperado de http://ssrn.com/abstract=1840547.

15 Sobre este tema se pueden consultar los siguientes autores: Andre, M. (Julio 12 de 2010). *Sales and Use Taxation in the Clouds.* Recuperado de http://www.kpmginstitutes.com/taxwatch/insights/2010/pdf/wnit-071210-sales-use-taxation-in-clouds.pdf. y Marchimi R. (2010) *A Practical Introduction To The Legal Issues.* London: Ed. British Standards Istitution.

puestos por el proveedor del servicio (Marchimi, 2010, p. 60), razón por la cual, el punto de partida ha de ser determinar efectivamente qué tipo de relación jurídica se establece por medio de ese vínculo contractual y cuál es la legislación aplicable. Esto último es relevante pues de la ley que gobierna a las partes se deriva del régimen jurídico en materia de servicio, privacidad, transferencia de datos, encriptación de información y acceso a la misma por el mismo prestador del servicio; y sólo en el supuesto que se entiendan y se acepten las condiciones de uso se puede proceder a mover la información a un servidor en la nube o a desarrollar las aplicaciones en dicho sistema (Gellman, 2009).

Ahora bien, considerando que en Colombia no existe ley especial para este tipo de contratos debemos revisar la figura jurídica que se asimila a los servicios prestados en la nube. Teniendo en cuenta la legislación colombiana se trata de dos contratos, a saber:

El primero es el contrato de arrendamiento definido en el artículo 1974 del *Código Civil*, estableciéndose que: *"son susceptibles de arrendamiento todas las cosas corporales o incorporales, que pueden usarse sin consumirse"* (Congreso de la República de Colombia, 2008, Artículo 1974º). Dentro de dicha definición caben los servicios prestados por empresas cloud, ya que se generan relaciones jurídicas que encajan dentro de la figura (Silver, 2012). Al tratarse del alquiler de espacios materiales (servidores), se puede presentar que algunas personas lo confundan con el arrendamiento de espacios inmateriales al no conocerse efectivamente dónde se encuentra almacenada la información, desconociéndose que al final la información reside en un data center real y tangible, enmarcándose el concepto anteriormente expresado en los servicios de plataforma como servicio e infraestructura como servicio.

La segunda figura jurídica que se aplicaría en este caso, al software como servicio, es la del contrato de suministro consagrado en el artículo 968º del Código de Comercio por el cual se entiende que: *"el contrato por el cual una parte se obliga, a cambio de una contraprestación, a cumplir en favor de otra, en forma independiente, prestaciones periódicas o continuadas de cosas o servicios"*(Congreso de la República de Colombia, 2010, Artículo 968º). Prestaciones económicas que se suministrarán según las necesidades del usuario, cumpliéndose con el principio de pagar, efectivamente, el software utilizado, permitiéndose la elasticidad del consumo.

A su vez, es pertinente hacer la claridad sobre la naturaleza jurídica de las obligaciones que emanan del contrato de computación en la nube en el caso colombiano, los cuales no se encuentran tipificados en la legislación nacional. No obstante, por tratarse del arrendamiento de un espacio material o un contrato de suministro (según sea el caso), nos encontramos ante una obligación de resultado por parte del CSP (Cloud Service Provider), ya que es posible cumplirla en el orden normal de las cosas_ (Tamayo, 2011, *Tratado de Responsabilidad Civil, Tomo I*). Eso conduce a concluir que sólo se podrá eximir de responsabilidad al proveedor del servicio por el incumplimiento de las obligaciones por caso for-

tuito, causa extraña y culpa del usuario teniendo que cumplir las obligaciones emanadas del contrato, como es permitir el almacenamiento de la información, correr las aplicaciones en su plataforma o permitir el acceso al software.

Una vez se determinen los términos y condiciones del contrato se debe analizar el lugar donde efectivamente está la información, es decir, el sitio donde se encuentran los data centers del proveedor del servicio Cloud[16]. Esto porque en el momento que se presenten reclamaciones por mal servicio tendrán que ser llevadas ante la jurisdicción competente que se determinará teniendo en cuenta las cláusulas compromisorias[17] o, en el mejor de los casos, el domicilio del contratante (Kyer, C. & Stern, G.,2011, *Where in the World is My Data? Jurisdictional Issues with Cloud Computing,* p. 4); con la consecuencia que si aquél se encuentra fuera del territorio nacional del usuario, será casi imposible para las entidades estatales[18] velar por sus intereses (Gamboa, 2005, *Soberanía estatal en internet; análisis desde la perspectiva de conflictos de jurisdicción y competencias en el plano nacional e internacional,* p.659).

No obstante lo anterior, es pertinente hacer una mención a la Ley 1480 de 2011 por la cual se promulgó el nuevo estatuto del consumidor en Colombia. En el artículo 50 establece la territorialidad de la ley al determinar que esta aplicará a: *"los proveedores y expendedores ubicados en el territorio nacional"* (Ley 1480, 2011, Artículo 50º.), de donde se puede concluir que la ley de protección al consumidor no cobijará a las compañías que presten servicios cloud en el país y no tengan una sede física en Colombia. Ahora bien, la norma anteriormente expuesta debe ser interpretaba de forma estricta, ya que se puede presentar el supuesto en que el proveedor del servicio no se encuentre en el país, pero el producto, está siendo comercializado por un agente en el territorio Colombiano, supuesto en el cual existe una responsabilidad solidaria en la calidad, idoneidad y seguridad del servicio cloud

16 Esta información se encuentra generalmente en los términos y condiciones del contrato de adhesión que se acepta cuando se contrata el servicio, de no encontrarse la información en este documento, se puede solicitar directamente al oferente del servicio.

17 En las clausulas compromisorias solo se podrá establecer que las partes escogen una jurisdicción de las obligaciones que se emanen del vínculo contractual, no extendiéndose la ley aplicable del contrato a reclamaciones de responsabilidad extracontractual por daños a terceros donde quedarán registradas las creaciones protegidas por la propiedad intelectual o la protección a los consumidores. (Kyer, C. & Stern, G.,2011, *Where in the World is My Data? Jurisdictional Issues with Cloud Computing,*p. 3). Ahora bien, en el caso particular Colombiano es pertinente traer a colación que la *Ley 1480 de 2011 "Por medio de la cual se expide el estatuto del consumidor y se dictan otras disposiciones*" establece en el artículo 43 numeral 12 "*Cláusulas abusivas ineficaces de pleno derecho. Son ineficaces de pleno derecho las cláusulas que: 12. Obliguen al consumidor a acudir a la justicia arbitral"*. Por tanto, en el caso Colombiano las relaciones que surjan entre el proveedor del servicio en la nube y el consumidor no podrán ser llevados a la jurisdicción arbitral, teniendo que sujetarse a las normas colombianas en el supuesto que el proveedor del servicio se encuentre en Colombia: *"sin perjuicio de las demás obligaciones establecidas en la presente ley, los proveedores y expendedores ubicados en el territorio nacional que ofrezcan productos utilizando medios electrónicos, deberán"*(Ley 1480, 2011, Artículo 50º). En este punto es pertinente entrar a analizar cual es el ámbito de aplicación de la Ley 1480 de 2011 referente a la protección al consumidor, el artículo 2 de dicho cuerpo normativo establece que. *"Las normas contenidas en esta ley son aplicables en general a las relaciones de consumo y a la responsabilidad de los productores y proveedores frente al consumidor en todos los sectores de la economía";* siendo el elemento fundamental para definir la aplicación de la ley a la definición de consumidor que trae la misma ley en el artículo 5 numeral 3 en el cual se aclara que consumidor o usuario es: "toda persona natural o jurídica que, como destinatario final, adquiera, disfrute o utilice un determinado producto, cualquiera que sea su naturaleza para la satisfacción de una necesidad propia, privada, familiar o doméstica y empresarial **cuando no esté ligada intrínsecamente a su actividad económica** (…)" (negrilla y subraya fuera del texto original). Por tanto, la ley de protección al consumidor será aplicable a los contratos cloud, cuando el objeto del contrato no este intrínsecamente ligado a su actividad económica.

18 En este supuesto se hace referencia a la protección que el Estado colombiano ejerce frente sus nacionales, como puede ser el caso de protección al consumidor o la responsabilidad civil por el daño causado.

entre el productor y el proveedor, si este último de manera habitual, directa o indirectamente ofrece, suministra o distribuye el producto[19].

Una vez analizado el marco contractual general de la computación en la nube, aplicable a todos los esquemas comerciales de ofertas de servicios, analizaremos las consecuencias jurídicas de los servicios de software como servicio, plataforma como servicio e infraestructura como servicio.

En el caso del software como servicio se le garantiza al usuario el acceso, a partir de un navegador de internet, a ciertos servicios de software administrados por un tercero, ya sea de forma gratuita u onerosa. Ahora bien, en el supuesto en que no sólo se garantice la disponibilidad sino que se presten servicios de almacenamiento de información, como la creación de documentos en línea, no se trata sólo de un contrato de acceso a la información, sino de una responsabilidad por parte del proveedor de servicio en la nube (empresa que ofrece los servicios, que puede o no ser la propietaria de los Data centers), de velar porque la información sea accesible en el momento que se necesite. Además, debe garantizar la integridad de la información del contratante, sólo eximiéndose de la responsabilidad por caso fortuito o de fuerza mayor (Clark Street Wine And Spirits Vs. Emporos Systems Corporation, Noviembre 29 de 2010, p. 4).

De esta forma se define una naturaleza jurídica de suministro de servicio y, a su vez, de arrendamiento de un espacio virtual con las respectivas obligaciones del depositario de un bien inmaterial, tales como la custodia y la devolución de la información en las mismas condiciones en que fue entregada, no pudiendo accederse a ella o manipularla.

En los supuestos de plataforma como servicio no sólo se tiene el derecho de acceder a un programa, sino que se trata de la capacidad de desarrollar aplicaciones que corran en dichas plataformas. Esto implica un contrato de arrendamiento de espacio material en el cual se desarrolla un proyecto y, a su vez, habría lugar a un derecho de uso de herramientas tecnológicas para el desarrollo de software. Es preciso que la empresa proveedora de cloud tenga especial cuidado ya que, en caso de presentarse perjuicios al consumidor final del software alojado en la plataforma, podrá exigir al proveedor del servicio que responda por los daños causados sobre la información, así este subcontratase con un tercero el almacenamiento en data centers externos[20].

19 Sobre este tema la Ley 1480 de 2011, en su artículo 6 establece "todo productor debe asegurar la idoneidad y seguridad de los bienes y servicios que ofrezca o ponga en el mercado, así como la calidad ofrecida. En ningún caso estas podrán ser inferiores o contravenir lo previsto en reglamentos técnicos y medidas sanitarias o fitosanitarias. El incumplimiento de esta obligación dará lugar a: 1. **Responsabilidad solidaria del productor y proveedor por garantía ante los consumidores**. 2. Responsabilidad administrativa individual ante las autoridades de supervisión y control en los términos de esta ley. 3. Responsabilidad por daños por producto defectuoso, en los términos de esta ley." (Ley 1480, 2011,Artículo 6º. Subrayas y negrita fuera del texto original). Se entiende entonces por proveedor o expendedor del servicio según el artículo 5 numeral 11 a "*quien de manera habitual, directa o indirectamente, ofrezca, suministre, distribuya o comercialice productos con o sin ánimo de lucro."*

20 La relación jurídica que surge entre el proveedor del servicio y el contratante del servicio, al ser de naturaleza contractual, implica que el oferente del servicio en la nube deberá responder por los daños que se causen sobre la información sin importar si está contratando el almacenamiento con un data center externo. Ahora bien, al ser una obligación de resultado (responsabilidad contractual), solo podrá exonerarse si demuestra causa extraña o culpa de la víctima, teniendo las mismas características de una subcontratación de un servicio con un

En el caso de la infraestructura como servicio, el contrato de arrendamiento versa sobre el espacio de almacenamiento y la capacidad inmaterial por parte de la empresa prestadora del servicio. En este supuesto, el contratante tiene plena autonomía para manejar los recursos. No obstante lo anterior, la responsabilidad por los perjuicios que se pueden causar por el deterioro de la información, pérdida o filtración serán responsabilidad del contratista o prestador del servicio arrendatario ya que él es quien debe velar por la custodia y por la existencia de un back up de la información almacenada en caso de un ataque o mal funcionamiento (Silver, 2012).

Ahora bien, haciendo referencia a los derechos sobre la información (problema recurrente en todos los esquemas comerciales expuestos, ya que se tiene que definir quién es el titular de los datos) que se encuentra almacenada en los data centers, algunos autores como Chris Reed (2011), establecen que los derechos de propiedad sobre la información que se encuentra en los data centers es una colcha de retazos entre derechos de propiedad intelectual (específicamente sobre las creaciones en la web, como pueden ser los servicios de software en PaaS), confidencialidad de la información y régimen contractual (p. 20). Haciendo especial énfasis en la propiedad intelectual, creaciones sobre las cuales (según el criterio de este autor) recae un derecho que se encuentra en cabeza de su creador, no existe posibilidad de discusión sobre el titular de la creación o de la información aunque él puede ser el contratante del servicio cloud. .

No obstante, para evitar conflictos entre las partes, este tema se debe definir en el contrato, haciendo la salvedad que, al tratarse de un contrato de arrendamiento en la nube (en el caso particular de una plataforma PaaS, para desarrollar un software), no se transmiten los derechos de propiedad intelectual sobre la información o las creaciones de software, encontrándonos en desacuerdo con la posición esbozada por Reed, dado que la naturaleza del contrato en ningún supuesto está trasmitiendo el derecho real de dominio sobre la información o las creaciones sujetas a propiedad intelectual, ya que quien custodia o almacena la información no adquiere derecho alguno sobre la misma.

Por último, en el momento de la terminación del vínculo contractual se deben tener en cuenta aspectos como la recuperación y/o destrucción de la información que se encuentra alojada en los servidores del proveedor, teniendo especial relevancia en estos supuestos la falta de pago y la violación de condiciones contractuales (Martínez, 2011, Los Retos de Cloud Computing, p.4). En este sentido, es esencial que desde la negociación de los contratos se pacte que, en caso de terminación del contrato, la información deberá ser borrada en su integridad (previo que el usuario pueda migrar o recuperarla, con el fin de no perderla); pudiéndose prever eventualidades futuras a partir de la adquisición de pólizas de cumplimiento, sobre todo, en el supuesto de que el contratista cloud se encuentre en otras jurisdicciones.

tercero y la responsabilidad de responder al ser el oferente y obligado contractual. (Zuleta, 2010, *La Responsabilidad Civil Extracontractual, Contractual y Precontractual De Las Personas Jurídicas*, p. 288-293). Ahora bien, no obstante lo anterior, si el perjuicio sucede por causa del data center, aquel podrá repetir contra este último.

Una vez aclarado el marco general contractual legal, quién es el propietario de la información en la nube y, sobre todo, qué naturaleza jurídica tiene el contrato podemos entrar a analizar el problema de la jurisdicción en los contratos de computación en la nube.

B. Jurisdicción[21]

Visto lo anterior, resulta pertinente retomar el problema de la localización de los data centers donde estará alojada la información. Este asunto se torna relevante para los usuarios ya que, dependiendo de la naturaleza del conflicto, se determinará la ley aplicable para el contrato, siendo este asunto crucial para cualquier servicio que se ofrezca utilizando los modelos de negocio de la computación en la nube.

Microsoft Corporation en el documento: *Privacy and data access in a world of online computing: a call to action* evidencia los problemas en materia de jurisdicción que están afrontando las empresas que ofrecen servicios[22]. La discusión se centra sobre la jurisdicción que los proveedores del servicio en la nube están ejerciendo sobre los contenidos de los usuarios de los servicios y sobre la administración de datos personales (Microsoft Corporation, Enero de 2011, p. 1); situaciones que, en algunos casos, causan conflictos entre las partes y los Estados donde efectivamente se encuentran los data centers. Ciertos regímenes determinan que la jurisdicción existe sólo si los datos están almacenados físicamente en el país, mientras que otros ejercen su jurisdicción en tanto el servicio en cuestión está siendo ofrecido allí o si el usuario a quien se refieren los datos reside en el lugar. Otros declaran su jurisdicción en tanto el proveedor del servicio tenga un sitio de negocios en el país, sin considerar dónde están localizados los datos (Microsoft Corporation, Enero de 2011, p. 3).

De los problemas evidenciados anteriormente se debe hacer la salvedad sobre la ley aplicable a los contratos, pues ésta tendrá un trato diferente dependiendo del tema sujeto de estudio, por esto, se analizará la jurisdicción bajo la protección de datos.

C. Protección de datos personales

Por la naturaleza de la actividad que realizan las empresas de Cloud Computing: recolectan datos provenientes de diferentes ciudadanos, los cuales son almacenados en servidores alrededor del planeta (Timmermans, J, Ikonen, V., Stahl, B.C. & Bozdag, E., 2010, p. 614-615). En el en-

21 A lo largo del presente escrito, cuando se hable de jurisdicción ésta se tendrá como *"la facultad de administrar justicia"* (Gamboa, 2005p. 643); lo cual está atado directamente a la competencia que debe ser entendida como *"el juez que debe decidir determinada controversia*" (Gamboa, 2005,p. 643). Entendiéndose por jurisdicción la ley aplicable y, por ende, el poder de coacción del Estado para hacerla cumplir en un determinado territorio sobre las personas naturales o jurídicas.

22 Los problemas de jurisdicción en materia de computación en la nube, han sido puestos de manifiesto en reiteradas ocasiones por la doctrina, al tratarse de un servicio que se puede prestar por internet sin necesidad de desplazarse físicamente. Si se quiere ver otros autores obre este tema se pueden consultar: Reingold, B., Mrazik, R. & D´Jaen, M. (2010). Cloud Computing: Wose Law Governs The Cloud? (PART III). *Westlaw.* 15. 1. Ciudad: Ed. Thomson Reuters. Recuperado de http: http://www.techrepublic.com/whitepapers/cloud-computing-whose-law-governs-the-cloud-part-iii/1930805, Silver, G. (1 de Enero de 2012). *5 Key Considerations When Litigating Cloud Computing Disputes* Recuperado de http://www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202538844687&slreturn=1. y Kyer, C. & Stern, G. (2011). *Where in the World is My Data? Jurisdictional Issues with Cloud Computing.* Recuperado de http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/aea8833f-ab3c-48f1-854d-6ec4be989775/Jurisdictional_Issues_with_Cloud_Computing_Ian_Kyer_Gabriel_Stern.pdf.

tendido que cada país maneja de forma diferente la protección de los datos de las personas, se debe revisar con especial detenimiento por parte de la empresa contratante la jurisdicción en la cual se encuentran los servidores (por ende, en la cual residirá la información finalmente) y el domicilio de la empresa que presta el servicio.

Para definir datos personales tomaremos la definición consagrada en el proyecto de ley estatutaria numero 184 de 2010 del Senado de la República de Colombia y 046 de 2010 de la Cámara de Representantes, que en su artículo 5, literal c, define dato personal como "*cualquier información vinculada o que pueda asociarse a una o varias personas determinadas o determinables."*(Congreso de la República de Colombia, 2010, *Informe de conciliación al proyecto de ley número 046 de 2010 Cámara de Representantes, 184 de 2010 Senado de la República. Por medio de la cual se dictan disposiciones generales para la protección de datos personales*. Gaceta del Congreso Senado y Cámara).

Para el análisis que motiva este escrito, evaluaremos la situación considerando el ordenamiento jurídico colombiano. Según el mismo, la responsabilidad será de la empresa que recolecte, almacene, utilice, circule y elimine los datos personales, teniendo que sujetarse al cumplimiento de las normas, ya que la entidad puede entenderse como "operador"[23] o "fuente de la información"[24], "responsable"[25] o "encargado" del tratamiento en los términos de la futura Ley de protección de datos personales que se encuentra bajo estudio de la Corte Constitucional. Consecuentemente, la empresa deberá cumplir con una serie de requisitos legales frente a las entidades de control y los titulares de la información, con el agravante que cualquier transferencia a servidores que se encuentren fuera del territorio nacional se entenderá como transferencia internacional de datos, con las respectivas consecuencias jurídicas (Remolina-Angarita, Septiembre 9 de 2011, p. 12), que pueden ser, incluso, de tipo penal, tal como lo señalaremos posteriormente.

Es preciso hacer especial énfasis en la transferencia internacional de datos en el caso colombiano, ya que la Ley 1266 de 2008 en el numeral f, del artículo 5, establece que la facultad para decidir si un país, diferente a Colombia, ga-

23 El artículo 3, numeral c de la ley L266 de 2008 define el operador de la información como la *"persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley. Por tanto el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente".*

24 El artículo 3 numeral b de la Ley 1266 de 2008 define fuente de la información como la *"persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos"*

25 El autor hace referencia al proyecto de Ley número 046 de 2010 de la Cámara de Representantes y el proyecto de Ley 184 de 2010 del Senado de la República, el cual en su artículo 3 numeral e) establece que se entenderá por responsable del tratamiento a la *" persona natural o jurídica, pública o privada, que por si misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos".*

rantiza un nivel adecuado de protección, es del operador de la información. No obstante, en el proyecto de Ley 046 de 2010 de la Cámara de Representantes, bajo estudio por la Corte Constitucional, que trata sobre la protección de datos personales[26], establece en el artículo 26 que:

> *se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.* (Congreso de la República de Colombia, 2010, *Informe*).

Por tanto, si bien en la actualidad la potestad de revisar si el destinatario de la información tiene una adecuada protección o no de datos es de la empresa que opera la información, una vez sea Ley de la República el proyecto anteriormente expuesto se deberá revisar con especial atención la jurisdicción donde quede depositada la información.

En materia de protección de datos existen diferentes relaciones jurídicas y obligaciones, a saber:

• El Cloud Service Provider (CSP) y el usuario del servicio (Empresa, persona natural o jurídica, entidad pública): relación jurídica de naturaleza contractual, en la cual se paga por el arriendo de un espacio material para guardar información en el caso de (Infraestructura como servicio y plataforma como servicio) o acceso a un programa de computadora (presentándose una transmisión hacia los servidores del proveedor del servicio, en los supuestos en los cuales se almacene información en la nube).

• Entre el usuario del servicio y los titulares de los datos personales[27]: el usuario, al recopilar los datos personales, necesita autorización previa e informada del titular de la información (Proyecto de Ley número 046 de 2010, Cámara de Representantes, Artículo 9º) y (Proyecto de Ley 184 de 2010, Senado de la República), a su vez, al realizar el tratamiento de los datos personales se consideraría como responsable (Proyecto de Ley número 046 de 2010, Cámara de Representantes, Artículo 3º) y (Proyecto de Ley 184 de 2010, Senado de la República), ya que éste tendrá el poder de decisión al contratar el servicio con el CSP. Adicionalmente, debe observar los requisitos legales para realizar transferencias internacionales de datos personales a los países donde estén los data centers.

• Entre el CSP y los titulares de la información: el CSP se podrá entender como un encargado del tratamiento de los datos personales[28], ya

26 El proyecto de ley estatutaria número 184 de 2010 del Senado de la República de Colombia y 046 de 2010 de la Cámara de Representantes, al tratarse de una ley estatutaria, debe pasar un control previo y automático por parte de la Corte Constitucional. Por medio del Comunicado de prensa 040 del 5 y 6 de Octubre de 2011, el Alto Tribunal Constitucional manifestó, que los artículos 27,29,30 y 31 fueron declarados inexequibles y los artículos 8, 20, 23 y 26 declarados inconstitucionales, ahora bien, el texto completo de la sentencia C-748 de 2011 no se conoce en su totalidad y solo hasta que este sea publicado por la Corte Constitucional el proyecto de ley *"por la cual se dictan disposiciones generales para la protección de datos personales*" podrá pasar a sanción presidencial y por ende ser Ley de la República.

27 El artículo 2, numeral f, del proyecto de Ley número 046 de 2010 de la Cámara de Representantes y el proyecto de ley 184 de 2010 del Senado de la República, conocida como futura ley de protección de datos establece que el titular de los datos personales es la *"persona natural cuyos datos personales sean objeto de tratamiento"*.

28 El artículo 2 numeral f del proyecto de ley número 046 de 2010 de la Cámara de Representantes y el proyecto de ley 184 de 2010 del

que en efecto, está tratando los datos personales en nombre del usuario en desarrollo del contrato comercial. En el supuesto que el CSP se encuentre fuera del territorio Nacional se deberá revisar la normatividad de protección de datos de dicho país, teniéndose que pedir autorización expresa al titular si este país no cuenta con un nivel igual o superior que proporcione niveles adecuados para la protección de datos al colombiano (Proyecto de Ley número 046 de 2010, Cámara de Representantes, Artículo 26º) y (Proyecto de Ley 184 de 2010, Senado de la República).

• Por último el CSP al entenderse como encargado del tratamiento y el usuario como responsable de la información, serán los obligados a responder en el caso de violarse alguna de la normas de protección de datos. En el caso colombiano, bajo la futura Ley de protección de datos, mencionada en este artículo, tanto el CSP como el usuario podrán ser sujetos de multas de hasta 2000 salarios mínimos legales mensuales vigentes, así como la suspensión de las actividades relacionadas con el tratamiento de datos, cierre temporal de las operaciones e incluso el cierre inmediato y definitivo de la operación por parte de la Superintendencia de Industria y Comercio. (Proyecto de Ley número 046 de 2010, Cámara de Representantes, Artículo 23º) y (Proyecto de Ley 184 de 2010, Senado de la República).

En este punto resulta pertinente analizar algunas normas particulares de otros Estados sobre la materia:

Países como Japón adoptaron normas como la Personal Information Protection Act (PIPA) de 2003, la cual en su artículo 22 establece el concepto de la supervisión del fideicomisario. Por este se entiende que:

> *cuando un operador manipule información personal encomendada como individuo, o como operador de un negocio, en el cual se incluya manipulación de información personal en todo o en parte, éste deberá realizar una necesaria y apropiada supervisión de la información del depositario, asegurándose el control y la seguridad de la información personal.* (Natsui, p. 2).

Aquí se evidencia que, aunque se traslade la información, la empresa que entrega la información sigue teniendo responsabilidad sobre el manejo que el proveedor del mismo pueda dar a ésta, sin hacer referencia a las jurisdicciones a las que posiblemente se pueda enviar, evidenciándose un alcance ilimitado a las posibilidades que presenta hoy la tecnología cloud y maximizándose los beneficios de la misma.

En el caso de los Estados Unidos, normas como la Children's Online Privacy Protection Act (COPPA), la Gramm-Leach-Bliley Act (GLBA) y el Computer Fraud and Abuse Act (CFAA) entre otras regulaciones aplicables en función del mercado o sector económico en el cual se utilizan los datos, aseguran la jurisdicción basadas en la ubicación del titular de la información, a quien se le debe proteger su información personal, así esta fuese trasferida de servidores localizados en Estados Unidos a territorio extranjero a partir de la tecnología Cloud Computing (Reingold, Mrazik, D´Jaen, Febrero 2010, p. 3). De este modo, se sigue que la información que fuera entregada a

Senado de la República, conocida como futura ley de protección de datos establece que por encargado del tratamiento se entiende: *"persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento".*

una compañía en Estados Unidos, sin importar donde se encuentre en ese momento, deberá ser protegida bajo las normas de los Estados Unidos.

Ahora bien, la posición anteriormente expuesta presenta problemas en el efectivo cumplimiento de la jurisdicción, en el supuesto que los datos se encuentren fuera del territorio de los Estados Unidos. Esto se debe a que sólo cuando un proveedor tenga activos físicos en una jurisdicción las autoridades de ésta podrán ejercer de forma efectiva la competencia judicial o administrativa en contra del proveedor (Kyer, & Stern, 2011, p. 7). En caso contrario, sería muy complejo para los ejecutores de la ley, resultando necesaria la implementación de tratados internacionales con el fin de proteger los datos personales (Reingold, Mrazik, D´Jaen, Febrero 2010, p. 4). En el caso Alemán, la ley federal de protección de datos especifica la adquisición, procesamiento y almacenamiento de datos personales. En dicha norma los datos personales sólo podrán ser trasmitidos a países que tengan igual o mayor protección sobre los datos, con la característica específica de que si se traslada la información a un tercero, se le debe comunicar directamente a los involucrados (Doelitzscher, Reich & Sulistio, 2010, p. 931). Con esto se busca que las personas conozcan efectivamente la jurisdicción donde se encuentra su información; situación que, como se expuso anteriormente, también se presentaría en Colombia con la sanción presidencial del actual proyecto de Ley sobre la protección de datos personales.

Como se desprende de los casos anteriormente expuestos, la protección personal de datos varía dependiendo del país al que pertenecen los ciudadanos propietarios de la información y en el cual queden alojados los datos (Cloud Legal Project, Queen Mary, University of London, 5 de Marzo de 2012, R*esponse to the UK Ministry of Justice´s Call for Evidence on the European Comission´s Data Protection Proposals*). De este modo, es relevante para las empresas conocer el lugar donde efectivamente se encuentran los servidores de la compañía a la cual encomiendan sus datos antes de contratar servicios de almacenamiento en la nube; ya que, dada la condición intrínseca de la información, ésta debe ser manipulada con altos estándares de seguridad (Gellman, 2009, p.18). A modo de ilustración se puede mencionar el caso de Estados Unidos, en el cual la información de las entidades farmacéuticas y de las organizaciones financieras, por pedido de auditores fiscales y contadores, no se debe alojar en servidores cloud computing (Mowbray, Abril 2009, p. 134).

Ahora bien, algunas empresas pueden asegurar que la información va a estar ubicada en un país determinado; sin embargo, con la inamovilidad de los recursos se estaría quebrantando uno de los principios característicos de la tecnología que es la flexibilidad de la capacidad instalada, teniendo que pasar por un control previo antes de contratar el servicio, con el fin de definir dónde se encuentran los servidores. Este ejercicio podría ser realizado por las grandes compañías que poseen poder de negociación, pero no por las pequeñas o medianas empresas que no tendrán el tiempo, el conocimiento ni la capacidad de negociación para lograrlo (Corregio, p. 26-28). En este caso, la ley aplicable para la

protección de los datos será determinada por el lugar donde efectivamente se encuentren almacenados y donde el proveedor de servicios cloud tenga su sede social (Corrales, 2011, p. 16).

Es importante resaltar que todos los datos personales no tienen el mismo tratamiento. Existen los denominados datos sensibles[29], sobre los cuales existe una mayor protección e incluso una prohibición (con excepciones taxativamente establecidas en la Ley) para su tratamiento en la futura Ley de protección de datos personales de Colombia.

Esto último nos conduce a los efectos de la violación de datos personales y los potenciales efectos derivados del incumplimiento de las obligaciones consagradas en la legislación colombiana actual y futura. Sobre este punto particular, la Ley 1273 de 2009, por la cual se modificó el código penal y se creó el bien jurídico tutelado denominado protección de datos, establece en su artículo 269f la violación de datos personales, en los siguientes términos:

> *el que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, **intercambie, envíe**, compre, intercepte, divulgue, modifique o emplee códigos personales, **datos personales** contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.* (Subraya y negrilla fuera del texto original).

Es pertinente repetir la expresión consagrada por el artículo transcrito, "*sin estar facultado para ello",* hecho que significa que cualquier persona que transmita datos personales en el territorio nacional, sin estar facultado para ello (es decir, sin estar autorizados por el titular del dato o por la ley) y actué por provecho propio incurrirá en el tipo penal anteriormente transcrito.

III. CONCLUSIONES

Siguiendo el planteamiento realizado se evidencia que la prestación de los servicios de computación en la nube no se presenta como un nuevo tipo de contrato, sino como una forma de prestarse y consumirse los servicios apalancados en las bondades que ofrece Internet. Esto se configura como una verdadera revolución en el concepto de almacenamiento de información y el consumo de recursos tecnológicos que permite acceso remoto y un sin número de posibilidades para las empresas y los usuarios. Esta condición conlleva ahorro en costos gracias a la disminución de la capacidad instalada de las empresas en materia de servidores, así como ahorro en espacio físico, electricidad, servicios de mantenimiento y soporte.

Desde el punto de vista legal, no estamos ante un nuevo tipo de contrato. Se trata de una adaptación de los servicios ofrecidos a una forma de arrendamiento de un espacio en un Data Center

29 En los términos del proyecto de Ley número 046 de 2010 de la Cámara de Representantes y el proyecto de Ley 184 de 2010 del Senado de la República establece que: *"Para los propósitos de la presente ley, se entiende por datos sensibles aquellas que afecten la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales de derechos humanos o que promueva interés de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos"* (Artículo 5º).

para los casos de infraestructura como servicio y plataforma como servicio o un contrato de suministro en el caso de software como servicio. No obstante lo anterior, dicha clasificación no es excluyente, ya que al final, tanto la Infraestructura como servicio o plataforma obedecen a un servicio que se puede ubicar dentro del contrato de suministro.

De acuerdo a lo expuesto, no hay dificultades cuando ambas partes, el contratante del servicio en la nube (usuario), el proveedor de los servicios y los data centers se encuentran en el mismo país. Por el contrario, las discrepancias pueden presentarse cuando aquellos se encuentran en jurisdicciones diferentes o, cuando encontrándose en la misma, los servidores del que provee el servicio están fuera del territorio colombiano. Esta situación acarrea la discusión respecto a la territorialidad de la relación y sus posibles consecuencias (contractuales, protección de datos, responsabilidad extracontractual, penales y tributarias). Así, el derecho se enfrenta a un reto, como ciencia, que lo desafía a adaptarse a las situaciones de un mundo inmaterial en el cual las fronteras son accesorias, pues se puede acceder a la información sin importar dónde se encuentre.

Si bien en esta propuesta se plantean soluciones aproximadas a los conflictos antes enunciados, la principal conclusión que se deriva de esta investigación es que las normas jurídicas ya no se pueden analizar solamente frente a la jurisdicción de las partes. Por el contrario, es preciso estudiar las implicaciones, así como el lugar donde efectivamente se encuentra la información, las políticas de privacidad y de seguridad del proveedor del servicio y las garantías del servicio que ofrece el oferente del servicio; ya que estos son los factores determinantes a la hora de contratar con una empresa dedicada a los servicios de Cloud Computing.

Esta propuesta se configura como un reto para el derecho, ya que hasta el momento en que se llegue a acuerdos internacionales de cooperación o se armonicen las normas de los diferentes países buscando marcos regulatorios semejantes, existirán Estados más o menos proteccionistas, razón por la cual las organizaciones podrán tomar sus propias decisiones sobre dónde ubicarse o cómo ofrecer sus servicios. No obstante, en la medida en que los Estados se vuelvan excesivamente proteccionistas se generarán barreras al comercio y se podrá desincentivar la evolución del Cloud Computing, por lo que se deberá generar un equilibrio en el control, para no desmotivar la utilización de esta tecnología.

En el análisis puntual de Colombia, la necesidad de una normatividad específica en materia de Cloud Computing aún no se visualiza como imprescindible. No obstante, se debe considerar el caso de la protección de datos con el fin de proteger al consumidor o contratante del servicio cloud.

Es así como la computación en la nube se presenta como una alternativa para el almacenamiento de datos, el acceso a la información de un modo ubicuo y el acceso a servicios y plataformas desarrollados por terceros, sin tener que recurrir a una inversión en infraestructura. Pese a ello, no es posible olvidar que las leyes de todos los Estados son aplicables a las relaciones

que se generen sobre éstas, especialmente en lo relativo a los posibles perjuicios que se pueden causar; porque así como es relativamente simple contratar por la web, es proporcionalmente difícil, en algunos casos, encontrar a los responsables que puedan responder por las consecuencias, así como ejercer medidas sobre ellos, razón por la cual el consumidor deberá realizar un análisis del oferente del servicio con el fin de evitar inconvenientes futuros.

Bibliografía

Libros

Corrales, M., Barnitzke, B, & Forgó Nikolaus. (2011). *Aspectos Legales de la computación en la Nube: protección de datos y marco general sobre propiedad intelectual en la legislación Europea*. Trad. María Clara Bouchoux. Buenos Aires: Editorial Allbremática. (1ª Edición).

ISACA. (2009). *Computación en la nube: Beneficios de negocio con perspectivas de seguridad, gobierno y Aseguramiento.* IL, USA: Ed. Isaca, Rolling Meadows.

Gamboa, R. (2005). Soberanía estatal en internet; análisis desde la perspectiva de conflictos de jurisdicción y competencias en el plano nacional e internacional*. Comercio Electrónico*. Bogotá: Ed. Legis- Universidad de los Andes, Facultad De Derecho.

Marks, A. & Lozano, B. (2010). *Executive´s Guide To Cloud Computing*, NJ, USA: Ed. Wiley, Hoboken.

Reed, C. (2004). *Internet Law, Text And Materials, Second Edition*. Cambridge: Cambridge University Press.

Marchimi R. (2010) *A Practical Introduction To The Legal Issues.* London: Ed. British Standards Istitution.

Tamayo, J. (2011). *Tratado de Responsabilidad Civil, Tomo I.* Bogotá: Ed. Legis. (Segunda Edición).

Zuleta, A. (2010). La Responsabilidad Civil Extracontractual, Contractual y Precontractual De Las Personas Jurídicas. *Derecho de las Obligaciones.* Tomo II, Volumen I. Bogotá: Ed. Temis – Universidad de los Andes.

Revistas

Beaty, K. Kochut, A. & Shaikh, H. (2009). Desktop to cloud transformation planning, Parallel & Distributed Processing. IPDPS 2009*. IEEE International Symposium on*. 1-8. doi: 10.1109/IPDPS.2009.5161236.

Chunye G., Jie L, Qiang Z., Haitao C, & Zhenghu G. (2010). The Characteristics of Cloud Computing, Parallel Processing Workshops (ICPPW). *2010 39th International Conference.* 13, *(16)*, 275-279doi: 10.1109/ICPPW.2010.45. Dillon, T., Chen W. & Chang, E. (2010). Cloud Computing: Issues and Challenges. *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference.* 27-33. Recuperado de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5474674&isnumber=5474664.

Doelitzscher, F, Reich, C. & Sulistio, A. (2010). Designing Cloud Services Adhering to Government Privacy Laws, Computer and Information Technology (CIT). *2010 IEEE 10th International Conference on.* 930-935. doi: 10.1109/CIT.2010.172 Gellman, R. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. *World Privacy Forum*. Recuperado dewww.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

Greenberg, A., Hamilton, J. Maltz, A. & Patel, P. (2009). The cost of a cloud: research problems in data center networks. *Newsletter ACM SIGCOMM Computer Communication Review archive*. 39, *(1)*. NY, USA: ACM New York.

Marston, S., Zhi Li, Bandyopadhyay, S. & Ghalsasi, A. (2011). Cloud Computing - The Business Perspective. En System Sciences *(HICSS), 2011 44th Hawaii International Conference.* 4, (*7),* 1-11.. doi: 10.1109/HICSS.2011.102

Minqi Z., Rong, Z., Wei X.e, Weining, Q. & Aoying, Z. (2010). Security and Privacy in Cloud Computing: A Survey, Semantics Knowledge and Grid (SKG). *2010 Sixth International Conference on*. 1, *(3)*, 105-112 doi: 10.1109/SKG.2010.19 Mowbray, M. (April 2009). The Fog over the Grimp: Cloud Computing and the Law. *SCRIPTed Journal of Law, Technology and Society.* 6, *(1),* 132-146. DOI:10.2966/scrip.060109.132. Presented at the BrightTalk Cloud Security Summit, 30 Sept 2009; and to the West London branch of the BCS, 13 Oct 2009.

Petcu, D. (2010). Identifying Cloud computing usage patterns. *Cluster Computing Workshops and Posters (CLUSTER WORKSHOPS), 2010 IEEE International Conference*. 20, *(24)*, 1-8. doi: 10.1109/CLUSTERWKSP.2010.5613106.

Pearson, S. & Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on.* 93-702. doi: 10.1109/CloudCom.2010.66

Reingold, B., Mrazik, R. & D´Jaen, M. (Febrero 2010). Cloud Computing: Wose Law Governs The Cloud? (PART III). *Westlaw.* 15. *(1)*. Croydon, UK: Ed. Thomson Reuters. Recuperado de http: http://www.techrepublic.com/whitepapers/cloud-computing-whose-law-governs-the-cloud-part-iii/1930805

Robison, W., J. (2010). Free at What Cost?: Cloud Computing Privacy Under The Storage Communicatios Act. En *The Georgetown Journal*. 98, *(1195)*. Washington: USA.

Timmermans, J, Ikonen, V. & Stahl, B.,C. & Bozdag, E. (2010). The Ethics of Cloud Computing: A Conceptual Review, Cloud Computing Technology and Science (CloudCom). (2010). *2010 IEEE Second International Conference, Nov. 30 2010-Dec. 3 2010.* Recuperado de http://ieeexplore.

ieee.org/stamp/stamp.jsp?tp=&arnumber=5708509&isnumber=5708426.

University Of Chicago and The University of Southern California. (2002). *Introduction to Grid Computing*. The Globus Project™. Argonne National Laboratory. USC Information Sciences Institute. Recuperado de http://www.cs.umd.edu/class/spring2004/cmsc818s/Lectures/gridcomputingintro.pdf.

Zhang, S., Chen, X. Zhang, S. & Huo, X. (2010). The comparison between cloud computing and grid computing, Computer Application and System Modeling (ICCASM)*. 2010 International Conference.* Recuperado dehttp://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5623257&isnumber=5623111.

Zhixiong C. & Yoon, J. (2010). IT Auditing to Assure a Secure Cloud Computing, Services. *(SERVICES-1), 2010 6th World Congress*. Recuperado de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5575840&isnumber=5575460.

Normatividad mexicana

Estados Unidos Mexicanos, Presidencia de la República. (2011). Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Diario Oficial de la Federación*. México DF.

Normatividad colombiana

Congreso de la República de Colombia. (2000). *Ley 590 de 2000, Por la cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresa*. Diario Oficial No. 44.078 del 12 de Julio de 2000.

Congreso de la República de Colombia. (2000). *Ley 633 de 2000, Por la cual se expiden normas en materia tributaria, se dictan disposiciones sobre el tratamiento a los fondos obligatorios para la vivienda de interés social y se introducen normas para fortalecer las finanzas de la Rama Judicial.* Diario Oficial No. 44.275 del 29 de diciembre de 2000.

Congreso de la República de Colombia. (2008). *Ley Estatutaria 1266 de 2008, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*. Diario Oficial No. 47.219 del 31 de diciembre de 2008.

Congreso de la República de Colombia. (2008). *Código Civil*. Bogotá: Ed. Legis.

Congreso de la República de Colombia. (2010) *Código de Comercio*. Bogotá: Ed. Legis

Congreso de la República de Colombia. (2010) *Estatuto Tributario*. Bogotá: Ed. Legis- Dirección de Impuestos y Aduanas Nacionales DIAN.

Congreso de la República de Colombia. (2010). *Informe de conciliación al proyecto de ley número 046 de 2010 Cámara de Representan-*

tes, 184 de 2010 Senado de la República. Por medio de la cual se dictan disposiciones generales para la protección de datos personales. Bogotá: Gaceta del Congreso Senado y Cámara. Año XIX – n. 1.01. Miércoles 15 de Diciembre de 2010.

Congreso de la República de Colombia. (2011). *Ley 1480 de 2011, Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones*. Diario Oficial No. 48.220 de 12 del octubre de 2011.

Jurisprudencia americana

United States District Court Eastern District Of New York, Brooklyn Office. (Noviembre 29 de 2010*). Clark Street Wine And Spirits Vs. Emporos Systems Corporation.* Recuperado de http://docs.justia.com/cases/federal/district-courts/new-york/nyedce/1:2010cv01392/302617/47/0.pdf?1291114492.

Informes, reportes, documentos

Andre, M. (Julio 12 de 2010). *Sales and Use Taxation in the Clouds.* Recuperado de http://www.kpmginstitutes.com/taxwatch/insights/2010/pdf/wnit-071210-sales-use-taxation-in-clouds.pdf.

Breckinridge, C. (February 27, 2012). *From the Experts: Cloud Computing's Hidden Export Regulation Risks How to avoid violating U.S. trade controls when storing data in the cloud. Ed.* Corporate Counsel -ALM Media, Inc-. Recuperado de http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202543464867&thepage=1

Castro, Jorge, & Trimmiño Ana María. & Ramirez, Iván. & Montenegro, Mauricio, & Campo, Miryam, & Garzón Juan David. (Abril de 2010). *Cloud Computing: Una Perspectiva Para Colombia, Mesa Sectorial Cloud Computing*, Versión 1.0.0. Recuperado el 20 de Febrero de 2012. URL: http://www.interactic.org.co/documentos?page=shop.product_details&flypage=flypage.tpl&product_id=17&category_id=2.

Cloud Legal Project, Queen Mary, University of London. (5 de Marzo de 2012). *Response to the UK Ministry of Justice´s Call for Evidence on the European Comission´s Data Protection Proposals.* Recuperado de http://www.cloudlegal.ccls.qmul.ac.uk/docs/65220.pdf.

Corregio L., Laíse, D. & Walden, I. (s.f.). *Ensuring competition in the Clouds: The role of competition law?* Recuperado de http://ssrn.com/abstract=1840547.

Hon, W., K. Hornle, J. & Millard, C. (2011). Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3. *School of Law, Legal Studies Research Paper No. 84/2011*. London: Queen Mary University of London. , Recuperado de http://ssrn.com/abstract=1924240.

Hon, W. K., Millard C. & Walden I. (2010). The Problem of "Personal Data" in Cloud Computing – What information is Regulated? The Cloud of Unknowing, Part 1.

School of Law, Legal Studies Research Paper. 75. London: Queen Mary University of London. Recuperado de http://ssrn.com/abstract=1783577.

Hon, W. K., Millard, C, Walden, I. (2011). Who is Responsible for "Personal Data" in Cloud Computin? The Cloud of Unknowing, Part 2. *University of London, School of Law, Legal Studies Research Paper*. 77. London: Queen Mary Recuperado de http://ssrn.com/abstract=1794130.

Hon, W. K. & Millard, C. (2011). Data Export in Cloud Computing – How can Personal Data de Transferred outside the EEA? The Cloud of Unknowing, Part 4. *School of Law, Legal Studies Research Paper*. 85. London: Queen Mary University of London. Recuperado de http://ssrn.com/abstract=1925066.

Instituto Colombiano para la Evaluación de la Educación –ICFES (2011) *Comunicado de prensa 5 de Abril de 2011: ICFES Utiliza soluciones tecnológicas de vanguardia para la consulta de resultados*. Recuperado el 11 de Abril de 2013 http://www.icfes.gov.co/index.php?option=com_docman&task=doc_view&gid=4131.

Kang, Esq. Peter H. (2011). *Intellectual Property and Legal Issues Surrounding Cloud Comuting.* Recuperado el 23 de Febrero de 2012. URL: www.aipla.org/learningcenter/library/papers/MWI/11MWI/2011%20MWI%20Meeting%20Materials/Kang_Paper.pdf.

Kyer, C. & Stern, G. (2011). *Where in the World is My Data? Jurisdictional Issues with Cloud Computing.* Recuperado de http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/aea8833f-ab3c-48f1-854d-6ec4be989775/Jurisdictional_Issues_with_Cloud_Computing_Ian_Kyer_Gabriel_Stern.pdf.

Martínez, R. (2011). Los Retos de Cloud Computing. En *Revista Logicalis Now*. 5, *(14),* 52-55. Recuperado de http://www.la.logicalis.com/pdf/Logicalis%20Now%2014%20-%20Nota17%20-%20Los%20retos--(52-55).pdf.

Más Publicidad y Marketing (7 de Abril de 2010) *Cloud Computing ya tiene casos de éxito en Colombia.* Recuperado de http://maspublicidadymarketing.com/cloud-computing-ya-tiene-casos-de-exito-en-colombia.

Microsoft Corporation. (Enero de 2011) *Privacy and Data Access in a World of Online Computing: A Call To Action.* Recuperado de http://download.microsoft.com/download/2/9/5/295CE281-A6C4-4C6B-A677-3564C01AE52B/MicrosoftPrivacyandDatainCloud.doc.

Microsoft Corporation. (Junio 28 de 2011) *Microsoft Office 365: Identify For Enterprises, Service Description.* Recuperado de www.microsoft.com/downloads/info.aspx?na=41&srcfamilyid=6c6ecc6c-64f5-490a-bca3-8835c9a4a2ea&srcdisplayl

ang=en&u=http%3a%2f%2fdownload.microsoft.com%2fdownload%2f0%2f9%2f6%2f096C9441-8089-4655-ABB3-DC0ABA01A98D%2fOffice%20365%20Identity%20Service%20Description.docx.

Natsui, T. (s.f.). *Cloud Computing Service And Legal Issue*s. Recuperado de http// cyberlaw.la.coocan.jp/Documents/Cloud%20Computing%20Service%20and%20Legal%20Issues%20x.pdf

Ramgovind, S, Eloff, M., M. & Smith, E. (2010). *The management of security in Cloud computing. Information Security for South Africa (ISSA)*. Recuperado de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5588290&isnumber=5588257.

Reed, C. (2010). Information Ownership" in the Cloud. *School of Law, Legal Studies Research Paper.* 45. London: Queen Mary University of London. Recuperado de http://ssrn.com/abstract=1562461.

Remolina-Angarita, N. (Septiembre 9 de 2011). Cloud computing y protección de datos personales: aunque la responsabilidad esté en la nube, la responsabilidad se asumen en la tierra. Periódico Ámbito Jurídico. 330, 12.

Robison Breckinridge, C. (Febrero 27 2012). *From the Experts: Cloud Computing's Hidden Export Regulation Risks How to avoid violating U.S. trade controls when storing data in the cloud. Ed.* Corporate Counsel -ALM Media, Inc.-. Recuperado de http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202543464867&thepage=1Silver, G. (1 de Enero de 2012). *5 Key Considerations When Litigating Cloud Computing Disputes* Recuperado de http://www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202538844687&slreturn=1.

Velasco San Martin, C. (Febrero 28, 2009) *Jurisdictional Aspects Of Cloud Computing* Recuperado de http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf .

Walden, I. (s.f.). *Accesing Data in the Cloud: The Long Arm of the Law Enforcement Agent*. London: Queen Mary University Of London. Recuperado de http://ssrn.com/abstract=1781067.

Where are my files stored? (s.f.) Recuperado de

http://cyberlaw.la.coocan.jp/Documents/Cloud%20Computing%20Service%20and%20Legal%20Issues%20x.pdf