

**TIPOS DE CONFLICTOS JURÍDICOS DE HABEAS DATA EN LOS  
CONTRATOS DE ALMACENAMIENTO DE NUBE BANCARIA “*CLOUD  
BANKING*” EN COLOMBIA, EN EL QUE GOOGLE SEA PROVEEDOR Y SU  
RESOLUCIÓN A TRAVÉS DEL ARBITRAJE EN DERECHO**

**GLORIA AMPARO BRICEÑO FIGUEROA  
DOLLY ANDREA LUGO CORTÉS**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER  
FACULTAD DE CIENCIAS HUMANAS  
ESCUELA DE DERECHO Y CIENCIA POLÍTICA  
BUCARAMANGA**

**2017**

**TIPOS DE CONFLICTOS JURÍDICOS DE HABEAS DATA EN LOS  
CONTRATOS DE ALMACENAMIENTO DE NUBE BANCARIA “*CLOUD  
BANKING*” EN COLOMBIA, EN EL QUE GOOGLE SEA PROVEEDOR Y SU  
RESOLUCIÓN A TRAVÉS DEL ARBITRAJE EN DERECHO**

**GLORIA AMPARO BRICEÑO FIGUEROA  
DOLLY ANDREA LUGO CORTÉS**

Trabajo de grado para optar el título de  
**ABOGADA**

**DIRECTOR  
EDUARDO HERNANDO MUÑOZ SERPA.  
ABOGADO**

**CODIRECTOR  
JULIÁN ALFREDO CALDERÓN PEREIRA.  
ABOGADO**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER  
FACULTAD DE CIENCIAS HUMANAS  
ESCUELA DE DERECHO Y CIENCIA POLÍTICA  
BUCARAMANGA**

**2017**

## **AGRADECIMIENTOS.**

A Dios, por brindarme una vida llena de aprendizajes y experiencias; a mi familia, por su apoyo incondicional, en especial a mi madre Gloria Figueroa y a mi pequeño hijo Jose Ángel por ser el motor que me impulsa día a día a superarme para ser mejor persona y profesional.

A mi orgullosa Universidad Industrial de Santander por darnos la oportunidad de crecer profesionalmente; a nuestros docentes por todo el apoyo brindado a lo largo de la carrera, por su tiempo, amistad y por todos los conocimientos transmitidos. En este sentido, agradezco a nuestro director Eduardo Muñoz Serpa y codirector Julián Calderón Pereira por su valiosa dirección y crítica. A mis amigos, por ser una parte muy importante de mi vida, por su apoyo, ánimo y compañía en los momentos difíciles, en especial a Dolly, mi compañera de lucha, por hacer realidad este esfuerzo, al haber compartido conmigo sus conocimientos y sobre todo su amistad.

En general, cada una de las personas que de una u otra manera hicieron esto posible, a todos ustedes, mi mayor reconocimiento y gratitud en este camino que recién empieza.

Gloria Briceño.

Agradecida con Dios, mi mejor amigo, inspirador y dueño de mi vida, con mi mamá Lina Cortés Orjuela y mi hermana Sandra Patricia Lugo Cortés, quienes siempre han estado conmigo apoyándome en mi formación profesional, con el profesor Eduardo Muñoz Serpa, mi gran maestro y amigo, con Julián Calderón Pereira por su importante colaboración, con el profesor César Quijano y el ingeniero Leonardo Jaimes, quienes dispusieron de su tiempo para guiarnos en este trabajo, con mis amigos Gloria, Jimmy y Daniela quienes me motivaron a seguir con esta idea.

Al profesor Javier Alejandro Acevedo y al ingeniero Juan Carlos Escobar, quienes siempre han creído en mis capacidades, a mis docentes de la Escuela de Derecho y Ciencia Política, quienes aportaron al brindarme sus valiosas enseñanzas, apoyo y amistad, al personal administrativo de la Escuela de Derecho, la Dirección de Admisiones y Registro Académico, quienes me ayudaron en mi formación laboral y a la magnífica Universidad Industrial de Santander, mi gran casa de aprendizaje.

Dolly Lugo.

## CONTENIDO

INTRODUCCIÓN.....	13
1. ANTECEDENTES DE LOS CONTRATOS DE ALMACENAMIENTO DE NUBE BANCARIA, EL HABEAS DATA Y EL ARBITRAJE EN DERECHO.....	20
2. LAS FUENTES DE LOS CONFLICTOS RELACIONADOS CON EL HÁBEAS DATA EN LOS CONTRATOS DE ALMACENAMIENTO DE NUBE. ....	27
2.1 LAS PARTES DEL CONTRATO DE NUBE BANCARIA.....	27
2.2.1 Google como proveedor.....	27
2.2.2 Los bancos.....	31
2.2.3 Terceros.....	33
2.2 TIPO DE CONTRATO. ....	35
2.3 MODELOS DE DESPLIEGUE DE LA NUBE.....	38
2.4 LOS SERVICIOS. ....	39
2.4.1 Los servicios de Google con el banco. ....	40
2.4.2 Servicios del proveedor con el banco y la entidad financiera con los usuarios. .....	41
2.5 CLÁUSULAS CONTRACTUALES.....	45
2.5.1 Ausencia de cláusula arbitral. ....	46
2.6 LA RESPONSABILIDAD.....	47
2.6.1 La responsabilidad de Google como proveedor.....	47
2.6.2 La responsabilidad del banco. ....	48
2.6.3 La responsabilidad del usuario financiero.....	50
2.7 ANÁLISIS DEL CONTRATO DE GOOGLE Y LAS EMPRESAS. ....	50

2.8 ¿POR QUÉ ALGUNAS EMPRESAS NO CONTRATAN A GOOGLE? .....	55
3. LOS CONFLICTOS RELACIONADOS CON EL HABEAS DATA EN LOS CONTRATOS DE ALMACENAMIENTO DE NUBE. ....	56
3.1 FALTA DE NORMATIVIDAD. ....	56
3.2 LA INFLUENCIA DE LAS PARTES CONTRATANTES EN LOS CONTRATOS. .....	61
3.3 RESPONSABILIDADES RELACIONADAS CON LOS SERVICIOS DE COMPUTACIÓN EN LA NUBE.....	63
3.4 FALTA DE AUDITORÍAS.....	63
3.5 CONTRATACIÓN DE TERCEROS, POR PARTE DEL PROVEEDOR. ....	63
3.6 FALTA DE SEGURIDAD EN LA PROTECCIÓN DE LOS DATOS.....	64
3.7 AUSENCIA DE CONCIENCIA DE SEGURIDAD.....	66
3.8 ACCESO FÍSICO NO AUTORIZADO.....	67
3.9. LOS EMPLEADOS REVELAN INFORMACIÓN CONFIDENCIAL DE LA EMPRESA. ....	67
3.10 LOS RECURSOS COMPARTIDOS.....	68
3.11 DIFUSIÓN DE LA INFORMACIÓN PERSONAL.....	68
3.12 PÉRDIDA DE GOBERNANZA.....	69
3.13 PROPIEDAD DE LOS DATOS. ....	69
3.14 DEPENDENCIA DE PROVEEDORES CONCRETOS.....	70
3.15 LOS PROVEEDORES REVELAN INFORMACIÓN CONFIDENCIAL POR ORDEN POLICIAL O JUDICIAL. ....	71
3.16 DERECHOS DE AUTOR DE LAS OBRAS ALMACENADAS.....	72
3.17 ALMACENAMIENTO DE LA INFORMACIÓN EN UN SÓLO CENTRO DE DATOS. ....	73

3.18 EI RIESGO DE SHUTDOWN.....	73
3.19 LUGAR DONDE SE ALMACENAN LOS DATOS .....	73
3.20 LA JURISDICCIÓN COMPETENTE Y TIPO DE ACCIÓN JUDICIAL.....	74
3.21 SISTEMA JURÍDICO APLICABLE AL SERVICIO DE LA COMPUTACIÓN DE LA NUBE. ....	76
3.22 TRANSFERENCIA DE DATOS A OTROS PAÍSES. ....	77
3.23 NO ACCESO A LOS DATOS POR FALTA DE INTERNET.....	78
3.24 NO ACCESO A LOS DATOS POR EL DAÑO DE LOS SERVIDORES.....	79
3.25 AISLAMIENTO DE DATOS.....	80
3.26 SUPRESIÓN O MODIFICACIÓN DE DATOS INSEGURA O INCOMPLETA	80
3.27. LOS DATOS ALMACENADOS SON FALSOS. ....	81
3.28 RECUPERACIÓN DE DATOS.....	83
3.29 NULO CONTROL SOBRE LA DILIGENCIA DE LAS OPERACIONES DEL PROVEEDOR. ....	83
3.30 SECUESTRO DE SESIÓN O DE SERVICIO .....	83
3.31 ESPIONAJE EN EL PROVEEDOR DE LA NUBE Y ROBO DE INFORMACIÓN CORPORATIVA. ....	84
3.32 EL PODER DE LOS GOBIERNOS SOBRE EL MANEJO DE LA INFORMACIÓN. ....	84
4. CÓMO SE REPLICAN LOS CONFLICTOS DE HABEAS DATA EN LOS CONTRATOS DE ALMACENAMIENTO DE NUBE BANCARIA.....	87
4.1 CONSECUENCIAS DE ANALIZAR LOS CONFLICTOS JURÍDICOS RELACIONADOS CON EL HABEAS DATA EN EL CLOUD BANKING. ....	94
5. LA RESOLUCIÓN DE LOS CONFLICTOS DE HÁBEAS DATA EN EL CLOUD BANKING Y LA COMPETENCIA DEL ARBITRAJE EN DERECHO. ....	100
5.1 EJEMPLO DE RESOLUCIONES INTERNACIONALES.....	101

5.2 EJEMPLO DE LAUDO ARBITRAL EN COLOMBIA.....	103
5.3 LA COMPETENCIA DEL ÁRBITRO. ....	108
5.4 LA CLÁUSULA COMPROMISORIA. ....	110
5.5 EL COMPROMISO. ....	112
5.6 LAUDO EN DERECHO.....	112
5.7 EL ARBITRAJE INTERNACIONAL.....	113
5.7.1 El domicilio de las partes. ....	114
5.7.2 Lugar de cumplimiento de la obligación.....	116
5.7.3 Afectación de intereses comerciales.....	116
5.7.4 La ley aplicable. ....	116
5.8.LAS PRETENSIONES. ....	117
5.9 LAS MEDIDAS CAUTELARES INNOMINADAS.....	117
5.10 EL ANÁLISIS DE LA PRUEBAS. ....	119
5.11 MOTIVACIÓN DEL LAUDO.....	121
5.12 RESUELVE.....	121
6. CONCLUSIONES. ....	123
BIBLIOGRAFÍA.....	127

## RESUMEN

**Título:** Tipos de conflictos jurídicos de habeas data en los contratos de almacenamiento de nube bancaria “*cloud banking*” en Colombia, en el que Google sea proveedor y su resolución a través del arbitraje en derecho\*.

**Autores:** Gloria Amparo Briceño.  
Dolly Andrea Lugo Cortés\*.

**Descripción:** Esta investigación analizó la computación en la nube bancaria, un modelo que permite el acceso a la información mediante tecnologías que abordan una gran base de datos. Para recibir estos servicios, las entidades financieras contratan grandes proveedores como Google, empresa que elabora unilateralmente el contrato con condiciones que no pueden ser discutidas previamente. Empero, si los bancos contratan con otros proveedores se les da la oportunidad de modificar las cláusulas del contrato; y al tratarse de servicios profesionales que realizan las empresas proveedoras corresponde a un contrato de prestación de servicios, en los cuales se pueden presentar conflictos jurídicos de los que se deriva la vulneración del habeas data, por el incumplimiento de las cláusulas que determinan la separación de la información, la transferencia de datos a otros países, la indebida migración de la información, falta de auditoría y medidas de seguridad, uso de los datos con fines publicitarios, que derivan inquietudes relacionadas con el desconocimiento de la jurisdicción y ley aplicable para que los bancos puedan solucionar estas controversias ante un juez y no vulnerar los derechos de terceros.

Por lo anterior, se planteó como solución que estas controversias sean solucionadas por el mecanismo del arbitraje, resolviéndose con un laudo en derecho, toda vez que, se van a analizar las disposiciones del contrato que inciden directamente en la protección de los datos del consumidor financiero.

**PALABRAS CLAVE:** Proveedor, banco, nube bancaria, habeas data, información, contrato, conflicto y arbitraje.

---

\* Tesis de grado

\* Facultad de Ciencias Humanas, Escuela de Derecho y Ciencia Política. Director Eduardo Muñoz Serpa, codirector Julián Alfredo Calderón Pereira.

## ABSTRACT

**Title:** Types of habeas data legal conflicts in cloud banking storage contracts in Colombia, in which Google es a provider and its resolution through arbitration in law\*.

**Authors:** Gloria Amparo Briceño.  
Dolly Andrea Lugo Cortés\*.

**Description:** This research analyzed the cloud banking, a model that allows access to information through technologies that address a large database. To receive these services, financial entities hire large suppliers like Google, a company that unilaterally elaborates the contract with conditions that cannot be previously discussed. However, if banks contract with other suppliers they are given the opportunity to modify the clauses of the contract; But, in the case of professional services carried out by the supplier companies, it is a contract for the provision of services, in which legal disputes can arise, from which the breach of habeas data derives, for breach of the clauses that determine the separation of Information transfer, transfer of data to other countries, undue migration of information, lack of auditing and security measures, use of data for advertising purposes, which give rise to concerns related to the lack of jurisdiction and applicable law so that Banks can resolve these disputes before a judge and not violate the rights of third parties.

Due to the above, it was proposed as a solution that these disputes are resolved by the arbitration mechanism, being resolved with an award in law, since, will analyze the provisions of the contract that directly affect the protection of financial consumer data.

**KEY WORDS:** Provider, bank, cloud banking, habeas data, information, contract, dispute and arbitration.

---

\* Thesis, degree

\* Faculty of Human Sciences, School of Law and Political Science. Director Eduardo Muñoz Serpa, codirector Julián Alfredo Calderón Pereira.

“Se ha vuelto espantosamente obvio que nuestra tecnología ha superado nuestra humanidad”<sup>1</sup>

Albert Einstein

## INTRODUCCIÓN.

En la presente investigación se analizará el servicio de la computación en la nube bancaria, un modelo innovador que permite el acceso ubicuo<sup>2</sup> a los datos e información mediante un conjunto de recursos informáticos configurables (las redes, servidores, almacenamiento, aplicaciones y servicios), el cual es considerado como la etapa siguiente en la evolución del internet, que elimina la costosa tenencia y mantenimiento de *hardware*<sup>3</sup>, debido a tecnologías como la virtualización en donde se aborda con un mismo conjunto de recursos físicos una gran base de datos de usuarios con diferentes necesidades<sup>4</sup>.

En consecuencia, se mencionarán en el primer capítulo algunos bancos que adoptan en debida forma esta tecnología, no sólo reduciendo costos, sino maximizando la cartera de productos ofrecidos a sus clientes actuales, para captar otros nuevos, teniendo una capacidad ágil y flexible que responda adecuadamente

---

<sup>1</sup> Premisa cuya validez se corrobora al observar la cantidad de invenciones tecnológicas que permiten al ser humano suplir sus diversas necesidades, transformando de manera paulatina la naturaleza y su interacción con el entorno, repercutiendo en los bienes y servicios que circulan mediante las dinámicas comerciales establecidas entre los miembros de la sociedad. De esta manera, la tendencia al consumo excesivo que incrementa los factores de producción y el progreso del mundo empresarial ante las innovaciones tecnológicas, se han consolidado como un evento predominante, al aumentar los bienes y servicios ofertados, según los avances de la ciencia, la ingeniería, la globalización de los mercados y el desarrollo del ciberespacio; entendido como un conjunto de interconexiones electrónicas dispuestas en la red, es *per se*, un activo de la humanidad, un bien jurídico digno de protección y una tendencia exponencialmente creciente que mantiene vinculaciones recíprocas con el individuo, las instituciones, corporaciones, organizaciones; y con los bienes intangibles como la información, ver al respecto: MOLINA, José. Aproximación jurídica al ciberespacio. Instituto Español de Estudios Estratégicos. [en línea]. Disponible en <[http://www.ieee.es/Galerias/fichero/docs\\_opinion/2015/DIEEE0572015\\_Aproximacion\\_Juridica\\_Ciberespacio\\_MolinaMateos.pdf](http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEE0572015_Aproximacion_Juridica_Ciberespacio_MolinaMateos.pdf)> [citado el 22 de abril de 2017].

<sup>2</sup> Que está presente en todas partes al mismo tiempo.

<sup>3</sup> Son los componentes materiales de un sistema informático, (entrada, salida y almacenamiento), éstos están conectados a través de un conjunto de cables o circuitos, llamado bus, con la unidad central de proceso (CPU) del ordenador. Ver al respecto: Conceptos de hardware y software, [en línea] <<http://engendros.galeon.com/U1T6.htm>> [citado el 22 de abril de 2017].

<sup>4</sup> DEL VECCHIO, José, PATERNINA, Fabián. La computación en la nube: Un modelo para el desarrollo de las empresas. Vol. 13, No. 2, Julio-diciembre de 2015, pág. 82.

a las demandas del negocio y a la alineación con el área de la tecnología informática para generar una ventaja competitiva que acelere el aumento de rentabilidad<sup>5</sup>.

Igualmente, en el segundo capítulo, se identificarán las estrategias de los bancos encaminadas a crear nuevos actos jurídicos, relacionados con los avances tecnológicos<sup>6</sup>, para mantener control, supervisión, una estructura corporativa y alta prevención de los riesgos que pueden generar sus servicios<sup>7</sup>, al ser entidades bancarias, intermediarias en el mercado de dinero de capitales con actividades de captación, recepción de depósitos, financiación a personas o entidades, colocación de bonos, títulos, entre otras obligaciones que para su debido cumplimiento acceden a la tecnología del core bancario<sup>8</sup> con la computación en la nube.

Además, se analizará la infraestructura tecnológica de Google, como proveedor de nube, el cual en un principio surgió como un motor de búsqueda que permitía a los usuarios de internet encontrar la información que necesitan de manera expedita, pero que actualmente ha migrado a toda clase de productos y servicios web que buscan diversificar su objetivo, mediante condiciones generales planteadas a sus potenciales clientes y participantes de manera unilateral, para nada conmutativa en

---

<sup>5</sup>GASTÓN, Bruno. Cloud computing en la industria financiera. [en línea] <[http://www.palermo.edu/ingenieria/pdf2014/13/CyT\\_13\\_05.pdf](http://www.palermo.edu/ingenieria/pdf2014/13/CyT_13_05.pdf), 2013>, [citado el 22 de abril de 2017], páginas 71 y 72.

<sup>6</sup> "Una encuesta realizada por Avanxo, compañía especializada en servicio de computación en la nube, entre 800 ejecutivos de empresas colombianas del sector de las tecnologías de la información, arrojó que el 62 por ciento de las grandes compañías en Colombia ya utilizan la nube, principalmente soluciones de mensajería y colaboración, estrategias de relacionamiento con el cliente (CRM) y gestión del talento humano e infraestructura, lo que demuestra una alta penetración en el mercado colombiano". Ver al respecto Empresas le apuestan a estar en la nube, 14 de diciembre de 2011, [en línea] <<http://www.portafolio.co/tendencias/empresas-le-apuestan-nube-133834>> [citado el 22 de abril de 2017].

<sup>7</sup>El profesor del IESE Javier Zamora afirmó que, para que las empresas mejoren su competitividad es necesario utilizar las posibilidades que ofrecen las TIC sobre el resto de sus competidores. "Esto nos lleva a un cambio de paradigma. Sin un conocimiento de las posibilidades que ofrecen las nuevas tecnologías, el directivo no puede configurar una estrategia adecuada para su empresa". Ver al respecto: Las nuevas tecnologías y su impacto en la competitividad empresarial, [en línea], <<http://www.iese.edu/es/conoce-iese/prensa-noticias/noticias/2013/marzo/las-nuevas-tecnologias-y-su-impacto-en-la-competitividad-empresarial/>> 20 de marzo de 2013 [citado el 24 de abril de 2017]

<sup>8</sup> Core bancario –entendido como la plataforma donde se combinan la tecnología de la comunicación y la tecnología de la información para satisfacer las necesidades del negocio y de la industria bancaria– Ver al respecto: La Experiencia de Bancoldex. Core bancario: tecnología al servicio de la banca de desarrollo EN Alide [en línea]. Disponible en [http://www.alide.org.pe/fn11\\_fin\\_rev4\\_coreBancoldex.asp](http://www.alide.org.pe/fn11_fin_rev4_coreBancoldex.asp), [citado el 24 de abril de 2017]

"El core es tan importante, que el 60% de las entidades financieras de todo el mundo está pensando en cambiar su plataforma tecnológica para acelerar la mutación digital, así lo afirma el diario económico español, Cinco Días. Esto, porque la competencia acelerada de los startups más famosos en tecnología digital ha impulsado a los servicios bancarios a renovar su cartera de productos". Ver al respecto: ZAUZICH, Ivanna. La Importancia del Core Bancario en Bolivia, 16 de junio de 2016. EN COBIS [en línea]. Disponible en <http://blog.cobiscorp.com/como-tener-core-bancario-bolivia>> [citado el 24 de abril de 2017]

el cumplimiento de las obligaciones establecidas en el contrato a favor del proveedor<sup>9</sup> en el contexto de la sociedad de la información.

Aunque, si bien Google presenta estas condiciones en los contratos de almacenamiento de nube bancaria, es necesario identificar su responsabilidad y la de las entidades financieras, que tienen el deber de actualizar y rectificar permanentemente la información de sus usuarios reportada en las bases de datos, para que siempre sea verdadera y completa, involucrándose esta actividad con el *“derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma”*<sup>10</sup>, lo cual permite una mayor diligencia para las partes en el desarrollo del contrato y previsión ante cualquier riesgo.

En ese sentido, respecto de la protección de las bases de datos en los contratos de almacenamiento de nube bancaria, en el capítulo tercero de este trabajo se verificarán los conflictos que surgen relacionados con el habeas data, por los cuales los bancos buscan implementar la seguridad, privacidad, confidencialidad, integridad de los datos, requerimientos de autenticación, ubicación, disponibilidad y recuperación, preguntándose: *¿dónde guarda el proveedor de servicios de cloud banking<sup>11</sup> las cintas?, ¿si se borra la información en un sitio, se borra automáticamente en todos los demás sitios? ¿se emplean técnicas de blanqueo del medio o es posible que el próximo usuario recupere la información del volumen de*

---

<sup>9</sup> ORTEGA, Francisco. Derecho y TIC. Bogotá D, C: Temis S.A. ISBN 978-958-35-0863-9, páginas 304, 305 y 310.

<sup>10</sup> COLOMBIA, Constitución Política de 1991, artículos 15 y 20, citado por COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 de 2012 (octubre 17 de 2012) por la cual se dictan disposiciones generales para la protección de datos personales, Diario Oficial. Bogotá, D.C., 2012, artículo 1.

<sup>11</sup> De acuerdo con la Blazheski el “Cloud banking” o “Banca en la nube” se trata de servicios basados en la nube que utilizan las instituciones financieras para usos diferentes entre los que es posible mencionar “recursos humanos, correo electrónico, análisis de clientes, gestión de las relaciones con los clientes y desarrollo y prueba de productos”. Al trasladar los servicios básicos a la nube las entidades financieras, pueden adoptar unos modelos de implantación diferenciados en función del control, la gestión de los entornos informáticos y el nivel de exclusividad, como formas de prestación de los servicios en la nube. Ver al respecto: BLAZHESKI, Filip. ¿Banca en la nube o banca en las nubes? EN: BBVA. Observatorio Económico EEUU [en línea]. 2016. Disponible en <[https://www.bbvaesearch.com/wp-content/uploads/2016/05/160510\\_CloudBanking\\_esp.pdf](https://www.bbvaesearch.com/wp-content/uploads/2016/05/160510_CloudBanking_esp.pdf)> [citado en 8 de enero de 2017], pág. 1 y 3.

*datos?*, situaciones que se establecerán en el capítulo cuarto y que generarían varias controversias jurídicas complejas, porque cada país tiene diferentes regulaciones en cuanto a cómo se maneja la información de sus ciudadanos; y con el hecho de que *cloud banking* ofrece un modelo computacional que atraviesa fronteras puede llegar a ser un problema para estas instituciones financieras<sup>12</sup>.

Por tanto, una vez se presenten estos conflictos, que involucran el habeas data, se desarrollará en esta investigación en el capítulo quinto, un mecanismo de solución de conflictos que se encuentre regido por las normas del derecho internacional y que produzca efectos jurídicos en los diferentes Estados, tal como el arbitraje<sup>13</sup>, en el cual las partes difieren a árbitros la solución de un problema relativo a asuntos de libre disposición o aquellos que la ley autorice<sup>14</sup>, razonando una decisión jurídica que emplee estrictamente la norma aplicable al caso, según la interpretación de las cláusulas en los contratos de almacenamiento de nube bancaria.

Es decir, no se pretende analizar la vulneración del derecho fundamental al habeas data sino el incumplimiento de las obligaciones establecidas en el contrato, relacionadas con las medidas de seguridad, accesibilidad, niveles de servicios, aplicaciones, disponibilidad, tiempo de respuesta, capacidad de recursos que protegerían en la debida diligencia de las partes, las bases de datos de los individuos o personas jurídicas en el desarrollo de las funciones de la entidad bancaria. Así, con dichos resultados del análisis del contrato de almacenamiento de nube bancaria y la resolución de los conflictos a través del arbitraje se emitirán conclusiones en el sexto capítulo.

---

<sup>12</sup> GASTÓN, Bruno. Cloud computing en la industria financiera. [en línea] <[http://www.palermo.edu/ingenieria/pdf2014/13/CyT\\_13\\_05.pdf](http://www.palermo.edu/ingenieria/pdf2014/13/CyT_13_05.pdf), 2013>, [citado el 22 de abril de 2017], páginas 76 y 77.

<sup>13</sup> MINISTERIO DE JUSTICIA. Programa Nacional de Arbitraje. Arbitraje internacional. Disponible en <https://conciliacion.gov.co/portal/Arbitraje/-Qu%C3%A9-es-Arbitraje/Arbitraje-Internacional>.

<sup>14</sup> COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1563 de 2012” Por medio de la cual se expide el Estatuto de Arbitraje Nacional e Internacional y se dictan otras disposiciones”. Diario Oficial. Bogotá, D.C., 2012. artículo 1.

Por otro lado, en este trabajo se investiga el *cloud banking* en relación con el ciberespacio, porque es un modelo integrado por componentes de naturaleza material de base tecnológica, que evolucionan según los nuevos dispositivos como ordenadores, relojes inteligentes, *smartphones*, *tablets* entre otros, mediante los cuales se tiene acceso a la nube; de naturaleza inmaterial por la información y base de datos; de naturaleza sociológica fundamentada en la sociabilidad del ser humano al prestar y recibir servicios en un nuevo marco cultural (era digital) con efectos económicos, jurídicos y sociales, que tiene como límites la seguridad, el desarrollo y el respeto a los derechos humanos<sup>15</sup>, razones que incentivan a las entidades bancarias a realizar cambios y estar dispuestas a las nuevas tendencias del mercado, para crear nuevos negocios (*Startups*<sup>16</sup>); y de naturaleza jurídica, por los conflictos y sus resoluciones que se pueden presentar en el desarrollo de estos contratos de almacenamiento.

Por consiguiente, estos conflictos están relacionados con derechos fundamentales y el uso adecuado del internet, del cual según Frank La Rue, relator especial de la Organización de Naciones Unidas ONU en el 2011 debe ser de acceso universal, toda vez que, *“La única y cambiante naturaleza de internet no sólo permite a los individuos ejercer su derecho de opinión y expresión, sino que también forma parte de sus derechos humanos y promueve el progreso de la sociedad en su conjunto*<sup>17</sup>.

Al respecto, la Corte Constitucional en la Sentencia C-1147 de 2001 indicó: *“En Internet puede haber una realidad virtual pero ello no significa que los derechos, en dicho contexto, también lo sean”*, argumentando la necesidad de asegurar ciertas garantías mínimas a todos los usuarios que acceden a este sistema de información

---

<sup>15</sup>MOLINA, José. Aproximación jurídica al ciberespacio. Instituto Español de Estudios Estratégicos. [EN Instituto Español de Estudios Estratégicos, \[en línea\]. Disponible en <http://www.ieee.es/Galerias/fichero/docs\\_opinion/2015/DIEEO572015\\_Aproximacion\\_Juridica\\_Ciberespacio\\_MolinaMateos.pdf>](http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEO572015_Aproximacion_Juridica_Ciberespacio_MolinaMateos.pdf) [citado el 22 de abril de 2017]. página 3.

<sup>16</sup> *“Startup se define como una empresa pequeña o de reciente creación, delimitada en el tiempo y, por lo general, relacionada con el sector tecnológico. Una de sus bases es tener una idea innovadora y, con la aportación de unos pocos socios, intenta escalar hasta convertirse en un negocio rentable”* Ver al respecto: MUÑOZ, Ana, ¿Qué es Startup? [en línea]. Disponible en <http://computerhoy.com/noticias/internet/que-es-startup-56074> [24 de abril de 2017]

<sup>17</sup> El internet es un derecho según la ONU, 9 de junio de 2011. [EN CNN en español. \[en línea\]. Disponible en http://cnnespanol.cnn.com/2011/06/09/el-acceso-a-internet-un-derecho-humano-segun-la-onu/](http://cnnespanol.cnn.com/2011/06/09/el-acceso-a-internet-un-derecho-humano-segun-la-onu/) [citado el 24 de abril de 2017].

o a quienes desarrollan su actividad económica por este medio, en virtud de los derechos a la intimidad y el habeas data, para que la información registrada esté cobijada por mecanismos de protección, garantizándose un nivel de privacidad de los datos compartidos de acuerdo con la naturaleza y el contenido de los mismos<sup>18</sup>.

En consecuencia, para la protección de los datos personales en el almacenamiento de nube bancaria, se deben realizar contratos que obliguen al proveedor a realizar amplias medidas de seguridad que, ante cualquier incumplimiento, las partes puedan acudir a un mecanismo eficiente de solución de conflictos como el arbitraje, evitando los inconvenientes de cuál ley se aplica si las partes son de diferente lugar de procedencia o a cuál jurisdicción dirigirse.

Entonces, el arbitraje se configura en un medio eficaz que no sólo puede recurrir a los ingenieros para proferir un laudo técnico ante una controversia relacionada con aspectos tecnológicos, sino que también puede cuestionar en derecho el debido cumplimiento del contrato e interpretar las cláusulas establecidas por las partes, lo cual hace útil una investigación al respecto, en cuanto resalta la protección de los derechos fundamentales del cliente financiero en el desarrollo de la tecnología y construye un tejido social, al ser un mecanismo de resolución de conflictos; refiriéndose a las relaciones significativas que determinan formas particulares del ser, producir y proyectarse en la noción de respeto a los derechos de todos los miembros, que las partes cambien sus formas de participación social e incluso, que los empresarios revisen sus tradicionales formas de distribución de sus productos.

De esta manera, con el análisis del *cloud banking*, mediante una investigación cualitativa se busca obtener claridad acerca de los tipos de conflictos que se pueden presentar en el desarrollo de estos contratos bancarios, relacionados con el habeas data y su resolución en derecho, teniendo en cuenta un estudio estructurado y exploratorio de la doctrina, los laudos arbitrales, la jurisprudencia a nivel

---

<sup>18</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C-1147 de 2001. (13 de octubre de 2011) M.P Manuel José Cepeda Espinosa.

internacional y entrevistas semiestructuras a expertos en las tecnologías y el arbitraje<sup>19</sup>, lo cual se constituye en un insumo para posteriores investigaciones sobre el tema. Toda vez que, se han desarrollado aproximaciones sobre los riesgos relacionados con el almacenamiento de nube bancaria, pero no involucrando a Google como proveedor y a entidades financieras específicamente de Colombia, y tampoco, se mantiene un estudio de resolución de estos conflictos a través del arbitraje con un laudo en derecho.

---

<sup>19</sup> Estas entrevistas semiestructuradas fueron grabadas en audio y con previa autorización escrita de los entrevistados (consentimiento informado).

## 1. ANTECEDENTES DE LOS CONTRATOS DE ALMACENAMIENTO DE NUBE BANCARIA, EL HABEAS DATA Y EL ARBITRAJE EN DERECHO.

El profesor John McCarthy, en el año 1961, presentó el concepto de la computación como un servicio, al igual que la electricidad, el agua, gas y otros, pero en ese momento, la tecnología no permitía que este concepto fuera ampliamente adoptado en computación y desapareció por un tiempo<sup>20</sup>.

Hasta en la década de los noventa, sólo las empresas de telecomunicaciones ofrecían redes privadas virtuales (VPN)<sup>21</sup>. Así, uno de los pioneros, en 1999 fue *Salesforce.com*, con el concepto de entrega de aplicaciones empresariales a través de una página web, aunque en el 2002, Amazon lanzó *Amazon Web Service*<sup>22</sup> y en el 2006 se lanzó *Google Docs*<sup>23</sup>, con el concepto al público de *cloud computing*<sup>24</sup>.

En el 2008, nacieron los proyectos de *software libre* *Eucaliptus* y *Open Nebula*, que pueden crear nubes privadas, hasta el 2009, *Microsoft* incursiona lanzando *Windows Azure*<sup>25</sup>, en el 2010 nace *Openstack*<sup>26</sup>, un proyecto de *Rackspace*<sup>27</sup> en

---

<sup>20</sup> MACHADO, Jesús. Blogs Computación en la nube: Conceptos y recomendaciones, marzo 4 de 2015. [en línea] Disponible en <<https://blogs.vmware.com/latam/2015/03/computacion-en-la-nube-conceptos-y-recomendaciones.html>> [citado por 24 de abril de 2017].

<sup>21</sup> "Una VPN (*Virtual Private Network*) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar una VPN para que sus empleados desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían. Sin embargo, conectar la computadora de un empleado a los recursos corporativos es solo una función de una VPN". Ver al respecto: GOUJON, André, ¿Qué es y cómo funciona una VPN para la privacidad de la información?, 10 de septiembre de 2012, [en línea], <http://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/> [citado el 23 de abril de 2017]

<sup>22</sup> *Amazon Web Services* (AWS) es una plataforma de servicios de nube que ofrece potencia de cómputo, almacenamiento de bases de datos, entrega de contenido y otra funcionalidad para ayudar a las empresas a escalar y crecer. Ver al respecto <<https://aws.amazon.com/es/what-is-aws/>>.

<sup>23</sup> "Google Docs es un procesador de texto y hoja de cálculo, todo en línea, que nos permite crear nuevos documentos, editar los que ya teníamos o compartirlos en la red con otros usuarios" Ver al respecto [http://alerce.pntic.mec.es/bmarco1/pagina\\_web/googledocs.htm](http://alerce.pntic.mec.es/bmarco1/pagina_web/googledocs.htm)

<sup>24</sup> Computación en la Nube. Guatemala, 2012. [en línea] Disponible en <http://todosobrelanube.blogspot.com.co/p/historia.html> [citado el 24 de abril de 2017]

<sup>25</sup> *Microsoft Azure* es una colección de servicios integrados en la nube (análisis, procesos, base de datos, móviles, redes, almacenamiento y Web) Ver al respecto <https://azure.microsoft.com/es-es/overview/what-is-azure/>

<sup>26</sup> *OpenStack* es una plataforma cloud computing de software libre que en tan solo tres años de desarrollo se ha convertido en una de las principales opciones para implementar un cloud de IaaS público o privado. Ver al respecto: MOLINA, Alberto, ¿Qué es eso de OpenStack y por qué debería conocerlo? 25 de noviembre de 2013 [en línea] Disponible en <https://openwebinars.net/blog/que-es-eso-de-openstack-por-que-deberia-conocerlo/> [citado el 23 de abril de 2017].

<sup>27</sup> *Rackspace* es una compañía de gestión de computación en la nube, ver al respecto <https://www.rackspace.com/es-co/about/history>.

conjunto con *la NASA*, y *Vmware vCloud Director*<sup>28</sup> y en el 2011 *Apple* lanzó su servicio *Cloud* para cambiar la forma de usar los computadores, fomentando el lanzamiento de productos de nube para cualquier empresa<sup>29</sup>.

Por lo anterior, varias empresas comenzaron a utilizar esta tecnología para optimizar funciones y ofrecer mejores servicios a sus clientes, como es el caso de los bancos que ante la necesidad de ir al ritmo de las expectativas de los consumidores, la obligación de buscar modelos innovadores, flexibles y rentables en las soluciones financieras se fueron adaptando a los cambios del mercado con la computación en la nube que ofrece vías alternas para acceder a la tecnología del core bancario<sup>30</sup>.

Aunque, si bien las entidades financieras empezaron a mediados del siglo XX a hacer uso de la tecnología para automatizar y acelerar procesos, desde finales de la década de 1950, los bancos han dependido de servidores para el procesamiento de los datos, en 1955 utilizaron la primera computadora para procesar cheques, posteriormente, en la década de 1980 y 1990 emplearon las computadoras personales (PC), permitiendo el acceso a redes externas a través de la web y del correo electrónico y la banca en línea por los avances del internet, ofreciendo flexibilidad y comodidad a los clientes y reduciendo costos<sup>31</sup>.

De tal manera, prácticamente todos los bancos tienen soluciones en la nube, por ejemplo Unisys<sup>32</sup> está apoyando a una institución financiera que decidió migrar gran parte de sus activos a este modelo, bajo el requerimiento de garantizar los más altos

---

<sup>28</sup> MACHADO, Jesús. Blogs Computación en la nube: Conceptos y recomendaciones, marzo 4 de 2015. [en línea] Disponible en <<https://blogs.vmware.com/latam/2015/03/computacion-en-la-nube-conceptos-y-recomendaciones.html>> [citado por 24 de abril de 2017].

<sup>29</sup> Computación en la Nube. Guatemala, 2012. [en línea] Disponible en <http://todosobrelanube.blogspot.com.co/p/historia.html> [citado el 24 de abril de 2017].

<sup>30</sup> Banca en la nube. La computación en la nube es el futuro de la tecnología bancaria. EN TENEMOS, [en línea] Disponible en <https://www.temenos.com/es-mx/productos-y-servicios/banca-en-la-nube/>. [citado el 24 de abril de 2017]

<sup>31</sup> : BLAZHESKI, Filip. ¿Banca en la nube o banca en las nubes? EN: BBVA. Observatorio Económico EEUU [en línea]. 2016, P. 1. Disponible en <[https://www.bbvarresearch.com/wp-content/uploads/2016/05/160510\\_CloudBanking\\_esp.pdf](https://www.bbvarresearch.com/wp-content/uploads/2016/05/160510_CloudBanking_esp.pdf)> [citado en 8 de enero de 2017], pág. 1

<sup>32</sup> Unisys es una compañía global de tecnología de información que ofrece soluciones para desafíos de alta complejidad, ver al respecto <http://www.unisys.com.ar/>.

niveles de seguridad y capacidad de gestión de sus datos y activos establecidos por el Consejo de Instituciones Financieras Examen Federal (FFIEC)<sup>33</sup>, por su parte, Defontana<sup>34</sup> realizó con el Banco de Crédito e Inversiones Bci un sistema online que se conecta directamente para pagos y gestión en línea con una entidad para el sector pyme, involucrándose en servicios como factura electrónica, ventas, contabilidad, cuentas por cobrar y pagar, tesorería y nómina de pagos. Además, el banco de Chile desarrolló con la tecnología en la nube de la empresa SAP, la aplicación “Mi Banco” permitiendo que todos los cuentacorrentistas efectúen transferencias de dinero, pago de tarjetas de crédito, pago de cuentas, consulta de saldos, movimientos y recargas de celular<sup>35</sup>.

Asimismo, el banco australiano *Commonwealth Bank* es un ejemplo, habiendo iniciado negocios en el 2009 con diversos proveedores para superar los servicios básicos brindados por las entidades financieras; *RenMoney*, entidad financiera localizada en Nigeria también se considera como el caso de éxito africano y es un ejemplo que cambia la visión de la industria global, pues sus servicios financieros están totalmente en *Cloud*, igualmente *ScotiaBank*, uno de los cinco grandes bancos de Canadá ha implementado el core bancario enteramente en la nube como un servicio. También, Ecuador tiene una entidad financiera especializada en la banca *retail*<sup>36</sup> y de microfinanzas, y es uno de los bancos con mayor número de clientes y cartera, su core bancario está implementado de la manera tradicional en su propio *data center*<sup>37</sup> y sólo ciertos servicios internos están implementados en un esquema de *Cloud Computing* como: consultas de comportamiento de pagos,

---

<sup>33</sup>El FFIEC de Estados Unidos es un consejo especial compuesto por representantes de diversos organismos, como el Banco de la Reserva Federal, la Administración Nacional de Cooperativas de Crédito, la Oficina de Supervisión de Ahorros, la Oficina del Contralor de la Moneda y la Federal *Deposit Insurance Corporation* que hace recomendaciones sobre la ética que se adherirá a cada organismo representado. ¿Ver al respecto Qué es el Consejo Federal de Instituciones Financieras examen? [en línea]. 12 de septiembre de 2010. Disponible en <<http://www.prucommercialre.com/que-es-el-consejo-federal-de-instituciones-financieras-examen/>> [citado el 22 de abril de 2017]

<sup>34</sup> Defontana es la empresa líder del mercado latinoamericano en la implementación de software ERP, expertos en ERP online. Ver al respecto <http://www.defontana.com/seleccion.html>.

<sup>35</sup> FAJARDO, Daniel. Pasión por los negocios. Por qué los bancos y la industria financiera se están entusiasmando en la nube híbrida. EN Revista Pulso. [en línea] Disponible en <http://www.pulso.cl/noticia/tech/industria/2015/05/76-64216-9-por-que-los-bancos-y-la-industria-financiera-se-estan-entusiasmando-en-la-nube.shtml> [citado el 21 de abril de 2017].

<sup>36</sup> *Retail* es el término inglés para comercio al por menor o al detalle.

<sup>37</sup> *Data center*. Es donde están físicamente todos los servidores y se guarda la información. JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

modelos de campañas de crédito y consultas a burós de crédito<sup>38 39</sup>. Por el contrario, en Argentina, las entidades bancarias aún no han implementado masivamente el *Cloud Computing*, y las que han comenzado a incursionar, lo han hecho con aplicaciones como el mail corporativo, soluciones de productividad, colaboración, y aplicaciones de oficina<sup>40</sup>.

De tal forma, Andre Frederico<sup>41</sup>, director ejecutivo de planeación y marketing de Tivit, empresa brasilera, indicó que la nube ha permitido a los bancos mejorar la atención a sus clientes, hacer transacciones y realizar sistemas de pago electrónico de última generación “*con el fin de respaldar las transacciones desde dispositivos móviles*”. Además, con el *cloud banking* según el peruano Álvaro Merino Reyna<sup>42</sup>, gerente general de IBM, se previene el fraude en las transacciones bancarias y electrónicas, la mejora en la interacción entre el Estado y los ciudadanos, la optimización de procesos y reducción de costos, entre otros.

En Colombia, una de las primeras instituciones financieras que analizó la necesidad de tener el acceso a la nube fue el Banco Santander, con el fin de convertirse en un banco con almacenamiento de datos, acceso a las nuevas tecnologías y competitividad con los *startups* financieros. Igualmente, el banco BBVA migró su sistema de correo corporativo a *Google Apps*<sup>43</sup> con el propósito de aumentar la eficiencia, trabajar desde cualquier lugar; al entenderse, según uno de los directivos

---

<sup>38</sup> Empresa de México que proporciona información sobre el historial crediticio de las personas. Ver al respecto <<http://www.burodecredito.com.mx/glosario.html>>

<sup>39</sup> GONZÁLEZ, Hugo. Implementación y uso de un *core bancario* para banca retail en la tecnología *cloud computing*. Trabajo de grado de Magister en Gerencia de Tecnología de la información, Quito: Pontificia Universidad Católica de Ecuador. Maestría en Gerencia de Tecnología de la información. [en línea], mayo de 2015 Disponible en <http://repositorio.puce.edu.ec/bitstream/handle/22000/8539/CASO%20DE%20ESTUDIO%20-%20Hugo%20Gonzalez.pdf?sequence=1>, [citado el 12 de abril de 2017] .Páginas 34, 37, 38,40 y 41

<sup>40</sup> NOCETI, Héctor Y FREIJO, Aníbal. Cloud computing. Su aplicación en la banca privada Argentina. Buenos Aires, Argentina: Universidad Argentina de la Empresa (UADE) Facultad de Ingeniería y Ciencias Exactas, [en línea] Disponible en <<http://44jaiio.sadio.org.ar/sites/default/files/sts264-276.pdf> > [citado el 23 de abril de 2017] pág. 275.

<sup>41</sup> Los negocios de la “nube” viven una verdadera danza de los millones. 3 de marzo de 2016. EN Dinero [en línea]. Disponible en <<http://www.dinero.com/edicion-impresa/negocios/articulo/crecimiento-de-los-negocios-en-la-nube-o-cloud-en-el-2016/220999>> [citado el 8 de marzo de 2017].

<sup>42</sup> IBM inaugura el mayor centro de datos en nube de Colombia. EN: La vanguardia. [en línea]. Disponible en <http://colombia-inn.com.co/ibm-inaugura-el-mayor-centro-de-datos-en-nube-de-colombia-3/>, [citado el 25 de febrero de 2017]

<sup>43</sup> “Google Apps es un conjunto de aplicaciones que nos permite organizar de forma sencilla todo nuestro trabajo, y la comunicación entre los distintos trabajadores con diversas herramientas para la gestión del correo electrónico, mensajería instantánea, planificación de reuniones y tareas, generación de documentos”, etc. Ver al respecto <https://www.imaginanet.com/blog/google-apps-que-te-ofrece.html>

del BBVA que, *"el dinero son datos": "Los datos se pueden transformar en información, la información en conocimiento, y el conocimiento en nuevos productos"*<sup>44</sup>

No obstante, ante los diferentes riesgos por el almacenamiento de datos, estas entidades financieras colombianas están reguladas por una normatividad especial que les permite a las entidades vigiladas por la Superintendencia Financiera tomar medidas efectivas para garantizar que la entrega de la información a terceros esté sujeta a la verificación y cumplimiento de ciertos requisitos mínimos, según la ley de habeas data<sup>45</sup>.

De tal forma, en el ordenamiento jurídico colombiano está la Ley 1266 de 2008, por medio de la cual se dictan disposiciones generales del habeas data, el manejo de la información en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros<sup>46</sup>, luego, mediante el Decreto 1227 de 2005 se determinó la forma como se debía presentar la información<sup>47</sup>, en el Decreto 2952 de 2010 se aclararon vacíos normativos respecto de la Ley Estatutaria de protección de los datos financieros<sup>48</sup> y después la Superintendencia de Industria y Comercio, a través de la Resolución 76434 de 2012 dio instrucciones relativas a la protección de datos personales y el cumplimiento de la Ley de habeas data<sup>49</sup>.

---

<sup>44</sup> ZAUZICH, Ivanna. Cloud banking: De qué se trata la banca en la nube y cómo implementarla. 22 de marzo de 2016 EN Cobiscorp blog. [en línea] Disponible en <<http://blog.cobiscorp.com/banca-en-la-nube-cloud-banking>> [citado el 23 de marzo de 2017].

<sup>45</sup> COLOMBIA. SUPERINTENDENCIA FINANCIERA. Circular 052 de 2007 (octubre de 2007), [en línea]. Disponible en <https://www.bancodebogota.com/wps/themes/html/banco-de-bogota/pdf/nuestra-organizacion/transparencia/circular-052.pdf> [citado el 24 de marzo de 2017]

<sup>46</sup> COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 de 2008 (diciembre 31 de 2008), por la cual se dictan las disposiciones generales del habeas 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. Bogotá, D.C., 2008.

<sup>47</sup> COLOMBIA. PRESIDENTE DE LA REPÚBLICA, Decreto 1227 de 2005, por el cual se reglamenta parcialmente la Ley 909 de 2004 y el Decreto-ley 1567 de 1998. (abril 21 de 2005), [en línea]. Disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=16313> [citado el 04 de abril de 2017].

<sup>48</sup> COLOMBIA. PRESIDENTE DE LA REPÚBLICA, Decreto 2952 de 2010, Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008. (agosto 6 de 2010). [en línea]. Disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=40120> [citado el 21 de abril de 2017].

<sup>49</sup> COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 76434 de 2012 (diciembre 4 de 2012) Diario Oficial No. 48.635 de 5 de diciembre de 2012

Posteriormente, se promulgó la Ley 1581 de 2012 sobre la protección de datos personales para “*desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma*”<sup>50</sup>.

Además, la Corte Constitucional en la Sentencia T-833 de 2013 al hacer un análisis del habeas data en las entidades financieras indicó que:

*Tanto las entidades que recopilan y administran información crediticia como aquellas que efectúan reportes a las primeras tienen el deber de garantizar a los titulares de la misma que su actuación es respetuosa de las garantías fundamentales. En particular, la jurisprudencia constitucional ha señalado como obligaciones específicas a cargo de estos sujetos las de verificar (i) que la información sea veraz; (ii) que haya sido recabada de forma legal, y (iii) que no verse sobre aspectos reservados de la esfera personal del individuo*<sup>51</sup>.

Luego, para tutelar los derechos al habeas data y el derecho a la información, la Corte en Sentencia T-246 de 2014 afirmó:

*Así las cosas, la información que reposa en las bases de datos financieras, debe observar los principios establecidos para el derecho a la información personal, pues los datos que allí se conservan, permiten a los usuarios del sistema financiero acceder a prerrogativas como créditos de consumo y adquirir obligaciones bancarias, además de determinar los riesgos de los usuarios actuales y futuros del sistema financiero, pues dicha información es de interés público*<sup>52</sup>.

Por lo anterior, los conflictos relacionados con el habeas data, pueden surgir en el desarrollo de los contratos entre los bancos, proveedores y terceros relacionados con el derecho informático, el incumplimiento de las cláusulas contractuales, cuya resolución puede darse a través del arbitraje en derecho como sucede en el Colegio

---

<sup>50</sup> COLOMBIA, Constitución Política de 1991, artículos 15 y 20, citado por COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 de 2012 (octubre 17 de 2012) por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012.

<sup>51</sup> COLOMBIA. CORTE CONSTITUCIONAL. Sentencia T-833 de 2013 (diciembre 3 de 2013) M.P Luis Guillermo Guerrero Pérez.

<sup>52</sup> COLOMBIA. CORTE CONSTITUCIONAL. Sentencia T-246 de 2014 (abril 11 de 2014) M.P Mauricio González Cuervo.

Profesional de Ingenieros en Informática de la Comunidad de Madrid que incorpora árbitros que sean ingenieros y abogados en ejercicio con conocimientos demostrables en informática por el evidente desconocimiento de los jueces y Tribunales en las cuestiones técnicas que se plasman en los contratos de tecnología desarrollados por las partes<sup>53</sup>.

---

<sup>53</sup> COLEGIO PROFESIONAL DE INGENIEROS EN INFORMÁTICA DE LA COMUNIDAD DE MADRID CPIICM. Reglamento de la Corte de Arbitraje (8 de junio de 2016). [en línea] Disponible en <http://cpiicm.es/wp-content/uploads/sites/3/2016/06/Reglamento-Corte-Arbitral-CPIICM.pdf> [citado el 06 de marzo de 2017].

## 2. LAS FUENTES DE LOS CONFLICTOS RELACIONADOS CON EL HÁBEAS DATA EN LOS CONTRATOS DE ALMACENAMIENTO DE NUBE.

### 2.1 LAS PARTES DEL CONTRATO DE NUBE BANCARIA.

Según el artículo 1602 del Código Civil colombiano “*todo contrato legalmente celebrado es una ley para los contratantes*”<sup>54</sup>, razón por la cual, en este tipo de contratos de almacenamiento de nube bancaria, es necesario identificar a las partes:

**2.2.1 Google como proveedor:** Es la persona jurídica encargada de la protección de los datos personales, por cuenta del banco. Google es quien presta los servicios de computación en la nube cuando suministra los medios y la plataforma<sup>55</sup>.

Google es una de las empresas monopolísticas de la información más exitosas en el mundo de la tecnología y su buscador es el sitio más usado de toda la Internet, empezó en 1995 cuando Larry Page y Sergey Brin se reúnen en Stanford y empiezan a colaborar en un motor de búsqueda llamado *BackRub*, el cual cambian de nombre a Google, por el juego de la palabra “googol”, un término matemático representado por el número 1 seguido por 100 cero. Motor que con el tiempo se convirtió en el más utilizado en la web, permitiendo la invención de servicios como: *Gmail, Google Maps, Google News, Google Video, YouTube, Picasa, Google Chrome*, entre otros<sup>56</sup>.

Productos que trajeron a la mente del público la novedad de subir y editar documentos en la red, las funciones de *Google Docs*, (una simulación de Microsoft)

---

<sup>54</sup>COLOMBIA. Ley 57 de 1887. Código Civil. [en línea] Disponible en <<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=39535>>, [citado el 24 de abril de 2017], artículo 1602.

<sup>55</sup> SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Manual de protección de los datos personales en los servicios de contratación en la nube (cloud computing). [en línea] Disponible en [https://issuu.com/quioscosic/docs/cartilla\\_proteccion\\_datos](https://issuu.com/quioscosic/docs/cartilla_proteccion_datos) [citado el 3 de marzo de 2017].

<sup>56</sup> Historia de Google, 11 de enero del 2011. EN Blog historia de la informática, [en línea] Disponible en <http://histinf.blogs.upv.es/2011/01/11/historia-de-google/> [citado el 20 de febrero de 2017].

creado en el año 2006,<sup>57</sup> un asidero de la estrategia tecnológica de almacenar información de empresas que construyen espacios en la web de forma rápida, sin complejidad y de alto nivel en los clientes y terceros.

Aunque, según Monroy<sup>58</sup> tal vez la primera referencia a *cloud computing* se debe a Eric Schmidt, CEO<sup>59</sup> y presidente de Google durante la conferencia de “*Search Engine Strategies*”, el 9 de agosto de 2006, con el siguiente comentario:

*“(...) Lo que ahora es interesante es que está emergiendo un nuevo modelo, y todos ustedes están aquí porque son parte de ese nuevo modelo. No creo que la gente realmente esté entendiendo lo grande que es esta oportunidad. Comienza con la premisa de que los servicios de datos y la arquitectura deben estar en los servidores. Lo llamamos cloud computing - que deben estar en la "nube", en algún lugar. Y que, si usted tiene cualquier tipo de navegador o tipo de acceso, no importa si dispone de un PC, o un Mac, o un teléfono móvil, o una BlackBerry, o lo que sea - o nuevos dispositivos todavía no desarrollados - usted puede tener acceso a la nube. Hay una serie de empresas que se han beneficiado de esta. Obviamente, Google, Yahoo!, eBay, Amazon nos vienen a la mente...”*

Así, Google empezó a desarrollar una infraestructura para proporcionar seguridad a través de todo el ciclo de vida del procesamiento de la información, la cual proporciona un despliegue seguro de servicios, almacenamiento de datos, protección de la intimidad, comunicación privada con los clientes a través de Internet. Además diseña y construye sus propios centros de datos con varias estrategias físicas de seguridad como la identificación biométrica, cercas perimetrales, detección de metales, cámaras, sistemas de detección de intrusos basados en láser, chips de seguridad que permiten identificar y autenticar los dispositivos legítimos de Google, firmas criptográficas y filtrado de entradas y salidas en varios puntos de la red para evitar la suplantación del número que

---

<sup>57</sup> Computación en la Nube. Guatemala, 2012. [en línea] Disponible en <http://todosobrelanube.blogspot.com.co/p/historia.html> [citado el 24 de abril de 2017]

<sup>58</sup> MONROY, C.R., Arias, C.A., GUERRERO, Y.N., El nuevo paradigma de la computación en la nube: el camino hacia la TI visto como una utilidad. *EN* Revista Latinoamericana y del Caribe de Educación en Ingeniería, [en línea], 2013. Disponible en

<https://riunet.upv.es/bitstream/handle/10251/38864/Cloud%20Computing%20y%20Modelo%20de%20Negocio%20para%20pymes%20-%20TFM%20de%20Fernando%20Fons.pdf?sequence=1>, [citado el 15 de abril de 2017], pág. 26

<sup>59</sup> La Fundación del Español Urgente (Fundeu BBVA) señala: “consejero delegado o director general son alternativas adecuadas para traducir la sigla inglesa CEO en relación con el cargo ejecutivo de mayor rango en una empresa o compañía.

identifica a cada dispositivo dentro de una red (IP) lo cual permite maximizar el rendimiento y la disponibilidad de la red<sup>60</sup>..

Según Joe Kava<sup>61</sup>, vicepresidente de operaciones de centro de datos y Niels Provos, ingeniero de seguridad y privacidad de Google, los centros de datos también son diariamente vigilados por guardias de seguridad experimentados que han sido sometidos a rigurosa verificación de antecedentes y entrenamiento:

*“Empleamos una cadena de custodia de extremo a extremo muy estricta para el almacenamiento, desde la cuna a la tumba, desde la primera vez que un HD<sup>62</sup> entra en una máquina hasta que se verifica limpio / borrado o destruido. La seguridad de la información y la seguridad física van de la mano. Los datos son más vulnerables al acceso no autorizado a medida que viajan a través de Internet o dentro de las redes. Por esta razón, la seguridad de los datos en tránsito es una alta prioridad para Google”.*

Igualmente, usa revisiones de seguridad con extensos registros de auditorías, manuales con exámenes de diseño e implementación, con un equipo que incluye expertos en seguridad web, criptografía y seguridad del sistema operativo. Además, ejecuta un programa de recompensas de vulnerabilidad donde pagan a cualquier individuo quien es capaz de descubrir e informar los errores de la infraestructura o aplicaciones. Google ha pagado muchos millones de dólares en recompensas con este programa<sup>63</sup>.

Para la eliminación de datos, Google comienza marcando datos específicos como *"Programado para borrado"* en lugar de eliminar los datos completamente, lo cual permite recuperar las supresiones no intencionales, ya sea por error del cliente o de

---

<sup>60</sup>Google cloud plataform. Google Infraestructura Security Design Overview. [en línea] Disponible en <https://cloud.google.com/security/security-design/> [citado el 25 de abril de 2017]. Pág. 3 y 4.

<sup>61</sup> Google Cloud Platform Blog, Google shares data center security and design best practices, [en línea] marzo 24 de 2016. Disponible en [https://docs.google.com/document/d/17am-dv9UmarT7HQiuqM\\_NfWeyhhKi1sfExP14IsRwOE/edit#](https://docs.google.com/document/d/17am-dv9UmarT7HQiuqM_NfWeyhhKi1sfExP14IsRwOE/edit#) [citado el 20 de abril de 2017]

<sup>62</sup> Es un disco magnético en el que puede almacenar datos.

<sup>63</sup>. Google cloud plataform. Google Infraestructura Security Design Overview. [en línea] Disponible en <https://cloud.google.com/security/security-design/> [citado el 25 de abril de 2017]. Páginas. 7 y 10.

un proceso interno. Empero, los datos se eliminan de acuerdo con las políticas específicas del servicio<sup>64</sup>.

Por otro lado, las identidades de cada usuario se manejan por separado. La infraestructura proporciona un sistema de flujo de trabajo y gestión de estas identidades internas, incluyendo cadenas de aprobación, registro y notificación, en el cual, un ingeniero (primera parte), altamente calificado, puede proponer un cambio a un grupo que otro ingeniero (segunda parte), quien es también un administrador del grupo, debe aprobar. Del mismo modo, además de pedir un nombre de usuario y una contraseña simple, el servicio también desafía inteligentemente a los usuarios para obtener información adicional basada en factores de riesgo, como por ejemplo, les pregunta a través del correo electrónico si han iniciado sesión desde el mismo dispositivo o una ubicación similar, para establecer medidas de seguridad, aunque, los usuarios también tienen la opción de emplear otros factores como contraseñas válidas sólo para una autenticación (OTPs) o claves de seguridad resistentes al phishing<sup>65</sup> al iniciar sesión<sup>66</sup>.

También, Google invierte fuertemente en la seguridad de su infraestructura con los mejores ingenieros dedicados a la seguridad y privacidad, distribuidos en todo Google, incluyendo varias autoridades reconocidas de la industria. El equipo de seguridad de Google monitorea activamente el acceso a los datos e investiga eventos inusuales, ya que cuenta con sofisticadas líneas de procesamiento de datos en dispositivos individuales, señales basadas en la red procedentes de diferentes puntos en la infraestructura que comunican a los Ingenieros avisos de posibles

---

<sup>64</sup> *Ibidem* páginas 1 y 9.

<sup>65</sup> "El término *phishing* es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima". Ver al respecto RIVERO, Marcelo, ¿Qué es el phishing? [en línea]. Disponible en <<https://www.infospware.com/articulos/que-es-el-phishing/>>, [citado el 22 de abril de 2017].

<sup>66</sup> Google cloud plataform. Google Infraestructura Security Design Overview. [en línea] Disponible en <https://cloud.google.com/security/security-design/> [citado el 25 de abril de 2017]. Páginas 5y .9.

incidentes; para así, dar respuesta oportuna en las 24 horas al día, y los 365 días al año<sup>67</sup>.

Así mismo, Google mantiene una amplia seguridad con los empleados, incorporando en sus contratos cláusulas de confidencialidad y a la vez, realiza una actividad de monitoreo para descubrir posibles actividades ilícitas de información privilegiada. Paralelamente, para asegurar que la infraestructura sea operada de manera eficiente, ante el sofisticado *phishing*, utiliza claves de seguridad para las cuentas de cada empleado y hace una gran inversión en el monitoreo de las actividades de los que tienen acceso administrativo a la infraestructura<sup>68</sup>. Éstos empleados de Google operan en los centros de datos y no son terceros contratistas de otras empresas<sup>69</sup>.

**2.2.2 Los bancos:** Es la entidad quien contrata el servicio y determina el objetivo último de los datos,<sup>70</sup> mediante el uso de tecnologías que han transformado la banca global, a través del internet, como un medio de comunicación entre los bancos y los clientes ya sean personas naturales o jurídicas en el que se realizan diferentes operaciones en línea, optimizando mejor los recursos a un menor tiempo y costo<sup>71</sup>-

En un principio, cuando los bancos abrieron sus plataformas, para alinearse con las nuevas tecnologías del mercado no estaban seguros del potencial negocio. Así que, las primeras páginas tenían un diseño complicado, que impedía la navegación rápida, eficiente y que sólo emitía los mensajes publicitarios de las sucursales.

---

<sup>67</sup> *Ibidem*, pág. 11.

<sup>68</sup> *Ibidem*, pág. 10.

<sup>69</sup> Google Cloud Platform Blog, Google shares data center security and design best practices.[en línea] marzo 24 de 2016. Disponible en [https://docs.google.com/document/d/17am-dv9UmarT7HQiuqM\\_NfWeyhhKi1sfExPI4IsRwOE/edit#](https://docs.google.com/document/d/17am-dv9UmarT7HQiuqM_NfWeyhhKi1sfExPI4IsRwOE/edit#) [citado el 20 de abril de 2017]

<sup>70</sup> SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Manual de protección de los datos personales en los servicios de contratación en la nube (cloud computing). [en línea] Disponible en [https://issuu.com/quioscosic/docs/cartilla\\_proteccion\\_datos](https://issuu.com/quioscosic/docs/cartilla_proteccion_datos) [citado el 3 de marzo de 2017].

<sup>71</sup> HERRERA, Juan, JARA, Miguel y JEREZ María. Los bancos y las nuevas tecnologías. Seminario para optar al Título de Ingeniero en Información y Control de Gestión, Santiago: Universidad de Chile Facultad de Ciencias Económicas y Administrativas Escuela de Sistemas de Información y Auditoría. [en línea] marzo de 2005. Disponible en <http://repositorio.uchile.cl/bitstream/handle/2250/111497/Herrera,%20Juan%20S..pdf?sequence=1> [citado el 15 de abril de 2017], pág. 39.

Posteriormente, los bancos empezaron a realizar grandes inversiones en tecnologías y marketing para ofrecer servicios online gratuitos, desde consultas de saldos de cuentas de ahorros, transferencias a otros países, pago de servicios como luz, agua, teléfono, internet, pago de impuestos, información de productos y servicios para la banca personal y empresarial, etc., a los cuales puede accederse desde la casa, la empresa, la universidad o cualquier lugar<sup>72</sup>.

Respecto al habeas data, el negocio bancario al manejar grandes bases de datos, de clientes, cuentas, cotizaciones, transferencias, fondos, está relacionado estrechamente con la información, lo que le hace propicio liderar productos novedosos y la seguridad a toda prueba en un negocio en el que la confianza que le otorga el cliente lo es todo<sup>73</sup>

Por eso, las entidades financieras intentan garantizar a sus clientes la seguridad en las transacciones, por lo general, la mayoría de bancos tienen su personal encargado del mantenimiento de las plataformas, programas específicos para ciertos módulos de consulta o transacciones y dispositivos que brindan mayor seguridad tanto a los clientes como al propio negocio bancario<sup>74</sup>.

Igualmente, los bancos están recurriendo a plataformas de atención al cliente, que integran medios de comunicación con una tecnología informática avanzada, una base de datos actualizada constantemente por los responsables de ventas, operaciones y distribución, crédito y finanzas, mercadeo y servicio al cliente, pues distintos departamentos verifican el crédito, documentan las cobranzas, programan el servicio, ofrecen respaldo técnico, entre otros<sup>75</sup>.

En efecto, las ventajas de estos servicios ofrecidos al consumidor financiero se encuentran en la nube de un proveedor. Sin embargo, respecto a esta investigación, es complejo indicar los bancos que en Colombia específicamente utilizan los

---

<sup>72</sup> *Ibidem*, pág. 41

<sup>73</sup> *Ibidem*, pág. 14.

<sup>74</sup> *Ibidem*, pág. 31

<sup>75</sup> *Ibidem*, pág. 66

servicios de la gran empresa monopolística Google, debido a que su Acuerdo de licencia le permite al cliente declarar públicamente que utiliza sus servicios, si obtiene un permiso por escrito de Google a través del proceso especificado sobre las directrices de marcas, empero, por el contrario Google si puede incluir el nombre o marca del cliente en una lista en línea o en materiales promocionales.

De tal forma, son pocos los bancos que mencionan a Google como proveedor de nube, aunque BBVA si reveló que migró su sistema de correo corporativo a *Google Apps*<sup>76</sup> con el propósito de aumentar la eficiencia, trabajar desde cualquier lugar y entender que: " *la información se puede transformar en conocimiento, y el conocimiento en nuevos productos*"<sup>77</sup>. Una idea que incentiva el desarrollo de la computación bancaria,

**2.2.3 Terceros: El cliente:** La persona que accede a los servicios ofrecidos en la nube por el banco, es el afectado o interesado de los datos que sean objeto del tratamiento<sup>78</sup>.

**Propietarios de los centros de datos:** Google cuenta con algunos servidores en centros de datos de terceros, a los cuales confiere medidas de seguridad para la protección de los datos, en estos lugares también deben operar sistemas de identificación biométrica, cámaras y detectores de metales<sup>79</sup>.

**Empresas dedicadas a migrar los datos:** Según el ingeniero electrónico, Leonardo Jaimes<sup>80</sup>, si las empresas desean cambiarse de proveedor, por ejemplo,

---

<sup>76</sup> "Google Apps es un conjunto de aplicaciones que nos permite organizar de forma sencilla todo nuestro trabajo, y la comunicación entre los distintos trabajadores con diversas herramientas para la gestión del correo electrónico, mensajería instantánea, planificación de reuniones y tareas, generación de documentos", etc. Ver al respecto <https://www.imaginanet.com/blog/google-apps-que-te-ofrece.html>

<sup>77</sup> ZAUZICH, Ivanna. Cloud banking: De qué se trata la banca en la nube y cómo implementarla. 22 de marzo de 2016 [EN](#) Cobiscorp blog. [en línea] Disponible en <<http://blog.cobiscorp.com/banca-en-la-nube-cloud-banking>> [citado el 23 de marzo de 2017].

<sup>78</sup> AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Glosario de términos. [en línea] Disponible en [https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion\\_ficheros/preguntas\\_frecuentes/glosario/index-ides-idphp.php](https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/glosario/index-ides-idphp.php) [citado el 13 de abril de 2017].

<sup>79</sup> Google cloud plataform. Google Infraestructura Security Design Overview. [en línea] Disponible en <https://cloud.google.com/security/security-design/> [citado el 25 de abril de 2017], pág. 3.

<sup>80</sup> JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

de Amazon a Google, éstas mismas descargan la información y la suben, o consiguen una aplicación de terceros, ofrecida por otra empresa que migra toda la información.

**Las centrales de riesgo:** Con la elaboración de una historia crediticia, son las entidades que almacenan, procesan y suministran la información sobre la forma como las personas naturales y jurídicas han cumplido con sus obligaciones en entidades financieras, cooperativas o con almacenes y empresas que venden a crédito<sup>81</sup>.

**Proveedores de internet:** Son las empresas encargadas de suministrar el internet, pues la privacidad y protección de datos no sólo afectan a la computación en nube, sino que, plantean retos en el entorno de este servicio, especialmente, en situaciones transfronterizas e internacionales,<sup>82</sup> dado que, al utilizar un servicio basado en Internet, se presentan varios riesgos como la falta de conexión y la congestión de la red que pueden generar interrupciones, errores o dificultades para el procesamiento de las operaciones<sup>83</sup>. De tal forma, se puede obtener éxito con el *cloud computing* cuando es eficaz la conectividad de red y el ancho de banda para subir y bajar archivos de gran tamaño, guardar videos, imágenes, programas, entre otros datos. Toda vez que, la nube debe estar disponible siempre que se necesite, para acceder a la información, de lo contrario, las consecuencias no son diferentes a un ataque de denegación del servicio<sup>84</sup>.

---

<sup>81</sup> ¿Qué son las centrales de riesgo y para qué sirven[en línea]. Disponible en <http://www.finanzaspersonales.com.co/credito/articulo/que-centrales-riesgo-para-que-sirven/51380> [citado el 25 de abril de 2017]

<sup>82</sup> EUROPA. PARLAMENTO EUROPEO. Dirección general de políticas interiores. Departamento temático, política, economía y científica. Computación en la nube, [en línea] mayo de 2012. Disponible en <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO\\_ET\(2012\)475104\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf)>, [citado el 15 de abril de 2017], pág. 70.

<sup>83</sup> LÓPEZ, María, ALBANESE, Diana y otros. Identificación de riesgos vinculados con el uso de Cloud Computing en la Gestión Organizacional. Aplicación de la Risk Breakdown Structure a Entidades Financieras de la República Argentina. Rio Janeiro: ANPAD [en línea] 4 de septiembre de 2011. Disponible en <<http://www.anpad.org.br/admin/pdf/ADI2220.pdf>>, [citado el 12 de abril de 2017]. 13.

<sup>84</sup> TORO, Cristian, MURCIA, Johan y HERNÁNDEZ, Marien. Guía de auditoría para evaluar el aseguramiento de la disponibilidad de la información en un ambiente cloud computing IAAS, bajo la norma ISO 27001 de 2013. Trabajo de grado de especialistas en auditoría de sistemas de información, Bogotá: Universidad Católica de Colombia, Facultad de Ingeniería, Especialización en Auditoría de Sistemas de Información, [en línea], 2014. Disponible en

Aunque, según el ingeniero electrónico, Leonardo Jaimes<sup>85</sup> garantizar la conexión no es en un 100%, pues en unos minutos se deben hacer cambios en el sistema, y actualizar parámetros, pero estos tiempos son tan cortos que no tienen alguna incidencia en el usuario final.

## 2.2 TIPO DE CONTRATO.

De acuerdo con el artículo 1495 del Código Civil Colombiano, el contrato “*es un acto por el cual una parte se obliga para con otra a dar, hacer o no hacer alguna cosa. Cada parte puede ser de una o de muchas personas*<sup>86</sup>” Este concepto se ajusta a los contratos informáticos, dando lugar a una rica tipología comercial, en la que pueden distinguirse contratos de compraventa, “llave en mano”, alquiler, *leasing*, mantenimiento y servicio<sup>87</sup>.

En efecto, por las obligaciones que surgen para las partes (disponibilidad de la información, seguridad de los datos, *back up*, entre otras), permite que se les nombre como complejos y por el hecho de que involucran al fabricante, el adquiriente o usuario de la informática, que, a su vez, puede transferir los servicios a terceros. Además, es un contrato en el que no existe un equilibrio entre las posiciones, porque los constructores de *hardware* y *software*<sup>88</sup> poseen un conocimiento técnico de los aspectos básicos del contrato, más que el usuario<sup>89</sup>.

---

<<http://repository.ucatolica.edu.co/bitstream/10983/1751/1/TRABAJO%20GRADO%20CLOUD%20COMPUTING%20IAAS.pdf>>, [citado el 11 de abril de 2017], pág. 52.

<sup>85</sup> JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

<sup>86</sup> COLOMBIA. Ley 57 de 1887. Código Civil. [en línea] Disponible en <<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=39535>>, [citado el 24 de abril de 2017], artículo 1495.

<sup>87</sup> PÉREZ, Manuel. Manual de Informática y Derecho. Barcelona: Ariel, 1996. ISBN 84-344-1598-4, páginas 113 y 114.

<sup>88</sup> Es el conjunto de toda la información que utilizan las computadoras para trabajar, puede dividirse en dos grupos fundamentales de entidades: los programas o conjuntos de instrucciones y los datos. Ver al respecto Conceptos de hardware y software, [en línea] <<http://engendros.galeon.com/U1T6.htm>> [citado el 22 de abril de 2017].

<sup>89</sup> PÉREZ, Manuel. Manual de Informática y Derecho. Barcelona: Ariel, 1996. ISBN 84-344-1598-4, páginas 113 y 114.

En Colombia, no existe claridad sobre el tipo de contrato que se celebra cuando un proveedor almacena información en la nube de un banco, razón por la cual Gonzalo Moreno<sup>90</sup> argumenta que podría ser un contrato de arrendamiento<sup>91</sup>, dado que se arrienda un espacio virtual o un *data center* real y tangible que es donde finalmente residen los datos, con las respectivas obligaciones de conservar 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 ésta o manipularla. Así mismo, indica que podría ser un contrato de suministro<sup>92</sup>, en el cual el proveedor se obliga a cambio de una contraprestación a dar en forma continuada su *software*, plataforma e infraestructura como servicio.

Mientras que, la firma de abogados y consultores expertos en las tecnologías de la información, Velasco & Calle D'Aleman considera que la relación jurídica, entre el adquirente del servicio y el proveedor de nube es un contrato de adhesión<sup>93</sup>, en el cual, el proveedor no permite negociar los términos de las cláusulas incorporadas<sup>94</sup>.

Para la Superintendencia Financiera en el Concepto 2015019296-001, en Colombia no hay una norma específica que regule la contratación por parte de las instituciones financieras de servicios en la nube<sup>95</sup>, pero señala que la Ley 1341 de 2009 consagra la contratación de personas naturales o jurídicas, bajo la modalidad de *outsourcing*

---

<sup>90</sup> MORENO, GONZALO. Jurisdicción aplicable en materia de datos personales en los contratos de cloud computing: análisis bajo la legislación colombiana. Universidad de los Andes, Facultad de Derecho. Revista de Derecho, Comunicaciones y Nuevas Tecnologías. N°9 junio de 2013. ISSN 1909-7786, páginas 12 y 14.

<sup>91</sup>El artículo 1973 del Código Civil colombiano consagra que el arrendamiento “es un contrato en que las dos partes se obligan recíprocamente, la una a conceder el goce de una cosa, o a ejecutar una obra o prestar un servicio, y la otra a pagar por este goce, obra o servicio un precio determinado”.

<sup>92</sup> Según el artículo 968 del Código de Comercio “*El suministro es 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*”.

<sup>93</sup> “*La doctrina ha definido el contrato de adhesión como aquel acuerdo de voluntades por medio del cual uno de los contratantes, denominado predisponente, impone al otro, llamado adherente, el contenido del contrato sin ninguna posibilidad de discutirlo ni de modificarlo, contando únicamente con la facultad de decidir libremente si contrata o no bajo el clausulado ofrecido*”. Ver al respecto: POSADA, Camilo. Las cláusulas abusivas en los contratos de adhesión en el derecho colombiano EN Revista de la Universidad Externado. [en línea]. Disponible en <<http://revistas.uexternado.edu.co/index.php/derpri/article/view/4328/5081>> [citado el 24 de abril de 2017]

<sup>94</sup> VELASCO & CALLE D'ALEMAN. Contratación en la Nube, Privacidad y Recomendaciones de la Autoridad colombiana. Parte 2, agosto 10 de 2006. [en línea]. Disponible en <<http://velascocalle.co/blog/contratacion-en-la-nube-privacidad-y-recomendaciones-de-la-autoridad-colombiana-parte-2/>> [citado el 1 de abril de 2017]

<sup>95</sup> COLOMBIA, SUPERINTENDENCIA FINANCIERA. Concepto 2015019296-001, contratación en la nube, contratación de servicios de terceros (16 de abril de 2015).

o tercerización<sup>96</sup> por parte de las entidades financieras para la atención parcial o total de los servicios<sup>97</sup>.

Igualmente, argumenta que según la Circular Básica Jurídica CE 029 de 2014<sup>98</sup>. las entidades vigiladas deben:

*(i) definir los criterios y procedimientos a partir de los cuales se seleccionarán los terceros y los servicios que serán atendidos; (ii) exigir que los terceros contratados dispongan de planes de contingencia y continuidad debidamente documentados; (iii) establecer procedimientos que permitan identificar físicamente, de manera inequívoca, a los funcionarios de los terceros contratados; e (iv) implementar mecanismos de cifrado fuerte para el envío y recepción de información confidencial con los terceros contratados.*

*Así mismo, se requiere que en los contratos que se celebren con terceros, se incluya lo siguiente:*

*Niveles de servicio y operación, acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas, propiedad de la información, restricciones sobre el software empleados, normas de seguridad informática y física a ser aplicadas, procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de dispositivos o información y procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.*

Por último, resalta que, la posibilidad de las entidades vigiladas por la Superintendencia para contratar con terceros, no las exime de dar cumplimiento a las exigencias de seguridad en el manejo de la información, disponibilidad de la misma y protección de datos, que les imponen las normas<sup>99</sup>.

---

<sup>96</sup> Es un contrato de prestación de servicios, según el artículo 1495 del Código Civil que dispone que, es un acto por el cual una parte se obliga para con otra a dar, hacer o no hacer alguna cosa.

<sup>97</sup> COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1341 de 2009, (julio 30 de 2009), por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. Citado por COLOMBIA, SUPERINTENDENCIA FINANCIERA. Concepto 2015019296-001, contratación en la nube, contratación de servicios de terceros (16 de abril de 2015).

<sup>98</sup> COLOMBIA, SUPERINTENDENCIA FINANCIERA. Circular Básica Jurídica, Circular Externa 029 DE 2014, citado por COLOMBIA, SUPERINTENDENCIA FINANCIERA. Concepto 2015019296-001, contratación en la nube, contratación de servicios de terceros (16 de abril de 2015).

<sup>99</sup> COLOMBIA, SUPERINTENDENCIA FINANCIERA. Concepto 2015019296-001, contratación en la nube, contratación de servicios de terceros (16 de abril de 2015).

De este concepto, se entiende que los aspectos técnicos en la implementación medidas de seguridad, son difíciles de cumplir directamente por las entidades financieras, pues no hacen parte de su especialidad, razón por la cual, es necesario contratar a otros individuos expertos en estos temas.

## 2.3 MODELOS DE DESPLIEGUE DE LA NUBE.

Edwin Jimen<sup>100</sup> en el trabajo de grado “*Modelo de Tarificación Software como Servicio Saas*”, define los siguientes modelos del funcionamiento de la nube:

**Cloud Privado:** Modelo en el que la infraestructura es gestionada únicamente por una organización, (gestiona el mismo banco). Así, la administración de aplicaciones, centros de datos y servicios puede estar a cargo de los ingenieros de la misma empresa o de un tercero y la infraestructura puede estar dentro o fuera de ésta. En tal sentido, la organización usuaria debe tener control sobre la infraestructura, *software* y aplicaciones que conforman su nube. Verbigracia, cualquier servicio de nube propia de la organización o contratando a un proveedor (también puede ser Google) pero cuyos recursos sean exclusivos para dicha entidad financiera.

**Cloud Público:** Modelo de nube en el que la infraestructura y los recursos lógicos que forman parte del entorno se encuentran disponibles para el público en general o varios usuarios. Esta nube es propiedad de un proveedor que gestiona la infraestructura y los servicios ofrecidos, el cual adquiere ganancias indirectas por su uso externo<sup>101</sup>, ejemplo *Google Drive*<sup>102</sup>.

---

<sup>100</sup> JIMENEZ, Edwin. Modelo de Tarificación Software como Servicio Saas. Trabajo de grado de Magíster en ciencias de la información y las comunicaciones. Bogotá: Universidad Distrital Francisco José de Caldas. Facultad de Ingeniería. Maestría en ciencias de la información y las Comunicaciones, [en línea] 2015. Disponible en <<http://repository.udistrital.edu.co/bitstream/11349/2765/1/JimenezGarzonEdwinAlfonso2015.pdf>>, [citado el 24 de abril de 2017], pág. 29.

<sup>101</sup> *Ibidem*, pág. 29.

<sup>102</sup> *Google Drive* es un lugar seguro para todos tus archivos y te permite tenerlos a mano en cualquier *Smartphone*, *Tablet* u ordenador. Los archivos que guardes en Drive (vídeos, fotos, documentos, etc.) tienen una copia de seguridad para que nunca los pierdas. Después de guardarlos, puedes invitar a otras personas a ver, editar o comentar cualquiera de tus archivos o carpetas. Ver al respecto: <<https://play.google.com/store/apps/details?id=com.google.android.apps.docs&hl=es>>.

**Cloud Comunitaria:** Modelo donde la infraestructura es compartida por varias organizaciones y su principal objetivo es soportar a una comunidad específica que posea un conjunto de características similares: misión, requisitos de seguridad o de cumplimiento normativo, etc. Al igual que la nube privada, puede ser gestionada por las organizaciones o bien por un tercero y la infraestructura puede estar en las instalaciones propias o fuera de estas<sup>103</sup>, un ejemplo es una nube para los bancos de Colombia en general.

**Cloud Híbrida:** Modelo donde se combinan dos o más tipos de nubes: pública, privada o comunitaria, que se mantienen como entidades separadas pero que están unidas por tecnologías estandarizadas o propietarias, que permiten la portabilidad de datos y aplicaciones<sup>104</sup>, por ejemplo, Bluemix.

## 2.4 LOS SERVICIOS.

Para Leonardo Jaimes <sup>105</sup>, *“todo lo que se encuentra en internet es nube, todo lo que no esté en el computador físico”*. La nube es un conjunto de servicios que ofrecen empresas privadas o públicas a otras sociedades que requieran implementar una infraestructura de sistemas de redes o manejo de la información en todo momento, en todo lugar, disponible las 24 horas y hasta los fines de semana.

---

<sup>103</sup> JIMENEZ, Edwin. Modelo de Tarificación Software como Servicio Saas. Trabajo de grado de Magíster en ciencias de la información y las comunicaciones. Bogotá: Universidad Distrital Francisco José de Caldas. Facultad de Ingeniería. Maestría en ciencias de la información y las Comunicaciones, [en línea] 2015. Disponible en <<http://repository.udistrital.edu.co/bitstream/11349/2765/1/JimenezGarzonEdwinAlfonso2015.pdf>>, [citado el 24 de abril de 2017], pág. 30.

<sup>104</sup> *Ibidem*.

<sup>105</sup> JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

**2.4.1 Los servicios de Google con el banco:** Según la Agencia Europea de Seguridad de las Redes y de la información<sup>106</sup>, los servicios suministrados son recursos informáticos y la nube ofrece principalmente tres servicios, conocidos como:

**Software como servicio (SaaS):** El proveedor del servicio proporciona aplicaciones y *software* a cambio de un pago por el servicio. Así, el usuario paga por los servicios que va a utilizar, por ejemplo: correo electrónico, uso de aplicaciones, core bancario, *Google Docs*<sup>107</sup>, etc.

**Plataforma como servicio (PaaS):** Es el uso de una plataforma tecnológica en internet, que incluye *hardware*, sistema operativo y *middleware*<sup>108</sup>, entre otros, sin necesidad de comprar y administrar su propia plataforma, sino pagando el servicio prestado. Por ejemplo, *Google App Engine*<sup>109</sup>.

**Infraestructura como servicio (IaaS):** Consistente en el acceso a servidores, subsistemas de almacenamiento de contenidos o de archivos digitales y redes<sup>110</sup>. El almacenamiento corresponde a guardar información en un lugar virtual, generalmente, los servicios ofrecidos por los proveedores en nube consisten en correo electrónico, mensajería, gestión de proyectos, gestión de nóminas, contabilidad, finanzas, facturación y gestión de las relaciones con los clientes,

---

<sup>106</sup> AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA). Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información, [e línea] Disponible en <<https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish>>, [citado el 20 de abril de 2017], pág. 112.

<sup>107</sup> *Google Docs* es un potente procesador de texto y hoja de cálculo, todo en línea, que permite crear nuevos documentos, editar o compartirlos en la red con otros usuarios. Ver al respecto: <[http://alerce.pntic.mec.es/bmarco1/pagina\\_web/googledocs.htm](http://alerce.pntic.mec.es/bmarco1/pagina_web/googledocs.htm)>.

<sup>108</sup> *Middleware* es la lógica de intercambio de información entre aplicaciones, es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, o paquetes de programas, redes, hardware y/o sistemas operativos. Ver al respecto <https://platzi.com/blog/middlewares-laravel/>.

<sup>109</sup> *Google App Engine* permite publicar aplicaciones web en línea sin necesidad de preocuparse por la parte de la infraestructura. Ver al respecto <https://platzi.com/blog/google-app-engine/>

<sup>110</sup> RENGIFO GARCÍA, Ernesto. Computación en la nube. Revista la propiedad inmaterial, ISSN 1657- 1959, n. 17, [en línea] 2013. Disponible en <<http://dialnet.unirioja.es/servlet/articulo?codigo=4775097>>, [citado el 15 de abril de 2017] pág. 224.

gestión de ventas, desarrollo de aplicaciones personalizadas y procesamiento de datos para los bancos<sup>111</sup>.

## **2.4.2 Servicios del proveedor con el banco y la entidad financiera con los usuarios.**

**2.4.2.1 Core bancario:** El core bancario está compuesto por un conjunto de funciones, como: la administración de usuarios, roles, perfiles, claves de seguridad, horarios de trabajo de usuarios, control de las transacciones, calendario de días importantes, hábiles locales y nacionales, niveles de acceso, montos máximos por moneda para cada transacción, creación de menús específicos de rol y niveles de aprobación; que se emplean con mecanismos de autenticación, entre los cuales se encuentra la tecnología biométrica<sup>112</sup>.

También, ofrece la administración de los clientes de la Institución Financiera, pues el cliente tiene un identificador a través del cual se registra y administra información del cliente como: datos personales, estado de situación financiera, actividad económica, domicilios y referencias familiares y laborales que permiten conocer inmediatamente la posición actual del cliente y su historia en el banco<sup>113</sup>.

Igualmente, el core bancario administra el proceso de concesión de créditos, desde el ingreso de la solicitud, control de documentos requeridos, verificación de datos, liquidaciones, manejo de varios tipos de créditos o préstamos y la generación de información para control del riesgo<sup>114</sup>.

---

<sup>111</sup> AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA). Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información, [en línea] Disponible en <<https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish>>, [citado el 20 de abril de 2017], pág. 112.

<sup>112</sup> GONZÁLEZ, Hugo. Implementación y uso de un *core bancario* para banca retail en la tecnología *cloud computing*. Trabajo de grado de Magister en Gerencia de Tecnología de la información, Quito: Pontificia Universidad Católica de Ecuador. Maestría en Gerencia de Tecnología de la información. [en línea], mayo de 2015 Disponible en <http://repositorio.puce.edu.ec/bitstream/handle/22000/8539/CASO%20DE%20ESTUDIO%20-%20Hugo%20Gonzalez.pdf?sequence=1>, [citado el 12 de abril de 2017] Pág. 10.

<sup>113</sup> *Ibidem*, pág. 11.

<sup>114</sup> *ibidem*, pág. 11

También, realiza un manejo completo de cuentas corrientes y cuentas de ahorro<sup>115</sup>, administra los tipos de captaciones como depósitos a plazo y certificados de depósito negociables, certificados de ahorros, pagarés, y se verifican las operaciones como pagos de intereses al vencimiento o periódicos con cualquier frecuencia, cesiones, renovaciones automáticas o manuales con incrementos o disminuciones, bloqueos, etc<sup>116</sup>.

Además, mantiene un control de documentos, pólizas de seguro, renovación y sustitución de garantías, control de avalúos e inspecciones<sup>117</sup> y la administración de perfiles o matrices contables que permiten la contabilización de las transacciones monetarias en línea de acuerdo a los requerimientos del organismo de control correspondiente<sup>118</sup>, como la Superintendencia Financiera de Colombia.

En las entidades bancarias también se maneja los reportes negativos del control, generados en los procesos en línea, para mantener una información histórica. De igual modo, con la implementación de la tecnología en los bancos se perfeccionan los referentes a la detección y prevención de lavado de dinero, manejo de perfiles de comportamiento de clientes, factores de riesgo y la detección de movimientos o transacciones inusuales<sup>119</sup>.

Finalmente, para facilitar el manejo de la solución a los usuarios, los bancos poseen manuales en línea, una ayuda rápida y eficiente, que reduce el requerimiento de personal especializado para soporte a usuarios<sup>120</sup>.

---

<sup>115</sup> *Ibidem*, páginas 11 y 12.

<sup>116</sup> *Ibidem*, pág. 12.

<sup>117</sup> *Ibidem*, pág. 12.

<sup>118</sup> *Ibidem*, pág. 12 y 13.

<sup>119</sup> *Ibidem*, Pág. 16

<sup>120</sup> *Ibidem*, pág. 16

En consecuencia, toda la información de los clientes, transacciones, servicios y contable se administra y gestiona a través de motores de base de datos y esquemas avanzados de almacenamiento eficiente, que les permite a las instituciones financieras adelantarse a las necesidades del mercado, las expectativas de los clientes, la tecnología y el cumplimiento de la ley<sup>121</sup>.

**2.4.2.2 Banca móvil:** La Banca Móvil es un canal electrónico en el cual “el dispositivo móvil es utilizado para realizar operaciones y su número de línea es asociado al servicio”, Es decir, son servicios a los que el consumidor financiero accede utilizando un dispositivo móvil, pero a través de un navegador web y sin que haya asociación del servicio a la línea móvil<sup>122</sup>.

La banca móvil ofrece el punto de contacto más eficiente para los clientes, y los costes de transacción más bajos para los bancos, ofreciendo un acceso en cualquier momento y lugar a productos y servicios financieros<sup>123</sup>.

En la legislación colombiana existe cierta libertad para los establecimientos de crédito de ofrecer canales de distribución de sus servicios financieros, por lo que se han desarrollado soluciones tecnológicas para que el consumidor administre sus productos y utilice los servicios ofrecidos por las entidades a través de plataformas que hacen más accesibles los trámites y operaciones del sistema financiero. Pero estos canales electrónicos deben cumplir con los estándares de seguridad para el manejo de la información<sup>124</sup>.

---

<sup>121</sup> ibidem pág. 17

<sup>122</sup> COLOMBIA, SUPERINTENDENCIA FINANCIERA. Concepto 2016070922-001, banca móvil, banca por internet, normatividad (11 de agosto de 2016).

<sup>123</sup> BBVA. Innovation Edge. Banca Móvil. Una nueva experiencia en la era post PC, [en línea] abril de 2012. Disponible en <[http://www.centrodeinnovacionbbva.com/sites/default/files/mobilebanking\\_spanish.pdf](http://www.centrodeinnovacionbbva.com/sites/default/files/mobilebanking_spanish.pdf)>, [citado el 16 de abril de 2017], pág. 10 y 16

<sup>124</sup> COLOMBIA, SUPERINTENDENCIA FINANCIERA. Concepto 2016070922-001, banca móvil, banca por internet, normatividad (11 de agosto de 2016).

Por lo tanto, las entidades financieras ofrecen a sus clientes los servicios que tradicionalmente se encuentran dentro de su portafolio, como consultas de saldo, transferencias y pagos, pero adaptados específicamente a una plataforma electrónica, para ser utilizadas a través del teléfono móvil celular. Sin embargo, por cuestiones tecnológicas u operativas, ejemplo para la protección de la información, estas entidades presentan algunas restricciones relacionadas con el funcionamiento de los mismos<sup>125</sup>.

**2.4.2. 3 Cuentas electrónica:** Es un sistema de información en línea que permite a los clientes realizar transacciones y acceder a la información a través de un computador personal o celular, desde cualquier parte del mundo y a cualquier hora. Este canal facilita la realización de operaciones bancarias con mayor agilidad y, el consecuente, ahorro de tiempo<sup>126</sup>.

**2.4.2.4 Intranet:** Es una red de ordenadores privados que utiliza la tecnología de internet para compartir sistemas de información y de operaciones, la cual está desplegada totalmente en la nube y que funciona cuando desde un sólo programa: el navegador, se pueden consultar informaciones para gestionar todos los documentos que el banco va produciendo (textos, correo electrónico, hojas de cálculo, bases de datos, etc.). Por consiguiente, es una herramienta orientadora y facilitadora de la información para los empleados, que mejora la comunicación vertical de la entidad y la publicación de la documentación corporativa<sup>127</sup>.

---

<sup>125</sup> COLOMBIA, SUPERINTENDENCIA FINANCIERA. Concepto 2016070922-001, banca móvil, banca por internet, normatividad (11 de agosto de 2016).

<sup>126</sup> Banca electrónica [en línea]. Disponible en <https://www.pichincha.com/portal/Canales-de-atencion/Banca-Electronica/Banca-Electronica>. [Citado el 23 de abril de 2017].

<sup>127</sup> LARA, Pablo y MANIEGA, David. Conocimiento en la nube: evolución de las intranets. El profesional de la información, [en línea], marzo-abril 2011, v. 20, n. 2, Disponible en <<http://www.elprofesionaldelainformacion.com/contenidos/2011/marzo/07.pdf>>, [citado el 14 de abril de 2017] páginas 176-177.

## 2.5 CLÁUSULAS CONTRACTUALES.

Las cláusulas establecidas por los grandes proveedores de nube, condicionan el comportamiento de las partes en la ejecución, estableciéndose de manera específica los usos permitidos o aceptables sobre la plataforma informática puesta a disposición del cliente.

Unos ejemplos de este tipo de cláusulas son los siguientes:

- *Usted acepta ser el único responsable de los contenidos de sus transmisiones a través de los servicios.*
- *Usted acepta no utilizar los servicios para fines ilegales o para la transmisión de material ilegal, difamatorio, calumnioso, invasivo de la privacidad, abusivo, amenazante, perjudicial, vulgar, pornográfico, obsceno, o que sea objetable, ofenda sentimientos religiosos, promueva el racismo, que contenga virus, o que infrinja o pueda infringir la propiedad intelectual u otros derechos de terceros.*
- *Usted se compromete a no utilizar los servicios para la transmisión de “correo basura”, “spam”, “cartas en cadena”, “phishing” o la distribución en masa de correo electrónico no solicitado. Nos reservamos el derecho de suspender el acceso a los servicios si hay motivos razonables para creer que ha utilizado los servicios para cualquier actividad ilegal o no autorizada<sup>128</sup>.*

También frente al control de datos existen cláusulas que sólo disponen:

- *El cliente es el único responsable de sus aplicaciones, proyectos y datos de clientes y de asegurarse de que sus aplicaciones, proyectos y datos de los clientes cumplir con la política de uso aceptable.*

---

<sup>128</sup> RENGIFO GARCÍA, Ernesto. Computación en la nube. Revista la propiedad inmaterial, ISSN 1657- 1959, n. 17, [en línea] 2013. Disponible en <http://dialnet.unirioja.es/servlet/articulo?codigo=4775097>, [citado el 15 de abril de 2017], pág. 236.

- El proveedor no es responsable por la eliminación de o falta de almacenamiento de datos de clientes y otras comunicaciones mantenidas o transmitida a través uso de los servicios. el cliente es el único responsable de fijación y copia de seguridad de sus datos de la aplicación, proyecto y cliente<sup>129</sup>.

Desde estas disposiciones, se colige que las cláusulas establecidas por el proveedor son abusivas o vejatorias, toda vez que, generan un desequilibrio injustificado que vulnera los intereses del consumidor, el principio de la buena fe y la confianza que la parte débil (el banco) ha depositado, por el propósito de obtener ventajas adicionales<sup>130</sup>.

**2.5.1 Ausencia de cláusula arbitral:** En Colombia, La Ley 1563 de 2012 define el arbitraje como un mecanismo alternativo de solución de conflictos mediante el cual las partes a través del pacto arbitral: una cláusula compromisoria o un compromiso, voluntariamente deciden renunciar a la justicia ordinaria para dirimir una controversia ante la justicia arbitral, pudiendo ser el laudo o decisión dentro del proceso en derecho, en equidad o técnico<sup>131</sup>.

Sin embargo, en los contratos de almacenamiento de nube bancaria, o en documento por separado no se evidencia la cláusula compromisoria<sup>132</sup>, infiriéndose que, ante cualquier controversia, si no realizan el compromiso de acudir al Tribunal arbitral, recurrirán a la jurisdicción ordinaria.

---

<sup>129</sup> Acuerdo de licencia de Google Cloud Platform, (marzo 7 de 2017) Disponible en <https://cloud.google.com/terms/>.

<sup>130</sup> POSADA, Camilo. Las cláusulas abusivas en los contratos de adhesión en el derecho colombiano EN Revista de la Universidad Externado. [en línea]. Disponible en <http://revistas.uexternado.edu.co/index.php/derpri/article/view/4328/5081> [citado el 24 de abril de 2017].

<sup>131</sup> COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1563 de 2012 (julio 12 de 2012) Por medio de la cual se expide el Estatuto de Arbitraje Nacional e Internacional y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2012. no.48. 489..

<sup>132</sup> *Artículo 4°. Cláusula compromisoria. La cláusula compromisoria, podrá formar parte de un contrato o constar en documento separado inequívocamente referido a él.*

*La cláusula compromisoria que se pacte en documento separado del contrato, para producir efectos jurídicos deberá expresar el nombre de las partes e indicar en forma precisa el contrato a que se refiere.*

Ver al respecto: COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1563 de 2012” Por medio de la cual se expide el Estatuto de Arbitraje Nacional e Internacional y se dictan otras disposiciones”. Diario Oficial. Bogotá, D.C., 2012, art 4.

## 2.6 LA RESPONSABILIDAD

Según David López<sup>133</sup> ante el daño que se derive de la intromisión en el derecho a la protección de datos, por la prestación de servicios tecnológicos en la nube, el afectado podrá determinar la exigencia de responsabilidad civil contractual, que supone la exigencia de una indemnización como consecuencia de los perjuicios generados por la violación del derecho de habeas data.

**2.6.1 La responsabilidad de Google como proveedor:** Para Gonzalo Moreno<sup>134</sup> la responsabilidad del proveedor es de velar porque la información sea accesible en el momento que se necesite. Además, debe garantizar la integridad de la información del contratante. Así que, los perjuicios que se pueden causar por el deterioro de la información, pérdida o filtración serán responsabilidad del prestador del servicio, ya que es quien debe velar por la custodia y por la existencia de un *back up* o respaldo de la información almacenada en caso de un ataque o mal funcionamiento.

Los abogados y consultores Velasco Calle D'Aleman<sup>135</sup> indican que, a la luz de las normas colombianas relacionadas con la transmisión de datos personales, el proveedor de servicios de nube, al tratarse de un encargado más, debe cumplir con todas las obligaciones descritas en el artículo 18 de la Ley 1581 de 2012, que disponen garantizar en todo tiempo, el pleno y efectivo ejercicio del derecho a la información, conservar los datos bajo medidas de seguridad, actualizar, rectificar o suprimir constantemente los datos, tramitar los reclamos de los titulares de la información, abstenerse de circular información que esté siendo controvertida y

---

<sup>133</sup> LÓPEZ, David. La "Computación en la nube o "cloud computing" examinada desde el ordenamiento jurídico español. Revista de Derecho de la Universidad Católica de Valparaíso. N° 40 agosto de 2013 ISSN 0718-685. [en línea]. Disponible en [http://www.scielo.cl/scielo.php?script=sci\\_arttext&pid=S0718-6851201300010002](http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-6851201300010002), [citado el 20 de abril de 2017].

<sup>134</sup> MORENO, GONZALO. Jurisdicción aplicable en materia de datos personales en los contratos de cloud computing: análisis bajo la legislación colombiana. Universidad de los Andes, Facultad de Derecho. EN Revista de Derecho, Comunicaciones y Nuevas Tecnologías. N°9 junio de 2013. ISSN 1909-7786, páginas 14 y 15

<sup>135</sup> VELASCO & CALLE D'ALEMAN. Contratación en la Nube, Privacidad y Recomendaciones de la Autoridad colombiana. Parte 2, agosto 10 de 2006. [en línea]. Disponible en <http://velascocalle.co/blog/contratacion-en-la-nube-privacidad-y-recomendaciones-de-la-autoridad-colombiana-parte-2/>[citado el 1 de abril de 2017]

avisar a la Superintendencia de Industria y Comercio cuando existen riesgos en la administración de la información<sup>136</sup>.

**2.6.2 La responsabilidad del banco:** Para Nelson Remolina Angarita “aunque los datos estén en la nube, la responsabilidad se asume en la tierra, por el eventual tratamiento indebido de datos personales. Esta recaerá, por lo menos, en cabeza de la organización que decidió acudir a los servicios de cloud”<sup>137</sup>.

De tal forma, el banco no se exime de responsabilidad frente al cumplimiento de las disposiciones colombianas en la materia, por la imposibilidad de negociar las condiciones del contrato de adhesión por parte del responsable del tratamiento; por el contrario, en el caso de la celebración del contrato de transmisión internacional de datos sin las garantías legales colombianas, tendría que responder y solucionar conflictos por el acto de negligencia de los administradores de la entidad<sup>138</sup>.

Para la Superintendencia de Industria y Comercio el cliente, en este caso el banco es el responsable del tratamiento de los datos personales y de tal forma debe cumplir con las obligaciones que le impera la ley, no se puede exonerar de éstas por el hecho de contratar a un proveedor, por tal razón debe obrar de manera diligente para salvaguardar la información de los titulares de la información: el consumidor financiero<sup>139</sup>.

La Superintendencia Financiera ha indicado que, el artículo 1398 del Código de Comercio prefigura la responsabilidad contractual de la entidad financiera “*por el*

---

<sup>136</sup> COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 de 2012 (octubre 17 de 2012) por la cual se dictan disposiciones generales para la protección de datos personales, Diario Oficial. Bogotá, D.C., 2012, art 18

<sup>137</sup> REMOLINA, Nelson, ‘Cloud computing’ y protección de datos personales: aunque la información esté en la nube, la responsabilidad se asume en la tierra EN Periódico Ámbito Jurídico [en línea] 20 de septiembre de 2011. Disponible en <[www.ambitojuridico.com/BancoConocimiento/Educacion-y-Cultura/noti-110920-12-cloud-computing-y-proteccion-de-datos-personales-aunque-la-informacion-este-en](http://www.ambitojuridico.com/BancoConocimiento/Educacion-y-Cultura/noti-110920-12-cloud-computing-y-proteccion-de-datos-personales-aunque-la-informacion-este-en)> [citado el 14 de abril de 2017].

<sup>138</sup> VELASCO & CALLE D’ALEMAN. Contratación en la Nube, Privacidad y Recomendaciones de la Autoridad colombiana. Parte 2, agosto 10 de 2006. [en línea]. Disponible en <http://velascocalle.co/blog/contratacion-en-la-nube-privacidad-y-recomendaciones-de-la-autoridad-colombiana-parte-2>[citado el 1 de abril de 2017].

<sup>139</sup> SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Manual de protección de los datos personales en los servicios de contratación en la nube (cloud computing). [en línea] Disponible en [https://issuu.com/quioscosic/docs/cartilla\\_proteccion\\_datos](https://issuu.com/quioscosic/docs/cartilla_proteccion_datos) [citado el 3 de marzo de 2017].

*reembolso de sumas depositadas que haga a persona distinta del titular de su cuenta o su mandatario*". Por lo tanto, el banco cumple la obligación de que la entrega de las sumas depositadas se realice al titular de la cuenta, su mandatario o a la persona que este designe y así, el desembolso configura un auténtico pago; en caso contrario, el incumplimiento del designio negocial compromete la responsabilidad del establecimiento depositario, el banco; toda vez que, para la prestación adecuada y segura de los servicios ofrecidos por las entidades bancarias, se deben adoptar medidas que nutran el contenido obligacional propio del contrato, identificando los hábitos, patrones, prácticas y costumbres en el uso de los productos por parte del consumidor, insumo con el cual ha de elaborarse un control que permita la confirmación oportuna de las operaciones monetarias que no correspondan a sus hábitos<sup>140</sup>.

Igualmente, para efectos de establecer el régimen de responsabilidad que le resulta aplicable a los bancos, la Superintendencia Financiera consagra que debe hacerse referencia al artículo 335 de la Constitución Política, el cual califica la actividad financiera como de "interés público", toda vez que maneja, aprovecha e invierte recursos captados del público y por ello, requiere de previa autorización del Estado para su ejercicio. Por ello, se exige precisamente de las entidades que la ejercen, mayor diligencia y profesionalismo en el desarrollo de la misma<sup>141</sup>.

En el mismo sentido, la Corte Suprema de Justicia en la Sala de Casación Civil ha determinado que las instituciones bancarias, están sujetas a un especial régimen de responsabilidad civil frente a los daños que puedan sufrir los clientes o usuarios de sus servicios, por lo que surgen a su cargo especiales deberes de diligencia. Así entonces, el ejercicio de la actividad bancaria conlleva implícitamente que la entidad financiera cumpla con los deberes especiales que le son exigibles y asuma los

---

<sup>140</sup>COLOMBIA. Decreto 410 de 1971, (marzo 27 de 1971), por medio del cual se expide el Código de Comercio. Disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=41102>, artículo 13 98, citado por COLOMBIA, SUPERINTENDENCIA FINANCIERA. Expediente 2013 -0211. No. 2013041561(noviembre 20 de 2013)

<sup>141</sup> COLOMBIA, CONSTITUCIÓN POLÍTICA DE COLOMBIA, artículo 335, citado por COLOMBIA, SUPERINTENDENCIA FINANCIERA. Expediente 2013 -0063. No. 2013015100 (julio 31 de 2013).

riesgos inherentes de los diferentes canales de internet, cajero automático, entre otros, que pone a disposición de sus clientes para el manejo de los productos y servicios ofrecidos.<sup>142</sup>.

**2.6.3 La responsabilidad del usuario financiero:** Empero, Edwin Jiménez<sup>143</sup>, indica que al final el responsable en caso de infracción es el propietario de la información, razón por la cual, los proveedores de *Cloud Computing* deberán estar abiertos a cualquier tipo de auditoría externa y cumplir las medidas que sean necesarias para garantizar el cumplimiento de la ley la seguridad de sus clientes.

Según Leonardo Jaimes,<sup>144</sup> si el usuario no aplica niveles de seguridad: contraseñas seguras, diferentes para cada cuenta, autenticación en los datos, accede desde cualquier internet, otro individuo puede ingresar a su cuenta y suplantarla. Configurándose en estos casos, la responsabilidad del consumidor financiero.

## **2.7 ANÁLISIS DEL CONTRATO DE GOOGLE Y LAS EMPRESAS.**

Google tiene disponible el contrato en la plataforma <<https://cloud.google.com/terms/>>, y lo define como un Acuerdo de Licencia de la Nube, entre el proveedor y la entidad que acepta sus condiciones. En su contenido indica su denominación según la dirección de facturación del cliente<sup>145</sup>, empero, no se menciona a Colombia.

---

<sup>142</sup> COLOMBIA, CORTE SUPREMA DE JUSTICIA, Sala de Casación Civil, expediente 2010-00320 (11 de marzo de 2010), citado por COLOMBIA, SUPERINTENDENCIA FINANCIERA. Expediente 2013 -0063. No. 2013015100 (julio 31 de 2013).

<sup>143</sup> JIMÉNEZ, Edwin. Modelo de Tarificación Software como Servicio Saas. Trabajo de grado de Magíster en ciencias de la información y las comunicaciones. Bogotá: Universidad Distrital Francisco José de Caldas. Facultad de Ingeniería. Maestría en ciencias de la información y las Comunicaciones, [en línea] 2015. Disponible en <http://repository.udistrital.edu.co/bitstream/11349/2765/1/JimenezGarzonEdwinAlfonso2015.pdf>, [citado el 24 de abril de 2017], pág. 34.

<sup>144</sup> JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017

<sup>145</sup> *Google Cloud Platform Terms of Service*, marzo 7 de 2017, [en línea]. Disponible en <https://cloud.google.com/terms/> [citado el 22 de abril de 2017]

Posteriormente, señala que el Acuerdo será efectivo a partir de la fecha en que el cliente hace clic para aceptar y si se encuentra legitimado para decidir. Luego, describe los servicios de Google y dispone lo siguiente sobre los datos:

*1.3 Instalaciones: Todas las instalaciones que se utilizan para almacenar y procesar una solicitud y los datos de los clientes deberán cumplir con normas de seguridad razonables protección no inferior a las normas de seguridad de las instalaciones en los procesos de Google y almacena su propia información de un tipo similar. Google ha puesto en práctica sistemas y procedimientos estándar, al menos, de la industria para (i) garantizar la seguridad y confidencialidad de datos de la aplicación y el Cliente, (ii) proteger contra las amenazas o riesgos previstos para la seguridad o integridad de un Datos de programa y de los clientes, y (iii) proteger contra el acceso no autorizado o el uso de un cliente y datos de aplicación.*

*1.4 Datos de Ubicación. El cliente puede seleccionar dónde se almacenarán ciertos Datos del cliente ("Ubicación de los datos Selección"), y Google almacenará allí, de acuerdo con las condiciones específicas del servicio. Si una ubicación Selección de datos no está cubierto por las condiciones específicas del servicio (o una ubicación Selección de datos no es hecho por el Cliente con respecto a cualquier cliente de Datos), Google puede procesar y almacenar los datos de los clientes en cualquier lugar Google o sus agentes tengan instalaciones. Al utilizar los Servicios, el Cliente consiente a este tratamiento y almacenamiento de datos de clientes. En virtud de este Acuerdo, Google no es más que un procesador de datos<sup>146</sup>.*

Es decir, resalta los sistemas de seguridad que tiene Google para la protección de los datos personales, según los riesgos previstos y, a la vez, le da la opción al cliente de determinar el lugar de ubicación de los datos, pero si el cliente escoge un sitio donde no puede prestar efectivamente el servicio, se entiende que Google procesaría los datos en cualquier lugar.

Así mismo, precisa que al cliente se le asignará una cuenta con contraseña y señal, además, el cliente está en la obligación de notificar a Google ante un uso no autorizado de la contraseña. Luego, continúa describiendo las características de sus servicios e indica que Google puede hacer cambios al Acuerdo, de vez en cuando y, si el cliente no está conforme con las modificaciones, plantea como solución dejar de usar los servicios.

---

<sup>146</sup> *Ibíd.*

Respecto a los datos precisa:

*Google sólo puede cambiar las Condiciones de Procesamiento de Datos y Seguridad donde se requiere tal cambio de cumplir con la ley aplicable, regulación aplicable, orden judicial u orientación emitida por un regulador o agencia gubernamental, cuando con el cambio esté expresamente permitida por las condiciones de Procesamiento de Datos y Seguridad o cuando dicho cambio<sup>147</sup>.*

Por lo anterior, este proveedor para la protección de los datos personales se sujeta a las modificaciones del Acuerdo según la ley aplicable y no por la disposición de modificar bilateralmente lo acordado.

Después, se menciona las condiciones de pago e impuestos y las obligaciones de los clientes, frente al uso de los datos y deja claro que:

- *El cliente es el único responsable de sus aplicaciones, proyectos y datos de clientes y de asegurarse de que sus aplicaciones, proyectos y datos de los clientes cumplir con la política de uso aceptable. Google se reserva el derecho de revisar la aplicación del proyecto, y los datos de los clientes para el cumplimiento de la política de uso aceptable. El cliente es responsable de garantizar que todos los usuarios finales del cliente cumplan con las obligaciones del Cliente en virtud de la política de uso aceptable.*
- *El Cliente obtendrá y mantendrá los consentimientos requeridos necesarios para permitir el procesamiento de datos de clientes en virtud del presente Acuerdo.*
- *El cliente no podrá almacenar Datos del cliente que está sujeta al Tráfico Internacional de Armas Reglamento mantenida por el Departamento de Estado. A menos que se especifique lo contrario por escrito por parte de Google, Google no tiene la intención usos de los servicios para crear obligaciones bajo HIPAA<sup>148149</sup>.*

En ese sentido, la entidad bancaria, es responsable del tratamiento de datos de sus usuarios.

Luego de mencionar las condiciones para la licencia a terceros y la documentación requerida a la entidad, expone lo siguiente sobre los derechos de autor:

---

<sup>147</sup> *Ibidem.*

<sup>148</sup> *HIPAA, responsabilidades del seguro de salud. Ver al respecto: [https://translate.google.com.co/translate?hl=es&sl=en&u=http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00What isHIPAA.aspx&prev=search](https://translate.google.com.co/translate?hl=es&sl=en&u=http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00What%20isHIPAA.aspx&prev=search)*

<sup>149</sup> *Google Cloud Platform Terms of Service, marzo 7 de 2017, [en línea]. Disponible en <https://cloud.google.com/terms/> [citado el 22 de abril de 2017]*

*Política de copyright: Google ofrece información para ayudar a los titulares de derechos de autor a controlar su propiedad intelectual en línea, pero Google no puede determinar si algo está siendo usado legalmente o no sin su aporte. Google responde a los avisos de supuestas infracciones de los derechos de autor y termina las cuentas de los infractores reincidentes de acuerdo con las leyes de copyright aplicables, incluyendo, en particular, el proceso establecido en la Ley de Derechos de Autor del Milenio Digital. Si el cliente piensa que alguien está infringiendo los derechos de autor de Fin de atención al cliente de los clientes o de los Usuarios y quiere notificar a Google, el Cliente puede encontrar información sobre la presentación de avisos, y la política de Google sobre cómo responder a los avisos en <http://www.google.com/dmca.html><sup>150</sup>.*

Según lo anterior, Google determina el riesgo de vulneración de derechos de autor, sólo cuando existe una notificación por parte del cliente y no por cuenta propia.

Luego menciona cómo funciona la suspensión de alguna aplicación y respecto a los derechos de propiedad intelectual, resolviendo la inquietud ¿de quién son los datos? indica:

*“En las relaciones entre las partes, el cliente es titular de todos los derechos de propiedad intelectual en los datos del cliente y la aplicación o proyecto (en su caso), y Google posee todos los derechos de propiedad intelectual de los Servicios y Software” y para su uso: “Google no va a acceder o utilizar los Datos del Cliente, salvo que sea necesario para proporcionar los Servicios al Cliente”<sup>151</sup>.*

Después de seguir describiendo sus servicios, menciona el principio de confidencialidad de la información para el cumplimiento del Acuerdo:

*El destinatario no revelará la Información Confidencial, excepto a afiliados, empleados, agentes o asesores profesionales que necesiten conocerla y que hayan acordado por escrito (o en el caso de los asesores profesionales, que estén obligados) a mantener la confidencialidad. El beneficiario se asegurará de que las personas y entidades que utilizan la información recibida confidencial únicamente para ejercer los derechos y cumplir las obligaciones en virtud del presente Acuerdo, durante el uso de las precauciones razonables para mantener la confidencialidad<sup>152</sup>.*

En efecto, establece confusamente que sólo se podrá divulgar información confidencial en la medida requerida por un proceso legal aplicable, en el que se debe: notificar de inmediato a la otra parte de dicha divulgación antes de revelar y

---

<sup>150</sup> *Ibidem.*

<sup>151</sup> *Ibidem.*

<sup>152</sup> *Ibidem.*

cumplir con las solicitudes razonables de la otra parte en relación con sus esfuerzos para oponerse a la divulgación.

Luego, se precisa la duración del contrato, la resolución por incumplimiento y sus efectos: *“(iii) el Cliente se eliminará el software, cualquier aplicación, Instancia, Proyecto y Datos del cliente; y (iv) a petición, cada parte hará todos los esfuerzos comercialmente razonables para devolver o destruir toda la Información Confidencial de la otra parte”*<sup>153</sup>.

Es decir, una vez se termine el contrato se eliminarán los datos del cliente, pero no se menciona el proceso de migración de los datos a otro proveedor.

Después de exponer las condiciones de publicidad, hay una exención de responsabilidad en mayúscula relacionada con los datos:

*GOOGLE Y SUS PROVEEDORES NO SON RESPONSABLES POR LA ELIMINACIÓN DE O FALTA DE ALMACENAMIENTO DE DATOS DE CLIENTES Y otras comunicaciones mantenidas o transmitida a través USO DE LOS SERVICIOS. CLIENTE ES EL ÚNICO RESPONSABLE DE FIJACIÓN Y COPIA DE SEGURIDAD DE SUS DATOS DE LA APLICACIÓN, proyecto y cliente*<sup>154</sup>.

Esta cláusula conlleva al rompimiento del equilibrio contractual, porque no permite verificar la reciprocidad y equivalencia de derechos adquiridos y obligaciones contraídas que exige el ordenamiento jurídico en los contratos, pues están dirigidas a evitar o mitigar las consecuencias jurídicas para los eventos en que el proveedor incumpla las obligaciones<sup>155</sup>.

Luego de exonerarse totalmente de la responsabilidad en el tratamiento de los datos, indica más condiciones y confusamente menciona la Ley de los Estados Unidos e indica que *“si el cliente es una ciudad, condado o gobierno estatal entidad*

---

<sup>153</sup> *Ibídem.*

<sup>154</sup> *Ibídem.*

<sup>155</sup> POSADA, Camilo. Las cláusulas abusivas en los contratos de adhesión en el derecho colombiano *EN* Revista de la Universidad Externado. [en línea]. Disponible en <<http://revistas.uexternado.edu.co/index.php/derpri/article/view/4328/5081>> [citado el 24 de abril de 2017]

*estadounidense, a continuación, el acuerdo será en silencio con respecto a la ley aplicable y el lugar<sup>156</sup>.*

Es decir, si bien existen varias denominaciones de Google según la dirección de facturación del cliente, no es claro la legislación aplicable y la jurisdicción competente para conocer sobre alguna controversia derivada del contrato. Igualmente, se entiende que, en el contrato celebrado por Google como proveedor con la empresa, no existe una cláusula compromisoria que habilite al árbitro para dirimir las controversias y, si las partes no firman un pacto tendrán que recurrir a la jurisdicción ordinaria para que se resuelva un complejo conflicto jurídico.

## **2.8 ¿POR QUÉ ALGUNAS EMPRESAS NO CONTRATAN A GOOGLE?**

Según Leonardo Jaimes<sup>157</sup>:

*Google no es Microsoft, ya que tiene sus propias aplicaciones como Google Docs, y la mayoría de los computadores tienen Word, Excel, Power Point del Sistema Operativo Microsoft. Por lo general, las personas buscan lo que ya conocen, lo que es más compatible, a las empresas no les gusta pagar aplicaciones de más, pero si el cliente sólo utiliza Microsoft, se paga la licencia de este sistema y se deja la nube de Google*

---

<sup>156</sup> *Google Cloud Platform Terms of Service*, marzo 7 de 2017, [en línea]. Disponible en <https://cloud.google.com/terms/> [citado el 22 de abril de 2017]

<sup>157</sup> JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

### 3. LOS CONFLICTOS RELACIONADOS CON EL HABEAS DATA EN LOS CONTRATOS DE ALMACENAMIENTO DE NUBE.

Etimológicamente, la palabra “Conflicto” tiene su origen latín en la palabra “*conflingere*”, que en términos de la Real Academia Española de la Lengua hace alusión, entre otros, a “combate”, “lucha”, “pelea”, “problema”, “materia de discusión”. Así mismo, cuando se habla de conflicto jurídico, se hace referencia a una situación de disputa o desacuerdo entre dos o más partes, en el que se deriva la vulneración de un derecho, de una norma o el incumplimiento de obligaciones<sup>158</sup>.

De tal forma, en esta investigación se analizan los conflictos jurídicos que surgen al almacenar los datos personales o corporativos en un *data center* propiedad de una empresa como Google, según interrogantes como:

*¿Quién puede garantizar que nadie está accediendo de manera fraudulenta a información sensible o estratégica sobre clientes?, si en un momento dado no se paga la cuota mensual por el servicio: ¿puede el proveedor llegar a eliminar los archivos?, ¿qué ocurre si se producen cortes en el suministro eléctrico o de Internet? Y si la empresa proveedora de los servicios está en proceso de liquidación, ¿qué ocurre con los archivos de los clientes<sup>159</sup>.*

Así que, a continuación, se plantean los siguientes conflictos:

#### 3.1 FALTA DE NORMATIVIDAD.

No existe una regulación internacional y las reglamentaciones nacionales recogen confusamente el tema de computación en la nube. Aunque la función del regulador

---

<sup>158</sup> INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR (ICBF). Proceso servicios administrativos. Procedimiento saneamiento de inmuebles. Definiciones. Colombia, [en línea], 2016. Disponible en <http://www.icbf.gov.co/portal/page/portal/PortalICBF/procesos/apoyo/servicios>, [citado el 20 de abril de 2017].

<sup>159</sup> CERDÀ, Hugo. 'Cloud computing': informática en la nube, llega la tormenta. Técnica industrial, ISSN 0040-1838, n. 282, [en línea] 2009. Disponible en <<http://www.tecnicaindustrial.es/TIAdmin/Numeros/64/46/a46.pdf>>, [citado el 18 de abril de 2017], pág. 18.

es establecer unas reglas que den seguridad operativa y jurídica a los usuarios es un tema muy complejo por la propia idiosincrasia del modelo, que incluye ubicuidad y globalización de los servicios respecto a los usuarios.<sup>160</sup>

Respecto a los datos financieros, la Ley 1266 de 2008 regula la protección de la información del usuario de las entidades bancarias y determina que la actividad de administración de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países tiene un interés público, por cuanto ayuda a la democratización del crédito, la protección de la confianza pública en el sistema financiero y la estabilidad del mismo. Por tanto, los usuarios de esta información deberán valorar con elementos de juicio el estudio de riesgo y el análisis crediticio, sin basarse exclusivamente en la información relativa al incumplimiento de obligaciones suministradas por los operadores para adoptar decisiones frente a solicitudes de crédito<sup>161</sup>.

En Colombia, se encuentra la Ley 1581 de 2012<sup>162</sup> que desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, determinando las condiciones de legalidad, los deberes de los responsables y encargados del tratamiento de datos, la transferencia de información a terceros países, los mecanismos de vigilancia y sanción, entre otros aspectos, Empero, no se consagran disposiciones referentes a la protección del habeas data en los contratos de computación en la nube, presentándose ausencia legislativa en este tema.

---

<sup>160</sup>FONS, Fernando, Cloud Computing: caracterización de los impactos positivos obtenidos por la utilización del modelo Cloud Computing por las pymes, basado en la tipología de Modelos de Negocio de este tipo de empresas, [en línea]. Disponible en: <https://riunet.upv.es/bitstream/handle/10251/38864/Cloud%20Computing%20y%20Modelo%20de%20Negocio%20para%20pymes%20-%20TFM%20de%20Fernando%20Fons.pdf?sequence=1>, [citado el 4 de abril de 2017],pág. 59.

<sup>161</sup> COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 de 2008, (diciembre 31 de 2008), por la cual se dictan las disposiciones generales del habeas 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. Bogotá, D.C., 2008.

<sup>162</sup> COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 de 2012 (octubre 17 de 2012) por la cual se dictan disposiciones generales para la protección de datos personales, Diario Oficial. Bogotá, D.C., 2012.

En el Decreto 1074 del 26 de mayo de 2015, capítulo 25 reglamenta parcialmente la Ley 1581 de 2012 al indicar el procedimiento para la recolección de los datos personales, los derechos de los titulares a conocer, actualizar, rectificar y suprimir información, las transferencias y transmisiones internacionales de datos personales y la responsabilidad de las entidades demostrada frente al tratamiento de datos personales ante la Superintendencia de Industria y Comercio<sup>163</sup>.

En la actualidad, la Superintendencia de Industria y Comercio en virtud del artículo 19 de la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales y le atribuye la función de ejercer la vigilancia para garantizar que en el tratamiento de datos personales, está realizando un proyecto de Circular para la transferencia y transmisión de datos a otros países, según unos estándares de nivel adecuado de protección en el país receptor de la información personal<sup>164</sup>.

**3.1.1 Desarrollo jurisprudencial del derecho habeas data:** En la Sentencia T-443 de 1994, la Corte Constitucional se refirió al derecho del habeas data, indicando que es un derecho fundamental que contrarresta los riesgos del desarrollo de la informática que hace posible la difusión ilimitada de los datos personales. Toda vez que, el sistema centralizado de manejo de datos, cuenta con la capacidad de recoger, almacenar, relacionar, transmitir la información y potencia los peligros de manipulación de los datos, ya que este derecho otorga a la persona la posibilidad jurídica de impedir que terceras personas usen datos falsos, erróneos o reservados y desvirtúen su identidad o abusen del derecho a informar. Por tanto, el titular del derecho fundamental al habeas data goza del derecho a acceder al conocimiento

---

<sup>163</sup> COLOMBIA. PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. Decreto 1074 DE 2015 (mayo 26 de 2015) "Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62508>

<sup>164</sup> COLOMBIA, SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Proyecto de Circular Externa, Bogotá. Disponible en [http://www.sic.gov.co/sites/default/files/normatividad/Proyecto\\_Circular\\_Adiciona\\_capitulo\\_3\\_al\\_titulo\\_5\\_transferencia\\_internacional\\_de\\_datos.pdf](http://www.sic.gov.co/sites/default/files/normatividad/Proyecto_Circular_Adiciona_capitulo_3_al_titulo_5_transferencia_internacional_de_datos.pdf).

de la información recogida sobre él en bancos de datos, controlar razonablemente su transmisión, limitar el período de tiempo en el que puede conservarse, definir los objetivos para los que puede ser utilizada, actualizar su vigencia o hacer alguna rectificación<sup>165</sup>.

En ese sentido, el reconocimiento del derecho fundamental al habeas data, pretende la protección de los datos personales en un universo globalizado en el que el poder informático está avanzando (era digital). Esta protección responde a que de la importancia de los datos se deriva la garantía de otros derechos como la intimidad, el buen nombre, el libre desarrollo de la personalidad, entre otros<sup>166</sup>.

Por consiguiente, según la sentencia SU-082 de 1995, este derecho comprende al menos las siguientes prerrogativas:

*“a) El derecho a conocer las informaciones que a ella se refieren; b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos; c) El derecho a rectificar las informaciones que no correspondan a la verdad.”, e incluye el derecho a la caducidad del dato negativo<sup>167</sup>.*

En la Sentencia C-748 de 2011 el alto Tribunal precisó las tres líneas de interpretación que la jurisprudencia constitucional había determinado del derecho al habeas data y distinguió que en un primer momento fue interpretado como una garantía del derecho a la intimidad, se argumentaba la protección de los datos que pertenecen a la vida privada y familiar, en la que ni el Estado ni otros particulares pueden interferir. Luego existió una segunda línea interpretativa que consideraba el habeas data una manifestación del libre desarrollo de la personalidad, un ámbito de autodeterminación, relacionado con dignidad; y por último, la Corte Constitucional dejó claro que a partir de 1995, surge una tercera línea interpretativa que apunta al

---

<sup>165</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T- 443 de 1994. (12 de octubre de 1994) M. P Eduardo Cifuentes Muñoz.

<sup>166</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T- 167 de 2015. (15 de abril de 2015) M.P Jorge Ignacio Pretelt Chaljub.

<sup>167</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia SU-082 de 1995 (1 de marzo de 1995) M.P Jorge Arango Mejía.

habeas data como un derecho autónomo<sup>168</sup> que permite a las personas naturales y jurídicas conocer, actualizar y rectificar su información que se haya recogido por las entidades públicas y privadas<sup>169</sup>.

Igualmente, respecto a las entidades financieras en la Sentencia T-464 de 2002, la Corte Constitucional argumentó que el derecho al habeas data también cumple la función de proteger a las personas reportadas en las bases de datos contra el peligro del abuso de la información, por lo cual, cita el concepto de la base datos de la Superintendencia Bancaria de Colombia, actualmente Superintendencia Financiera:

*Las bases de datos, o centrales de información, son "sociedades especializadas en el manejo de información sistematizada, que de manera centralizada y de acuerdo a criterios únicos y preestablecidos proporcionan a las entidades vigiladas los datos sobre el comportamiento crediticio de los clientes del sector financiero"<sup>170</sup>.*

De tal forma, el sector financiero debe estar informado oportunamente sobre los antecedentes de sus clientes, para así garantizar la calidad del crédito, por cuanto, *"la permanencia del reporte en los bancos no puede ser indefinida, pero sí debe mantenerse por un tiempo razonable, aún con posterioridad al pago efectivamente realizado, aunque de manera tardía"*<sup>171</sup>.

*Así mismo, según la Corte Constitucional el derecho fundamental al habeas data puede ser amenazado cuando quiera que la información contenida en el banco de datos: i) es recogida de forma ilegal, es decir, sin el consentimiento del titular; ii) no es veraz, o iii) recae sobre aspectos íntimos de la vida del titular, no susceptibles de ser conocidos públicamente.*

*Por tanto, las entidades administradoras de bases de datos financieros son responsables de que (i) el ejercicio de recolección, tratamiento y circulación de datos sea razonable y no lesione los derechos fundamentales de los titulares de la*

---

<sup>168</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C-748 de 2011. (6 de octubre de 2011) M.P Jorge Ignacio Pretelt Chaljub.

<sup>169</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T- 167 de 2015. (15 de abril de 2015) M.P Jorge Ignacio Pretelt Chaljub.

<sup>170</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-464 de 2002. (13 DE JUNIO DE 2002) M.P Marco Gerardo Monroy Cabra.

<sup>171</sup> *Ibidem*.

*información; (ii) de la incorporación de los nuevos datos que les sean remitidos, en particular cuando de la inclusión de dichos datos se deriven situaciones ventajosas para el titular; (iii) de retirar los datos una vez se cumplan los términos de caducidad de los mismos; (iv) de mantener separadas las bases de datos que se encuentren bajo su cargo y de impedir cruces de datos con otros bancos de información; (v) de garantizar la integridad y seguridad de la información almacenada; (vi) de verificar que la entidad que le remite datos para divulgación, cuenta con autorización previa, expresa y escrita del titular del dato para el efecto, y (vii) de informar a este último que la información será incluida en su fichero<sup>172</sup>.*

Lo anterior, porque las entidades financieras y sus clientes se encuentran vinculados por relaciones económicas basadas en el postulado de la buena fe, donde se debe dar información en términos de certeza y condiciones de seguridad que garantice el manejo adecuado de los datos personales, asegurando la intervención de los usuarios financieros en la recolección, tratamiento y circulación de datos en todas las etapas del proceso informático, de manera tal que sus actividades económicas sean protegidas no sólo cuando la administración de datos es incompleta, falsa o inoportuna sino negligente, confusa o errada<sup>173</sup>.

### **3.2 LA INFLUENCIA DE LAS PARTES CONTRATANTES EN LOS CONTRATOS.**

Ante la ausencia de una definición exacta del servicio de nube, existen varias incertidumbres respecto a la legislación aplicable y las jurisdicciones competentes, razón por la cual, los contratos son los principales instrumentos para establecer las relaciones jurídicas entre el proveedor de nube y los clientes. Pese a que, la mayoría de las empresas contratantes tienen gran influencia en el mercado para negociar, los contratos plasman reglas determinadas por los proveedores, que pueden incluir cláusulas abusivas o ilegales; además, son poco claros, difíciles de entender y no disponen de un mecanismo de fácil reclamación<sup>174</sup>.

---

<sup>172</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T- 167 de 2015. (15 de abril de 2015) M.P Jorge Ignacio Pretelt Chaljub.

<sup>173</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T- 160 de 2005 (24 de febrero de 2005) M.P Marco Gerardo Monroy Cabra.

<sup>174</sup>EUROPA. PARLAMENTO EUROPEO. Dirección general de políticas interiores. Departamento temático, política, economía y científica. Computación en la nube, [en línea] mayo de 2012. Disponible en

Generalmente, las disposiciones de los proveedores sobre la protección de datos personales carecen de transparencia, no ofrecen garantías de la integridad de los datos, no existe precisión en las cláusulas relativas a la responsabilidad en los contratos, faltan normas de control y con frecuencia, la información sobre seguridad y privacidad en los sitios web de los proveedores de servicios en nube, es poco clara e incompleta<sup>175</sup>.

Un ejemplo, es el caso de Instagram, que de repente pretendió cambiar unilateralmente las condiciones del contrato de usuario, referentes a la propiedad, disponibilidad, control y uso del bien intangible<sup>176</sup> pues comunicó en diciembre de 2012 a sus numerosos usuarios que establecía una nueva política de privacidad para esta red social de fotos, en la cual sus anunciantes podrían utilizar libremente y sin compensación las fotos personales almacenadas en su nube, generando una fuerte reacción social que obligó a la empresa a retractarse de esta idea. Por consiguiente, una empresa proveedora del servicio de nube puede cambiar o extender el uso de la información personal recogida durante un lapso prolongado de tiempo, venderla a otra compañía con otros fines sociales, o a otro país con regulaciones diferentes del derecho de privacidad y control de la información de carácter personal<sup>177</sup>.

---

<[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO\\_ET\(2012\)475104\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf)>, [citado el 15 de abril de 2017], pág.100.

<sup>175</sup>Ibidem, pág. 9.

<sup>176</sup> Manuel Miró define el concepto intangible desde una perspectiva jurídica, haciendo referencia al derecho de propiedad que surge del ingenio humano, como bienes o derechos inmateriales con capacidad para satisfacer necesidades e intereses dentro de una determinada actividad económica, además de ser susceptibles de integrar el patrimonio empresarial o profesional, entre los cuales, puede mencionarse los relativos a los derechos de *software* y bases de datos, ver al respecto MIRÓ ECHEVARNE, Manuel. Valoración financiera de recursos intangibles. [en línea] 2006. Disponible en <<http://www.ub.edu/iafi/Recerca/Seminaris/miro.pdf>> [citado el 25 de abril de 2017], pág. 2-7.

<sup>177</sup> BUSTAMANTE DONAS, Javier. Ética en la nube: dilemas éticos y políticos en el modelo de "Computación en nube (Cloud computing)". Argumentos de razón técnica: Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología, ISSN 1139-3327, n. 16, [en línea] 2013, Disponible en <[http://institucional.us.es/revistas/argumentos/16/art\\_2.pdf](http://institucional.us.es/revistas/argumentos/16/art_2.pdf)>, [citado el 13 de abril de 2017], pág. 49.

### **3.3 RESPONSABILIDADES RELACIONADAS CON LOS SERVICIOS DE COMPUTACIÓN EN LA NUBE.**

Muchos proveedores se exoneran de toda la responsabilidad ante la pérdida de datos y no ofrecen ninguna información acerca de la ubicación de los centros de datos donde se almacenan los datos del usuario<sup>178</sup>.

### **3.4 FALTA DE AUDITORÍAS**

Según Javier Areitio,<sup>179</sup> en el desarrollo del contrato de almacenamiento de nube, no existe suficiente transparencia en las operaciones del proveedor de la nube a nivel de auditoría, por el contrario, Leonardo Jaimes<sup>180</sup> indica que los proveedores tienen un buen nivel de auditoría, saben quién ingresó, la hora, a hacer qué, ya sea a eliminar, modificar o trasladar la información, y si verifican que fue su personal, la empresa responde, o por el contrario, argumenta que el responsable de los datos es el usuario final.

### **3.5 CONTRATACIÓN DE TERCEROS, POR PARTE DEL PROVEEDOR.**

El proveedor de nube para ofrecer sus servicios puede subcontratar a terceros (proveedores desconocidos) que quizás no ofrecen las mismas garantías de seguridad y legalidad, ofrecidas por el proveedor en nube, o que modifican los términos y condiciones de sus servicios<sup>181</sup>.

---

<sup>178</sup> EUROPA. PARLAMENTO EUROPEO. Dirección general de políticas interiores. Departamento temático, política, economía y científica. Computación en la nube, [en línea] mayo de 2012. Disponible en <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO\\_ET\(2012\)475104\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf)>, [citado el 15 de abril de 2017], pág. 101.

<sup>179</sup> AREITIO BERTOLÍN, Javier. Protección del cloud computing en seguridad y privacidad. Revista española de electrónica, ISSN 0482-6396, n. 666, [en línea] 2010. Disponible en <[http://www.redeweb.com/\\_txt/666/42.pdf](http://www.redeweb.com/_txt/666/42.pdf)>, [citado el 12 de abril de 2017], pág. 46.

<sup>180</sup> JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

<sup>181</sup> AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA). Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información, [en línea] Disponible en <<https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish>>, [citado el 20 de abril de 2017], pág. 31.

Igualmente, un proveedor de computación en nube puede subcontratar determinadas actividades especializadas de su cadena de producción a terceros<sup>182</sup>. Ante esta situación, el nivel de seguridad del proveedor en nube puede estar supeditado al grado de dependencia de terceros del proveedor en nube. Una falta de coordinación de las responsabilidades entre las partes implicadas puede ocasionar: la no disponibilidad de los servicios, pérdida de la confidencialidad, integridad y disponibilidad de los datos, pérdidas económicas y del buen nombre, por la incapacidad de cumplir las demandas del cliente, el incumplimiento de los Acuerdos de nivel de servicio, el fallo en el servicio de conexión, etc<sup>183</sup>.

Además, el procesamiento de datos sensibles<sup>184</sup> fuera de las instalaciones de la empresa conlleva a un riesgo inminente, ya que es posible que estos servicios externos sorteen los controles físicos, lógicos y humanos, por esta razón, es necesario conocer quién maneja dichos datos<sup>185</sup>.

### **3.6 FALTA DE SEGURIDAD EN LA PROTECCIÓN DE LOS DATOS.**

Las empresas guardan rigurosamente la información acerca del volumen y los algoritmos<sup>186</sup> usados en sus transacciones, por lo que es difícil poder conocer el uso de los datos que circulan fuera de los límites de alcance de usuarios y proveedores de servicios. Esto significa que las medidas de protección locales frente a virus y

---

<sup>182</sup>JIMENEZ, Edwin. Modelo de Tarificación Software como Servicio Saas. Trabajo de grado de Magíster en ciencias de la información y las comunicaciones. Bogotá: Universidad Distrital Francisco José de Caldas. Facultad de Ingeniería. Maestría en ciencias de la información y las Comunicaciones, [en línea] 2015. Disponible en <http://repository.udistrital.edu.co/bitstream/11349/2765/1/JimenezGarzonEdwinAlfonso2015.pdf>, [citado el 24 de abril de 2017], pág. 29.

<sup>183</sup> *Ibidem*, pág. 35.

<sup>184</sup> Los datos sensibles son aquellos datos personales que revelen origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio al titular de los datos.

<sup>185</sup> INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN. (INTECO). Riesgos y amenazas en Cloud Computing. España: [en línea] marzo de 2011. Disponible en <[https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_riesgos\\_y\\_amenazas\\_en\\_cloud\\_computing.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf)>, [citado el 12 de abril de 2017], pág. 16.

<sup>186</sup> Algoritmo: Es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite llevar a cabo una actividad mediante pasos sucesivos que no generen dudas a quien deba hacer dicha actividad.

otras invasiones no son efectivas cuando la información está en circulación, creando mayores riesgos para la integridad de la misma. Vulnerabilidad que afecta también el procesamiento, toda vez que, la virtualización permite que el mismo conjunto de datos esté siendo procesado en máquinas con diferentes sistemas operativos y protocolos de comunicación<sup>187</sup>.

En consecuencia, la seguridad de los servicios en nube es fundamental para proteger los datos personales, corporativos y gubernamentales, garantizando la protección del acceso no autorizado, que la información no modifique ni se elimine por error, y la realización de copias de seguridad para salvaguardar la disponibilidad, la integridad y la confidencialidad en línea<sup>188</sup>. Es decir, la implementación del *backup*, o información de respaldo, como en el siguiente ejemplo: un archivo de word no se guarda en un sólo disco, sino que dividen el archivo de word y lo distribuyen en diferentes partes del mundo<sup>189</sup>.

Aunque, los proveedores comprimen y encriptan los datos, de tal forma que se vuelven en una serie de números desplazados en diferentes partes del mundo, con contraseñas para ser descryptados<sup>190</sup>, la nube hace que los ataques de autenticación basados en contraseñas, (práctica fraudulenta que utiliza un individuo experto en tecnología para robar contraseñas corporativas), tengan un impacto mayor, puesto que, las aplicaciones de las empresas ahora están expuestas en Internet. Por tanto, la acreditación basada en contraseñas llegará a ser insuficiente y será necesaria una autenticación más eficiente o de más factores para acceder a los recursos en nube. Además, la combinación de imágenes de sistema estándar,

---

<sup>187</sup>BUSTAMANTE DONAS, Javier. Ética en la nube: dilemas éticos y políticos en el modelo de "Computación en nube (Cloud computing)". Argumentos de razón técnica: Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología, ISSN 1139-3327, n. 16, [en línea] 2013, Disponible en <[http://institucional.us.es/revistas/argumentos/16/art\\_2.pdf](http://institucional.us.es/revistas/argumentos/16/art_2.pdf)>, [citado el 13 de abril de 2017], pág. 49, pág. 45.

<sup>188</sup>EUROPA. PARLAMENTO EUROPEO. Dirección general de políticas interiores. Departamento temático, política, economía y científica. Computación en la nube, [en línea] mayo de 2012. Disponible en <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO\\_ET\(2012\)475104\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf)>, [citado el 15 de abril de 2017], 56.

<sup>189</sup>JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

<sup>190</sup>Ibidem.

tecnologías de virtualización y una falta de dispositivos de entrada significa que un atacante en un equipo virtual puede ser capaz de averiguar las claves de codificación generadas en otros equipos virtuales,<sup>191</sup> de ahí que, sea necesario invertir en seguridad informática.

Empero, respecto a *Google*, según Leonardo Jaimes<sup>192</sup>:

*(...)Ningún otro proveedor tiene la seguridad de Google, es el único proveedor que podría soportar un ataque de red, todos los computadores en contra de Google y no se caería". Pues, por ejemplo, con el e- mail tienen como 50 nubes: una nube que se encarga de abrir la ventana para su intercepción, otra nube para validar la contraseña ingresada, otra nube que envía los correos, otra nube para el chat, otra nube para las propagandas.*

*Así mismo, Google empezó a contratar a ingenieros muy brillantes para diseñar su propio software de seguridad de redes e información, además. tienen sus propios centros de datos, no convencionales, en comparación a los demás proveedores, patentados de único uso de Google, nadie más sabe cómo funciona, han patentado desde la forma cómo almacenan la información hasta cómo ahorran energía.*

### **3.7 AUSENCIA DE CONCIENCIA DE SEGURIDAD**

Los clientes en nube no son conscientes de los conflictos que se podrían presentar al migrar hacia la nube, en particular, por los riesgos generados a partir de amenazas específicas de la nube: pérdida de control, cierre de la empresa proveedora, agotamiento de recursos del proveedor en nube, entre otros. La ausencia de conciencia también afecta al proveedor de nube, que no puede ser consciente de las medidas que debería tomar para mitigar los riesgos<sup>193</sup>.

---

<sup>191</sup>AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA). Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información, [e línea] Disponible en <<https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish>>, [citado el 20 de abril de 2017], páginas 57 y 61.

<sup>192</sup> JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

<sup>193</sup>AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA). Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información, [e línea] Disponible en <<https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish>>, [citado el 20 de abril de 2017], pág. 65.

### **3.8 ACCESO FÍSICO NO AUTORIZADO.**

Al concentrarse los recursos en centros de datos grandes, el impacto que produce la vulneración de los procedimientos de seguridad física es mayor. Así pues, se debe considerar entre los conflictos el hurto de equipamiento y la pérdida de copias de seguridad, ante las vulnerabilidades de procedimientos inadecuados de seguridad física, verbigracia, la falta de control en el perímetro con tarjetas de autenticación a la entrada, lo que genera perjuicios relacionados con el buen nombre de la empresa y la confianza del usuario.<sup>194</sup>, lo anterior, por la ausencia de cláusulas que garanticen la seguridad de la información.

### **3.9. LOS EMPLEADOS REVELAN INFORMACIÓN CONFIDENCIAL DE LA EMPRESA.**

Como en todos los sistemas de información, la amenaza que suponen los propios empleados es una de las más importantes, dado que tienen acceso de forma directa a los datos y aplicaciones de la empresa. Igualmente, en el desarrollo de la computación en la nube se pueden desencadenar incidentes de seguridad provocados por empleados descontentos, que actúan por error o desconocimiento. Además, quizás no hay control de quienes laboran y han dejado de trabajar en la empresa proveedora del servicio, que le permita tomar medidas de confidencialidad y métodos de control ante las amenazas internas<sup>195</sup>.

---

<sup>194</sup> TIEMBLO, Alexandra. Seguridad y Cumplimiento Normativo en el Cloud Computing. Trabajo de grado para optar por el título de ingeniero Informático. Madrid: Universidad Carlos III de Madrid, [en línea] 15 de junio de 2012. Disponible en < [http://e-archivo.uc3m.es/bitstream/handle/10016/16232/tfg\\_alexandra\\_tiemblo\\_moreno\\_2012.pdf?sequence=1](http://e-archivo.uc3m.es/bitstream/handle/10016/16232/tfg_alexandra_tiemblo_moreno_2012.pdf?sequence=1)>, [citado el 12 de abril de 2017] páginas. 17 y 18

<sup>195</sup> INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN. (INTECO). Riesgos y amenazas en Cloud Computing. España: [en línea] marzo de 2011. Disponible en <[https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_riesgos\\_y\\_amenazas\\_en\\_cloud\\_computing.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf)>, [citado el 12 de abril de 2017], pág. 13.

### 3.10 LOS RECURSOS COMPARTIDOS

Se refiere a la posibilidad de que las actividades maliciosas de un servicio puedan afectar al renombre de otro servicio. Por ejemplo, el spam, el escaneado de puertos o la prestación de contenido malicioso de la infraestructura en nube puede ocasionar: el bloqueo de un rango de direcciones de identificación personal IP y la confiscación de los recursos por la actividad contigua que se está realizando.<sup>196</sup>

### 3.11 DIFUSIÓN DE LA INFORMACIÓN PERSONAL.

Según Javier Bustamante<sup>197</sup>:

*(...) ante la pregunta del proveedor: ¿por qué se queja de que le miremos el correo, si de esa forma le ayudamos a gestionar mejor sus citas y sus compras? Lo que está en juego es la propia redefinición de lo que entendemos como derechos personales en relación con los derechos que competen a los Estados para promover el bien común y defender a la sociedad de sus enemigos. Para decidir qué tipo de sociedad queremos, debemos conocer las consecuencias políticas y éticas de las decisiones técnicas, ya que las tecnologías actúan como leyes: una vez extendidas, tienden a permanecer hasta que son sustituidas por otras, igual que las leyes son aceptadas inercialmente desde su promulgación hasta que son derogadas. Las tecnologías, igual que las leyes, son formas de vida: regulan la manera de entender el trabajo, el ocio, la participación política, y casi cualquier aspecto de la vida social que podamos imaginar*

Es decir, es común que el proveedor de nube verifique la información que se comparte en las redes sociales, el buscador de palabras y las páginas web que se visitan con frecuencia para enviar publicidad relacionada con los temas de interés del usuario.

---

<sup>196</sup> Ibídem, pág. 33

<sup>197</sup>BUSTAMANTE DONAS, Javier. Ética en la nube: dilemas éticos y políticos en el modelo de "Computación en nube (Cloud computing)". Argumentos de razón técnica: Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología, ISSN 1139-3327, n. 16, [en línea] 2013, Disponible en <[http://institucional.us.es/revistas/argumentos/16/art\\_2.pdf](http://institucional.us.es/revistas/argumentos/16/art_2.pdf)>,[citado el 13 de abril de 2017], pág. 49.

Por consiguiente, usar los servicios en la nube implica tener una confianza casi absoluta en el proveedor, dejando en sus manos información importante, pues resulta atractivo para los delincuentes cibernéticos y autores que planeen ser proveedores los servicios de computación en la nube con el propósito de buscar datos que puedan hurtar, vender, manipular o simplemente mirar.<sup>198</sup>.

### **3.12 PÉRDIDA DE GOBERNANZA.**

Al utilizar las infraestructuras en nube, el cliente necesariamente cede el control de cuestiones que pueden influir en la seguridad al proveedor en nube. Incluso, puede ocurrir que los Acuerdos de nivel de servicio no incluyan la protección de datos por parte del proveedor en nube, dejando vacíos en la seguridad,<sup>199</sup> control y disposición de la información.

### **3.13 PROPIEDAD DE LOS DATOS.**

Existe una controversia importante en torno a los términos ambiguos que utilizan las redes sociales en sus políticas de privacidad y propiedad de los datos, puesto que, particularmente en el contrato no se establece de forma clara que la organización mantiene el uso de los datos y que el proveedor no adquiere derechos o licencias a través de los acuerdos para usar los datos en su propio beneficio<sup>200</sup> y más aún cuando el usuario no es consciente de toda la información que está subiendo a la nube, porque al manipular un dispositivo inteligente, constantemente está desplazando datos que pueden ser de gran utilidad para Google.

---

<sup>198</sup>ÁVILA, Oscar, Computación en la nube. [en línea]. Disponible en <http://www.izt.uam.mx/newpage/contactos/anterior/n80ne/nube.pdf> [citado el 12 de abril de 2017], pág. 50.

<sup>199</sup>AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA). Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información, [e línea] Disponible en <<https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish>>, [citado el 20 de abril de 2017], pág. 9.

<sup>200</sup> INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN. (INTECO). Riesgos y amenazas en Cloud Computing. España: [en línea] marzo de 2011 Disponible en <[https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_riesgos\\_y\\_amenazas\\_en\\_cloud\\_computing.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf)>, [citado el 12 de abril de 2017], pág. 20

### 3.14 DEPENDENCIA DE PROVEEDORES CONCRETOS.

La rentabilidad de la oferta de servicios de tecnologías de información en nube aumenta con el número de usuarios, así que no hay incentivos para que los proveedores predominantes *Google, Amazon, Apple* hagan que sus sistemas sean compatibles con otros. Además, la falta de interoperabilidad provoca el riesgo de dependencia de proveedores concretos para los clientes, en especial cuando no existe ningún mecanismo para exportar grandes cantidades de datos almacenados a la nube de otra empresa<sup>201</sup>. Permitiendo una aceptación de los contratos de adhesión, por el hecho de ser un proveedor reconocido quien ofrece los servicios.

En otras palabras, la oferta actual sobre herramientas, procedimientos o formatos de datos estandarizados o interfaces de servicio que garantiza la portabilidad de las aplicaciones y de los datos personales resulta escasa. Por esta razón, la migración del cliente de un proveedor a otro o la migración de los datos y servicios es un procedimiento muy complejo. Así, lo anterior genera dependencia de un proveedor en nube para la prestación del servicio, especialmente, cuando no se tiene en cuenta la protección de los datos como aspecto fundamental en el contrato<sup>202</sup>.

Además, esta situación ocasiona una desventaja en el sentido que el proveedor de nube puede llegar a un estado de liquidez de la sociedad por cualquier motivo<sup>203</sup> y si no hay medidas de migración de los datos, pueden generarse varios perjuicios en los titulares de la información.

---

<sup>201</sup> EUROPA. PARLAMENTO EUROPEO. Dirección general de políticas interiores. Departamento temático, política, economía y científica. Computación en la nube, [en línea] mayo de 2012. Disponible en <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO\\_ET\(2012\)475104\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf)>, [citado el 15 de abril de 2017], pág. 101.

<sup>202</sup> *Ibidem*, pág. 9.

<sup>203</sup> *Ibidem*, pág. 28.

### 3.15 LOS PROVEEDORES REVELAN INFORMACIÓN CONFIDENCIAL POR ORDEN POLICIAL O JUDICIAL.

Está la posibilidad de que los proveedores de servicios en nube revelen información personal y confidencial cuando las autoridades policiales les obliguen a hacerlo, sin una orden (*como las fuerzas policiales estarían obligadas a hacer al incautar bienes personales en las dependencias del propietario, por ejemplo, un ordenador*), y sin informar a los propietarios de los datos<sup>204</sup>.

Según un análisis realizado por un bufete de abogados ubicado en Bruselas la seguridad pública o el bienestar público están en juego, toda vez que, en países de la Unión Europea, los proveedores de servicios en nube pueden estar obligados por ley a revelar los datos personales que alojan sin que se notifique al propietario o sujeto de los datos<sup>205</sup>.

Por tanto, los consumidores, respetuosos con la ley que almacenan sus datos, pueden verse afectados por órdenes de revelación de datos, verbigracia, cuando las autoridades policiales incautan los servidores u ordenadores que contengan información personal de individuos culpables e inocentes que a veces sin darse cuenta ha almacenado datos en las nubes, por el hecho de disponer de un teléfono inteligente<sup>206</sup>.

Aunque, en Colombia<sup>207</sup>, desde el punto de vista judicial, no existe claridad sobre la forma como un tribunal puede obtener acceso a información que esté en la nube, es posible que la legislación del país en donde se encuentren ubicados los datos

---

<sup>204</sup> *Ibidem*, pág. 73.

<sup>205</sup> *Ibidem*, pág. 73

<sup>206</sup> *Ibidem*, pág. 74

<sup>207</sup> Independientemente de que WhatsApp y Telegram sean nube o no, el Fiscal General de la Nación, Néstor Humberto Martínez, anunció que le enviará una propuesta al presidente de la República, Juan Manuel Santos, para que la entidad pueda tener un mayor acceso a la información contenida en redes sociales como WhatsApp y Telegram cuando los investigadores requieran dichos datos en los casos penales. Ver al respecto: Fiscalía buscará tener acceso al WhatsApp de los judicializados, *EN El País*, marzo 30 de 2017 [en línea]. Disponible en <http://www.elpais.com.co/colombia/fiscalia-buscara-tener-acceso-al-whatsapp-de-los-judicializados.html> [citado el 15 de abril de 2017]

sea flexible o estricta a la hora de permitir el acceso, previo mandato judicial a la información de un cliente administrada por un prestador de servicios en la nube, generando conflictos tanto a usuarios como a terceros por el acceso a tal información<sup>208</sup>.

### **3.16 DERECHOS DE AUTOR DE LAS OBRAS ALMACENADAS.**

Se afirma que en un futuro todo estará en la nube, y entonces, la relación entre tecnología y derechos de autor no será fácil, pues el conflicto es evidente entre los titulares de los derechos sobre los contenidos y aquellos que pregonan el acceso a la cultura y al conocimiento propiciado por las nuevas tecnologías de la información<sup>209</sup>.

Según Ernesto Rengifo<sup>210</sup>:

*“La discusión respecto de la computación en la nube tiene como eje determinar si cuando esta es usada como plataforma de gestión y almacenamiento de obras o contenidos digitales se compromete la protección de los derechos de autor de las obras almacenadas, dado que el almacenamiento supone la reproducción de la obra”.*

Es de tal forma, una controversia jurídica que debe ser claramente analizada en el desarrollo del contrato y más cuando se almacena contenido musical, videos, películas, libros, fotografías, entre otros datos.

---

<sup>208</sup> Mesa sectorial cloud computing. Cloud computing una perspectiva para Colombia, [en línea] abril de 2010. Disponible en <[http://cintel.co/wp-content/uploads/2013/05/16.clud\\_computing\\_Cloud-Computing-Mesa-sectorial-1.pdf](http://cintel.co/wp-content/uploads/2013/05/16.clud_computing_Cloud-Computing-Mesa-sectorial-1.pdf)>, [citado el 24 de abril de 2017],pág. 38.

<sup>209</sup> RENGIFO GARCÍA, Ernesto. Computación en la nube. Revista la propiedad inmaterial, ISSN 1657- 1959, n. 17, 2013p. 223-245. Disponible en <http://dialnet.unirioja.es/servlet/articulo?codigo=4775097> pág. 225.

<sup>210</sup> Ibidem, pág. 231.

### 3.17 ALMACENAMIENTO DE LA INFORMACIÓN EN UN SÓLO CENTRO DE DATOS.

El almacenamiento de datos en los mismos centros de datos incrementa los niveles de riesgo, toda vez que se puede perder o confundir.

### 3.18 EI RIESGO DE SHUTDOWN

Consiste en un cierre del servicio que dejaría al usuario no sólo sin su información, sino también sin el *know-how*<sup>211</sup>.

*Un día un gobierno puede prohibir el uso de ciertas aplicaciones, dejando indefenso a un usuario acostumbrado a la transparencia de los procesos de tratamiento de información que utiliza, entendiendo como transparencia el hecho de que no necesita ningún tipo de pericia técnica para poder llevar a cabo una tarea. En ese momento, lo transparente puede desaparecer como por arte de magia*<sup>212</sup>.

### 3.19 LUGAR DONDE SE ALMACENAN LOS DATOS

Uno de los principales problemas de los servicios en *cloud computing* es el desconocimiento de dónde son almacenados los datos y cómo se protegen. Aunque, la posesión de certificaciones de seguridad o la realización de auditorías externa del proveedor reduce, en parte, el problema, no es una solución absoluta. Cuando la información se mueve por diferentes países, sus marcos regulatorios cambian en la forma de tratar los datos. Por ejemplo, las leyes de protección de datos imponen obligaciones adicionales al manejo y procesamiento de datos que se transfieren a EEUU. Pues, el principal inconveniente del cumplimiento es conocer los límites que deja de aplicar la legislación del país que recoge los datos y comienza

---

<sup>211</sup> *Know how* es un conjunto de conocimientos técnicos y administrativos que son indispensables para conducir un proceso comercial y que no están protegidos por una patente, pero son determinantes para el éxito comercial de una empresa.

<sup>212</sup>BUSTAMANTE DONAS, Javier. Ética en la nube: dilemas éticos y políticos en el modelo de "Computación en nube (Cloud computing)". Argumentos de razón técnica: Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología, ISSN 1139-3327, n. 16, [en línea] 2013, Disponible en <[http://institucional.us.es/revistas/argumentos/16/art\\_2.pdf](http://institucional.us.es/revistas/argumentos/16/art_2.pdf)>,[citado el 13 de abril de 2017], pág. 46.

a materializar la legislación del país destino de la información, dado que supone algún riesgo o beneficio adicional<sup>213</sup>.

Los datos de las empresas-usuarios pueden albergarse en múltiples jurisdicciones, algunas de las cuales pueden presentarse varios conflictos jurídicos, verbigracia:

*“Si los centros de datos están ubicados en países de alto riesgo, por ejemplo, aquellos en los que no impera el Estado de Derecho cuyo marco jurídico y ejecución de leyes son impredecibles, los Estados policiales autocráticos, los Estados que no respetan los acuerdos internacionales, etc., los sitios podrían ser objeto de incursiones de las autoridades locales y los datos o sistemas podrían ser divulgados o confiscados por la fuerza”<sup>214</sup>.*

### **3.20 LA JURISDICCIÓN COMPETENTE Y TIPO DE ACCIÓN JUDICIAL.**

Algunos regímenes determinan que la jurisdicción competente es donde se encuentran almacenados físicamente los datos (ubicación del *data center*) o, el lugar donde se ofrece el servicio, o donde reside el usuario de quien refiere los datos. A la vez, otros declaran la jurisdicción en tanto el proveedor del servicio tenga un sitio de negocios en el país (sucursales), sin considerar dónde están localizados los datos<sup>215</sup>.

En Colombia, en el desarrollo del contrato entre el proveedor de nube y las empresas, es complejo conocer la jurisdicción competente ante una controversia jurídica, por ejemplo: Resolución del contrato por el incumplimiento de las cláusulas contractuales, la responsabilidad civil contractual por el daño de eliminar información confidencial de una compañía: En un principio, se puede inferir que le

---

<sup>213</sup>INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN. (INTECO). Riesgos y amenazas en Cloud Computing. España: [en línea] marzo de 2011 Disponible en <[https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_riesgos\\_y\\_amenazas\\_en\\_cloud\\_computing.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf)>, [citado el 12 de abril de 2017], páginas 18 y 19

<sup>214</sup>AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA). Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información, [e línea] Disponible en <<https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish>>, [citado el 20 de abril de 2017], pág. 49.

<sup>215</sup> Ibidem, pág. 16.

corresponde a la jurisdicción civil si se trata de entidades privadas, o contenciosa administrativa al involucrar al Estado, pero varias características van a generar duda en el accionante como: el proveedor tiene su domicilio principal en el extranjero, la empresa quien recibe el servicio también tiene su domicilio principal fuera del país, los datos están almacenados en un lugar lejano y el contrato se desarrolló en Colombia.

Pero, como el proveedor de nube presenta un servicio para las empresas, también se puede analizar que la Superintendencia de Industria y Comercio con la Acción de Protección del Consumidor tiene la competencia para conocer este tipo de conflictos, empero tendría que cumplirse con el requisito de procedibilidad de invitar a conciliar a un proveedor extranjero o, realizar una reclamación directa, notificando adecuadamente al encargado de ofrecer el servicio.

Además, el artículo 50 de la Ley 1480 de 2011 por la cual se promulgó el nuevo Estatuto del Consumidor establece la territorialidad de la ley al indicar que aplicará a: *“los proveedores y expendedores ubicados en el territorio nacional”*, deduciéndose que la Ley de Protección al Consumidor no cobijará a las compañías que, aunque presten servicios de nube en el país, no tengan una sede física en Colombia.

Ante la Superintendencia de Industria y Comercio también se pueden presentar la denuncia por vulneración del habeas data, pues le corresponde la vigilancia del tratamiento de los datos personales, pero surge de nuevo inquietudes que niegan su competencia como: si la entidad demandada es de otro país y aplica otra ley de protección de datos que le da competencia a otro juez y si el litigio no se centra directamente en la vulneración del derecho de habeas data sino en la solución de conflictos contractuales que se relacionan con este derecho, por ejemplo: el incumplimiento de una cláusula contractual que consagraba la obligación del

proveedor de establecer medidas de seguridad para proteger el lugar donde se almacena la información; un conflicto derivado del contrato.

Incluso, en la situación de revelar datos falsos que están almacenados en la nube y que perjudique el buen nombre, la dignidad y el habeas data de la persona jurídica, se podría interponer una denuncia penal, pero esta acción no solucionaría los conflictos derivados del contrato. Por otro lado, así los conflictos jurídicos se relacionen con el habeas data, un derecho fundamental, al indagar en mecanismo constitucional, quizás la acción de tutela no solucionaría la controversia contractual, si no se cumple con los requisitos de procedibilidad<sup>216</sup>.

### **3.21 SISTEMA JURÍDICO APLICABLE AL SERVICIO DE LA COMPUTACIÓN DE LA NUBE.**

Los proveedores, empresas contratantes, terceros- usuarios de las entidades y los centros de datos pueden ubicarse en cualquier lugar del mundo, incluso en varios lugares simultáneamente<sup>217</sup>

*La fragmentación del mercado único digital a lo largo de las fronteras geográficas debido a distintos marcos jurídicos puede restringir o ralentizar el desarrollo de servicios basados en la computación en nube a escala comunitaria, por ejemplo, los dependientes de los derechos de propiedad intelectual (música, películas, libros)<sup>218</sup>*

---

<sup>216</sup> Con todo, ha aclarado la jurisprudencia constitucional, que eventualmente podría proceder el amparo, incluso ante la existencia de otro mecanismo judicial para realizar el reclamo, si es que dicho mecanismo no resulta eficaz y no puede evitar la configuración de un perjuicio irremediable al (las) ciudadano). En efecto, según la jurisprudencia constitucional, aún si están envueltos asuntos de índole iusfundamental en una controversia de carácter contractual ello no supone necesariamente la procedencia de la acción de tutela, pues tal como se explicó en el acápite anterior, la acción de tutela tiene un carácter residual dado que su procedencia está supeditada a que el afectado carezca de otro medio de defensa judicial para la protección de sus derechos fundamentales, salvo que se utilice como mecanismo transitorio para evitar un perjuicio irremediable. Ver al respecto: COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-900 de 2008, (16 de septiembre de 2008), M.P. Humberto Antonio Sierra Porto.

<sup>217</sup>EUROPA. PARLAMENTO EUROPEO. Dirección general de políticas interiores. Departamento temático, política, economía y científica. Computación en la nube, [en línea] mayo de 2012. Disponible en <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO\\_ET\(2012\)475104\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf)>, [citado el 15 de abril de 2017], pág. 53.

<sup>218</sup> Ibidem, pág. 10.

En otras palabras, el desconocimiento de la ley aplicable, reduce la invención de los servicios de nube, y no le permite posicionarse totalmente en grandes mercados.

### **3.22 TRANSFERENCIA DE DATOS A OTROS PAÍSES.**

La transferencia internacional de datos a países terceros que no proporcionan un nivel adecuado de protección en materia de protección de datos es un problema para las empresas multinacionales con representación en diferentes países<sup>219</sup>.

Además, es muy frecuente que los datos que se encuentran en un lugar pasen a estar localizados en otro punto del planeta en pocas horas, cambios que el cliente suele desconocer<sup>220</sup> y en el momento que se presenten controversias por el mal servicio, tendrán que ser llevadas ante la jurisdicción competente, determinada por las cláusulas compromisorias o, quizás el domicilio del demandado, que puede ser en el exterior, situación compleja para solucionar el conflicto<sup>221</sup>.

En Colombia la sección quinta (5) del Decreto 1074 de 2005, que regula la transferencia y transmisión internacional de los datos, establece que:

**ARTÍCULO 2.2.2.25.5.2:** *El contrato que suscriba el responsable con los encargados para el tratamiento de datos personales bajo su control y responsabilidad señalará los alcances del tratamiento, las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y las obligaciones del encargado para con el titular y el responsable.*

*Además de las obligaciones que impongan las normas aplicables dentro del citado contrato, deberán incluirse las siguientes obligaciones en cabeza del respectivo encargado: 1. Dar Tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan. 2. Salvaguardar la seguridad de las bases*

---

<sup>219</sup> GUASCH, Vicente, SOLER José. Cloud computing: cláusulas contractuales y reglas corporativas vinculantes. RDUNED. EN Revista de derecho UNED, ISSN 1886-9912, n. 14, [en línea] 2014. Disponible en <<http://revistas.uned.es/index.php/RDUNED/article/view/13300/12171>>, [citado el 22 de abril de 2017], pág. 265

<sup>220</sup> *Ibidem*, pág. 253.

<sup>221</sup> MORENO, GONZALO. Jurisdicción aplicable en materia de datos personales en los contratos de cloud computing: análisis bajo la legislación colombiana. Universidad de los Andes, Facultad de Derecho. EN Revista de Derecho, Comunicaciones y Nuevas Tecnologías. N°9 junio de 2013. ISSN 1909-7786, pág. 13.

*de datos en los que se contengan datos personales. 3. Guardar confidencialidad respecto del tratamiento de los datos personales*<sup>222</sup>.

Aunque, como se indicó anteriormente, la Superintendencia de Industria y Comercio está elaborando un proyecto de Circular para la transferencia de datos a nivel internacional y por lo cual, dejó una lista con los países a los cuales se puede enviar información, no obstante, ha generado preocupaciones a nivel empresarial, particularmente en las áreas de tecnologías y seguridad de la información, ya que la gran mayoría de contratos de nube se celebran con empresas domiciliadas en el territorio de Estados Unidos, país en el cual se realizan múltiples tratamientos y que no se encuentra en dicha lista.<sup>223</sup>

### **3.23 NO ACCESO A LOS DATOS POR FALTA DE INTERNET.**

La intervención de un tercero es una causal de exoneración de responsabilidad, en el sentido de que hay proveedores que sólo dan el servicio de almacenamiento de nube, pero no de conexión a internet, y en el caso de que el usuario no tenga acceso a sus datos, pueden excepcionar respondiendo que el daño lo generó la empresa encargada de suministrar la conexión, congestión en la red o el uso no óptimo son los problemas que pueden ocurrir con las redes, la falta de recursos de aislamiento, la falta de planes de recuperación o de configuración errónea provocada por ejemplo por error humano.<sup>224</sup>

---

<sup>222</sup> COLOMBIA. PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. Decreto 1074 DE 2015 (mayo 26 de 2015) "Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62508>, Artículo 2.2.2.25.5.2

<sup>223</sup> VELASCO & CALLE D'ALEMAN. Incertidumbre en Colombia por Transferencia Internacional de Datos Personales con Estados Unidos, [en línea] marzo 15 de 2017. Disponible en <<http://velascocalle.co/blog/incertidumbre-en-colombia-por-transferencia-internacional-de-datos-personales-con-estados-unidos/>>, [citado el 12 de abril de 2017]

<sup>224</sup> TIEMBLO, Alexandra. Seguridad y Cumplimiento Normativo en el Cloud Computing. Trabajo de grado para optar por el título de ingeniero Informático. Madrid: Universidad Carlos III de Madrid, [en línea] 15 de junio de 2012. Disponible en <[http://e-archivo.uc3m.es/bitstream/handle/10016/16232/tfg\\_alexandra\\_tiemblo\\_moreno\\_2012.pdf?sequence=1](http://e-archivo.uc3m.es/bitstream/handle/10016/16232/tfg_alexandra_tiemblo_moreno_2012.pdf?sequence=1)>, [citado el 12 de abril de 2017], pág. 18.

Pues, la disponibilidad de las aplicaciones está sujeta a la existencia de acceso a Internet. Si un consumidor decide tener todos sus servicios informáticos en la nube, debe tener una buena cobertura de red; toda vez que, al carecer de conexión, su productividad es limitada<sup>225</sup>.

*Google* conociendo la importancia de la conexión a internet, creó el proyecto de lanzar globos al espacio para dar acceso a este servicio a las zonas más vulnerables del planeta, alrededor de 30 globos han sido lanzados desde Nueva Zelanda para navegar alrededor del mundo en una ruta controlada, y se espera en un futuro construir una flota más grande para ofrecer conexiones confiables. Incluso, los globos podrían ser desviados de sus rutas hacia áreas donde se han presentado desastres naturales, y así, reemplazar los sistemas de comunicaciones perjudicados. No obstante, un experto opina que controlar miles de globos a través de los aires es una tarea muy difícil de realizar<sup>226</sup>.

De acuerdo con lo descrito, es necesario aclarar que *Google* no provee internet, ya que le paga a un proveedor para establecer la conexión de manera gratuita y así poder brindar mejor sus ofertas<sup>227</sup>.

### **3.24 NO ACCESO A LOS DATOS POR EL DAÑO DE LOS SERVIDORES.**

Por el crecimiento de los servicios en nube, se han fortalecido las ventas de *netbooks*<sup>228</sup>, con la idea de que el usuario sólo acceda a su información a través de la red. El concepto es bueno, pero los fallos de los servidores en distintas ocasiones han alertado a muchos usuarios que desconfían de este servicio. Es el caso de

---

<sup>225</sup> ÁVILA, Oscar, Computación en la nube. [en línea]. Disponible en <http://www.izt.uam.mx/newpage/contactos/anterior/n80ne/nube.pdf> [citado el 12 de abril de 2017], pág. 50.

<sup>226</sup> VÁSQUEZ, Eduardo. Google lanza globos al espacio para dar internet gratis al mundo, *EN Sophimania*, esa manía por saber, [en línea] 24 de junio de 2013. Disponible en <<http://www.sophimania.pe/espacio-y-cosmos/cosmos/google-lanza-globos-al-espacio-para-dar-internet-gratis-al-mundo/>> [citado el 12 de abril de 2017].

<sup>227</sup> JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

<sup>228</sup> Netbook es una categoría de computadora portátil, de bajo coste y dimensiones reducidas, que aporta mayor movilidad y autonomía.

Google, por ejemplo, en varias ocasiones Gmail y su buscador han sufrido fallas, dejando a sus usuarios fuera de servicio por unas horas; las suficientes como para que millones de clientes presenten quejas <sup>229</sup>.

Aunque, según Leonardo Jaimes<sup>230</sup>, Google ha solucionado problemas que otras empresas no han podido, como la sostenibilidad de la información en los cinco continentes al mismo tiempo, en una sola línea de comunicación.

### 3.25 AISLAMIENTO DE DATOS.

*Los datos en los entornos cloud comparten infraestructura con datos de otros clientes. El proveedor debe garantizar el aislamiento de los datos de los respectivos clientes. El cifrado de los datos es una buena práctica, pero el problema es cómo aislar los datos cuando se encuentran en reposo ya que el cifrado, cuando no se hace uso de los datos, puede resultar una operación costo<sup>231</sup>.*

Es una interceptación de datos, un ejemplo del conflicto: no separar información confidencial de una compañía con los datos de otra empresa puede afectar la cláusula de confidencialidad del contrato.

### 3.26 SUPRESIÓN O MODIFICACIÓN DE DATOS INSEGURA O INCOMPLETA

Generalmente, en los contratos de almacenamiento en nube no existen cláusulas contractuales sobre la eliminación o modificación de los datos, razón por la que, se puede presentar lo siguiente:

Inconvenientes sobre la información, datos y calidad en la prestación de servicios *cloud*, dada la venta de la empresa proveedora, su cierre o transformaciones en sus

---

<sup>229</sup>ÁVILA, Oscar, Computación en la nube. [en línea]. Disponible en <http://www.izt.uam.mx/newpage/contactos/anterior/n80ne/nube.pdf> [citado el 12 de abril de 2017], pág. 49.

<sup>230</sup> JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

<sup>231</sup> INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN. (INTECO). Riesgos y amenazas en Cloud Computing. España: [en línea] marzo de 2011. Disponible en <[https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_riesgos\\_y\\_amenazas\\_en\\_cloud\\_computing.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf)>, [citado el 12 de abril de 2017], pág. 17.

líneas de negocio<sup>232</sup>, así, cuando se realiza una solicitud para suprimir un recurso en nube, al igual que sucede con la mayoría de sistemas operativos, en ocasiones el proceso no elimina definitivamente los datos. En ocasiones, la supresión adecuada de los datos también resulta imposible porque existen copias adicionales de datos almacenados, pero no disponibles o porque el disco que va a ser destruido también incluye datos de otros clientes<sup>233</sup>.

Existen varias formas en las que los datos se pueden ver comprometidos. Por ejemplo, el borrado o modificación de datos sin tener una copia de seguridad de los originales, supone una pérdida de datos. Esto deriva en pérdida de imagen de la compañía, daños económicos que podrían conllevar a una insolvencia empresarial, posterior liquidez y, si se trata de fugas, problemas legales, infracciones de normas, etc.<sup>234</sup>.

### **3.27. LOS DATOS ALMACENADOS SON FALSOS.**

Los datos están cambiando constantemente y, por lo tanto, quien autoriza la recopilación, puede conocer, actualizar y rectificar los datos recolectados por las Centrales de Información, al igual que aquellos que reposan en los archivos de entidades públicas y privadas.

*“Se analiza entonces lo importante que resulta que las entidades divulguen datos ciertos, previamente confirmados y permanentemente actualizados por los titulares,*

---

<sup>232</sup>JIMENEZ, Edwin. Modelo de Tarificación Software como Servicio Saas. Trabajo de grado de Magíster en ciencias de la información y las comunicaciones. Bogotá: Universidad Distrital Francisco José de Caldas. Facultad de Ingeniería. Maestría en ciencias de la información y las comunicaciones, [en línea] 2015. Disponible en <http://repository.udistrital.edu.co/bitstream/11349/2765/1/JimenezGarzonEdwinAlfonso2015.pdf>, [citado el 24 de abril de 2017], pág. 34.

<sup>233</sup>AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA). Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información, [e línea] Disponible en <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish>, [citado el 20 de abril de 2017], pág. 10.

<sup>234</sup>INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN. (INTECO). Riesgos y amenazas en Cloud Computing. España: [en línea] marzo de 2011 Disponible en [https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_riesgos\\_y\\_amenazas\\_en\\_cloud\\_computing.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf), [citado el 12 de abril de 2017], pág. 14.

*de manera que sus registros reflejen la realidad cambiante del comportamiento de los usuarios". Por consiguiente, en la jurisprudencia constitucional se observa una marcada insistencia en la necesidad de que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo, es decir que registre únicamente datos ciertos, totales, completos, suficientes, útiles y necesarios, que el afectado conoció y pudo rectificar oportunamente*<sup>235</sup>.

El creador de la Web Tim Berners-Lee ha advertido *"A menudo no tenemos ninguna manera de dar a conocer a las empresas qué información preferiríamos no compartir sobre todo con terceros, pues los términos y condiciones se toman o se dejan y lamentablemente ahora las personas se informan a través de las redes sociales y motores de búsqueda"*<sup>236</sup>.

Por este motivo, la red social Facebook ahora presenta un mensaje indicando que la información que se intenta compartir ha sido cuestionada, bajo prueba, para marcar posibles noticias falsas e información errónea, siendo el resultado de aliarse con agencias independientes de comprobación de hechos para atacar este fenómeno<sup>237</sup>.

Google conociendo este conflicto y con el fin de erradicar las noticias falsas de internet ha dispuesto *Fact Check*, un sistema de verificación de hechos a nivel global y en todos los idiomas. Así que, ahora algunos artículos saldrán con una etiqueta que los identifica como información comprobada por entidades dedicadas a verificar

---

<sup>235</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-943 de 2006. (16 de noviembre de 2006) M.P. Álvaro Tafur Galvis.

<sup>236</sup> Creador de la web advierte de manipulación con noticias falsas [EN Telesur](http://www.telesurtv.net/news/Creador-de-la-web-advierte-de-manipulacion-con-noticias-falsas-20170316-0054.html), [en línea] 16 de marzo de 2017. Disponible en <<http://www.telesurtv.net/news/Creador-de-la-web-advierte-de-manipulacion-con-noticias-falsas-20170316-0054.html>> [citado el 12 de abril de 2017]

<sup>237</sup> Facebook ya advierte a sus usuarios sobre noticias falsas [EN Telesur](http://www.telesurtv.net/news/Facebook-ya-advierte-a-sus-usuarios-sobre-noticias-falsas-20170322-0082.html) [en línea], 22 de marzo de 2017. Disponible en <<http://www.telesurtv.net/news/Facebook-ya-advierte-a-sus-usuarios-sobre-noticias-falsas-20170322-0082.html>> [citado el 11 de abril de 2017]

contenido; y si los medios de noticia quieren unirse a estas iniciativas deben seguir las directrices de *Google*<sup>238</sup>.

### **3.28 RECUPERACIÓN DE DATOS.**

En los contratos de almacenamiento de nube no existen pólizas de seguros ante cualquier eventualidad, razón por la cual, es necesario que los proveedores de nube, tengan una política de recuperación de datos en caso de desastre.<sup>239</sup>

### **3.29 NULO CONTROL SOBRE LA DILIGENCIA DE LAS OPERACIONES DEL PROVEEDOR.**

Un proveedor de nube no puede garantizar a un usuario que ha borrado datos no deseados o que almacena correctamente los datos del cliente<sup>240</sup>, y para el usuario es complejo determinar que sus datos han sido borrados, por lo general, no supervisa ese tipo de situaciones y no plantea el control como una obligación en el contrato.

### **3.30 SECUESTRO DE INFORMACIÓN O DE SERVICIO**

Conflicto jurídico relacionado con la ausencia de la obligación para el usuario de cuidar y evitar la manipulación de sus datos, pues “*en un entorno en la nube, si un atacante obtiene las credenciales de un usuario del entorno puede acceder a*

---

<sup>238</sup> Google vs, las mentiras. Disponible [EN](#) Softonic News letters. Lo mejor de la tecnología, en tu bandeja de entrada. También en Diario El País. Google amplía a todo el mundo su sistema de verificación de noticias falsas [en línea]. Disponible en <[http://tecnologia.elpais.com/tecnologia/2017/04/07/actualidad/1491552626\\_830458.html](http://tecnologia.elpais.com/tecnologia/2017/04/07/actualidad/1491552626_830458.html)>, [citado el 22 de abril de 2017].

<sup>239</sup> INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN. (INTECO). Riesgos y amenazas en Cloud Computing. España: [en línea] marzo de 2011 Disponible en <[https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_riesgos\\_y\\_amenazas\\_en\\_cloud\\_computing.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf)>, [citado el 12 de abril de 2017], pág. 17.

<sup>240</sup> AREITIO BERTOLÍN, Javier. Protección del cloud computing en seguridad y privacidad. Revista española de electrónica, ISSN 0482-6396, n. 666, [en línea] 2010. Disponible en <[http://www.redeweb.com/\\_txt/666/42.pdf](http://www.redeweb.com/_txt/666/42.pdf)>, [citado el 12 de abril de 2017], pág. 45.

*actividades y transacciones, manipular datos, devolver información falsificada o redirigir a los clientes a sitios maliciosos*<sup>241</sup>.

Igualmente, en la actualidad varios delincuentes cibernéticos están secuestrando información relevante de las empresas para solicitar dinero a cambio de su devolución.

### **3.31 ESPIONAJE EN EL PROVEEDOR DE LA NUBE Y ROBO DE INFORMACIÓN CORPORATIVA.**

Según Javier Areitio<sup>242</sup> en la red social Facebook, los usuarios dejan datos sensibles, los cuales, utiliza para presentarlos a otros usuarios y para aplicaciones de terceras partes que se ejecutan en la plataforma. Es decir, se podrían crear aplicaciones maliciosas y ejecutarlas en la nube Facebook para hurtar los datos.

Lo anterior, se puede presentar ante el incumplimiento del proveedor de cláusulas contractuales relacionadas con los protocolos de seguridad y confidencialidad de los datos.

### **3.32 EL PODER DE LOS GOBIERNOS SOBRE EL MANEJO DE LA INFORMACIÓN.**

Es un gran problema ético-político, que va en contra de la ética empresarial y responsabilidad corporativa en el manejo de la nube, frente al poder de los Estados que tienen la capacidad de tomar decisiones sobre la política tecnológica que quizás afecta a un ámbito que excede la extensión de su territorio nacional. De tal manera, ante la lucha contra el terrorismo, la seguridad nacional, la defensa de los valores

---

<sup>241</sup> INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN. (INTECO). Riesgos y amenazas en Cloud Computing. España: [en línea] marzo de 2011 Disponible en <[https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_riesgos\\_y\\_amenazas\\_en\\_cloud\\_computing.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf)>, [citado el 12 de abril de 2017], pág. 15.

<sup>242</sup> AREITIO BERTOLÍN, Javier. Protección del cloud computing en seguridad y privacidad. Revista española de electrónica, ISSN 0482-6396, n. 666, [en línea] 2010. Disponible <en [http://www.redeweb.com/\\_txt/666/42.pdf](http://www.redeweb.com/_txt/666/42.pdf)>, [citado el 12 de abril de 2017],

liberales, del libre comercio, etc., cada vez existe una mayor presión sobre las empresas tecnológicas para jugar un papel instrumental en estas políticas. En estos casos, hay muchos intereses, pues la colaboración entre gobiernos y empresas es amistosa y voluntaria, basada en relaciones de beneficio mutuo<sup>243</sup>.

Según Leonardo Jaimes<sup>244</sup> la mayoría de proveedores son de los Estados Unidos, y ante sus políticas de datos<sup>245</sup>, las agencias les están solicitando información de individuos que no son ciudadanos norteamericanos. Igualmente, Javier Bustamante<sup>246</sup> precisa que la prensa ha informado que grandes multinacionales como *Google*, aceptaron subvenciones del gobierno estadounidense para el desarrollo de servicios de computación en la nube, a cambio de colaboración en la identificación de usuarios y contenidos, así como de acceso generalizado sin orden judicial a los archivos depositados por los usuarios de estos servicios. De hecho, un representante de *Google* ante el defensor del consumidor en Estados Unidos argumentó: *"(...) al igual que a nadie le extraña que si manda una carta a un colega la abra su secretaria, los usuarios del correo electrónico no deberían sorprenderse al descubrir que sus mensajes son procesados durante el envío"*

De conformidad con lo anterior, se infiere que los conflictos jurídicos que pueden surgir se relacionan con el incumplimiento de cláusulas que consagran las obligaciones de tener medidas de seguridad, la responsabilidad en el manejo de los datos personales, el acceso, rectificación, separación, modificación, migración de la

---

<sup>243</sup> BUSTAMANTE DONAS, Javier. Ética en la nube: dilemas éticos y políticos en el modelo de "Computación en nube (Cloud computing)". Argumentos de razón técnica: Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología, ISSN 1139-3327, n. 16, [en línea] 2013, Disponible en <[http://institucional.us.es/revistas/argumentos/16/art\\_2.pdf](http://institucional.us.es/revistas/argumentos/16/art_2.pdf)>.[citado el 13 de abril de 2017], pág. 48.

<sup>244</sup> JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

<sup>245</sup> En Estados Unidos no hay una normativa general de protección de datos que dé seguridad para recibir cualquier tipo de información de otros países y, además, el presidente Donald Trump firmó un Decreto para eliminar las protecciones contempladas en la Ley de Privacidad de los EE. UU, para los extranjeros residentes en ese país, perjudicando la emisión de datos desde la Unión Europea. Ver al respecto: <http://www.eltiempo.com/mundo/eeuu-y-canada/trump-elimina-la-proteccion-de-datos-de-extranjeros-en-ee-uu-72126>

<sup>246</sup> BUSTAMANTE DONAS, Javier. Ética en la nube: dilemas éticos y políticos en el modelo de "Computación en nube (Cloud computing)". Argumentos de razón técnica: Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología, ISSN 1139-3327, n. 16, [en línea] 2013, Disponible en <[http://institucional.us.es/revistas/argumentos/16/art\\_2.pdf](http://institucional.us.es/revistas/argumentos/16/art_2.pdf)>.[citado el 13 de abril de 2017], páginas 48 y 49.

información, la terminación anticipada de los contratos sin garantías en el control de los datos, entre otros aspectos.

#### 4. CÓMO SE REPLICAN LOS CONFLICTOS DE HABEAS DATA EN LOS CONTRATOS DE ALMACENAMIENTO DE NUBE BANCARIA.

Las entidades financieras prestan muchos servicios que les permite almacenar varios datos del consumidor que son susceptibles de protección, y por lo cual se constituyen en meros proveedores de servicios a favor de empresas como Google, *“propietario de las relaciones con los clientes”*<sup>247</sup>.

Empero, en un informe reciente de la Unión Europea UE<sup>248</sup> se ha constatado que las entidades financieras no tienen claridad sobre los servicios basados en la nube, mientras que, en un estudio del Ponemon Institute<sup>249</sup> se concluyó que utilizar aplicaciones en la nube en lugar de utilizar soluciones de las tecnologías de la información tradicionales generaría perjuicios debido al costo de las filtraciones de datos, *“una filtración de los datos almacenados en la nube que involucrará la pérdida o el robo de más de 100 mil registros de clientes podría suponer un costo medio de hasta 5.32 millones de dólares, en comparación con un costo de 2.37 millones de dólares si lo datos están almacenados en instalaciones propias”*. Por lo tanto, los bancos desconocen los conflictos de filtraciones por parte de los proveedores de nube, magnificándose riesgos operativos y para su reputación.

Ivanna Zauzich<sup>250</sup> afirma que la clave de los bancos es innovar, pero también entender las regulaciones de cada país, ya que, algunos lugares permiten que las entidades financieras tengan la información en la nube, pero respaldada físicamente

---

<sup>247</sup> SALIDO, Ruben, RODRIGUEZ, Mario y ARRANZ, ÁLVARO, Innovación y Multicanalidad en Banca. “La amenaza de las “FinTech Start Up,s”, Colegio Universitario de Estudios Financieros CUNEF, 2014-2015, [en línea] Disponible en <[http://biblioteca.cunef.edu/gestion/catalogo/doc\\_num.php?explnum\\_id=1360](http://biblioteca.cunef.edu/gestion/catalogo/doc_num.php?explnum_id=1360)>, [citado el 14 de abril de 2017] pág. 103.

<sup>248</sup>ENISA. Secure Use of Cloud Computing in the Finance Sector Good practices and recommendations. <https://goo.gl/txcRKdBLAZHESKI>, citado por: BLAZHESKI, Filip. ¿Banca en la nube o banca en las nubes? EN: BBVA. Observatorio Económico EEUU [en línea]. 2016, P. 1. Disponible en <[https://www.bbva-research.com/wp-content/uploads/2016/05/160510\\_CloudBanking\\_esp.pdf](https://www.bbva-research.com/wp-content/uploads/2016/05/160510_CloudBanking_esp.pdf)> [citado en 8 de enero de 2017] páginas 6 y 7.

<sup>249</sup>Ponemon Institute. Data Breach: The Cloud Multiplier Effect. 2014, <http://goo.gl/e50p1f> citado por: BLAZHESKI, Filip. ¿Banca en la nube o banca en las nubes? EN: BBVA. Observatorio Económico EEUU [en línea]. 2016, P. 1. Disponible en <[https://www.bbva-research.com/wp-content/uploads/2016/05/160510\\_CloudBanking\\_esp.pdf](https://www.bbva-research.com/wp-content/uploads/2016/05/160510_CloudBanking_esp.pdf)> [citado en 8 de enero de 2017], páginas 6 y 7.

<sup>250</sup> ZAUZICH, Ivanna. Cloud banking: De qué se trata la banca en la nube y cómo implementarla. 22 de marzo de 2016 EN Cobiscorp blog. [en línea] Disponible en <<http://blog.cobiscorp.com/banca-en-la-nube-cloud-banking>> [citado el 23 de marzo de 2017].

en un *data center*, es decir, en un centro de datos en el que se almacena la información del banco, y si no existe una regulación clara, se pueden presentar inconvenientes ante el incumplimiento de las condiciones establecidas en cada jurisdicción.

Así, los datos del cliente pueden almacenarse en múltiples jurisdicciones, pudiendo ser algunas de estas de alto riesgo en virtud del marco jurídico vigente en cada Estado. En un país donde rige un conjunto de normativas impredecibles, los datos pueden quedar sujetos a divulgación forzada, o los proveedores pueden utilizarlos con fines ilícitos. Lo anterior, genera el riesgo de situaciones litigiosas complejas por parte de los clientes contra las entidades financieras con alta probabilidad de impactos negativos en los resultados de las mismas<sup>251</sup>.

Así también, Booz Allen Hamilton<sup>252</sup> considera que los bancos se enfrentan a desafíos regulatorios debido a la naturaleza sensible de sus datos y a riesgos procedentes de terceros, por la renuncia del control sobre partes importantes de la infraestructura corporativa, con el resultado de que se afecte la privacidad. Igualmente, cuando los bancos transfieren los servicios básicos a la nube asumen el riesgo de renovaciones de contratos oportunistas, con cláusulas abusivas, toda vez que, el proveedor adquiere un poder de negociación importante al conocer que el banco tendría que asumir mayores costos si decidiera cambiar de nube y, es muy difícil que un banco pudiera negociar eficazmente con *Google* o auditarlo.

Además, los incumplimientos de pautas contractuales o la existencia de cierta informalidad en los acuerdos para la prestación de servicios a través de Internet, junto con modificaciones de las condiciones que suelen adoptar los proveedores de

---

<sup>251</sup> LÓPEZ, María, ALBANESE, Diana y otros. Identificación de riesgos vinculados con el uso de Cloud Computing en la Gestión Organizacional. Aplicación de la Risk Breakdown Structure a Entidades Financieras de la República Argentina. Rio Janeiro: ANPAD [en línea] 4 de septiembre de 2011. Disponible en <<http://www.anpad.org.br/admin/pdf/ADI2220.pdf>>, pág. 11. [citado el 12 de abril de 2017]

<sup>252</sup> ALLEN, Booz citado: BLAZHESKI, Filip. ¿Banca en la nube o banca en las nubes? EN: BBVA. Observatorio Económico EEUU [en línea]. 2016, P. 1. Disponible en <[https://www.bbva.com/wp-content/uploads/2016/05/160510\\_CloudBanking\\_esp.pdf](https://www.bbva.com/wp-content/uploads/2016/05/160510_CloudBanking_esp.pdf)> [citado en 8 de enero de 2017], páginas 6 y 7.

manera unilateral, generan riesgos muy costosos que ninguna entidad financiera puede dejar al arbitrio del proveedor<sup>253</sup>.

Bruno Brastón<sup>254</sup> argumenta que algunos bancos se detienen en implementar *cloud computing* por la seguridad, privacidad, confidencialidad, integridad de los datos, requerimientos de autenticación, ubicación de los datos, disponibilidad y recuperación, y si estos aspectos no se tienen en consideración, se pueden violar regulaciones gubernamentales, dado que, cada país tiene diferentes normas en cuanto a dónde está permitido que resida la información de sus ciudadanos. Así, el hecho de que esta tecnología ofrece un modelo computacional que atraviesa fronteras puede llegar a ser un problema jurídico para ciertas instituciones financieras afectadas por estas regulaciones. Razón por la cual, debe ser un aspecto detalladamente observado en los contratos con los proveedores de nube dónde se almacena la información bancaria y la propiedad intelectual, toda vez que, existe la disyuntiva acerca de si los datos le pertenecen al proveedor de *cloud computing* o a la entidad financiera que consuma sus servicios.

Igualmente, para Héctor Noceti y Aníbal Freijo<sup>255</sup>, *“el hecho de que grandes cloud providers (Google, Microsoft, Amazon, etc.) no cuenten con infraestructura de data center dentro de los límites del país, implican de alguna manera una barrera para su adopción”*, también se debe tener en cuenta, el aspecto de la arquitectura de aplicaciones core, las cuales a veces están en entornos propietarios, con un alto grado de personalización, haciendo más complejo el proceso de migrar a soluciones de *software* existentes en la nube.

---

<sup>253</sup> LÓPEZ, María, ALBANESE, Diana y otros. Identificación de riesgos vinculados con el uso de Cloud Computing en la Gestión Organizacional. Aplicación de la Risk Breakdown Structure a Entidades Financieras de la República Argentina. Rio Janeiro: ANPAD [en línea] 4 de septiembre de 2011. Disponible en <<http://www.anpad.org.br/admin/pdf/ADI2220.pdf>>. [citado el 12 de abril de 2017], pág. 11.

<sup>254</sup> GASTÓN, Bruno. Cloud computing en la industria financiera. [en línea] <[http://www.palermo.edu/ingenieria/pdf2014/13/CyT\\_13\\_05.pdf](http://www.palermo.edu/ingenieria/pdf2014/13/CyT_13_05.pdf), 2013>, [citado el 22 de abril de 2017], Páginas 76 y 77.

<sup>255</sup> NOCETI, Héctor Y FREIJO, Aníbal. Cloud computing. Su aplicación en la banca privada Argentina. Buenos Aires, Argentina: Universidad Argentina de la Empresa (UADE) Facultad de Ingeniería y Ciencias Exactas, [en línea] Disponible en <<http://44jaiio.sadio.org.ar/sites/default/files/sts264-276.pdf>> [citado el 23 de abril de 2017] pág. 273.

Para María López y Diana Albanese<sup>256</sup>, aun cuando el proveedor del servicio garantice la seguridad de la información, el banco continúa siendo responsable de los datos que se proporcionan y de los daños que pudieran generarse a terceros, razón por la que es fundamental la evaluación de los conflictos y responsabilidades asociadas a la utilización de servicios *cloud computing*. De tal manera, el principal riesgo de esta tecnología en un sector como el financiero es la seguridad del significativo volumen de datos sensibles que se manejan, se incluyen también los riesgos referidos al incumplimiento por parte del proveedor de las cláusulas sobre el tratamiento legal de los datos de los clientes, de protección de propiedad intelectual por las aplicaciones creadas y ejecutadas en la nube, entre otras.

Además, en el caso que el proveedor sea adquirido por un tercero implica la probabilidad de un cambio estratégico que puede generar el incumplimiento de ciertas cláusulas contractuales, por ejemplo, las inversiones en seguridad, los controles de seguridad no contractual generan incumplimientos en los requisitos de seguridad preestablecidos y acordados, y perjudican la reputación de la organización, la confianza de clientes y la lealtad de los empleados<sup>257</sup>.

Asimismo, entre los conflictos se encuentra el incumplimiento de los mecanismos de separación de la información, pues los recursos en nube son compartidos por múltiples usuarios, y si el proceso de supresión de la información solicitada por los bancos no es protegido por el proveedor de la nube, se puede presentar la pérdida de contraseñas y transferencia de las mismas entre usuarios o accesos no autorizados de hackers y delincuentes de la web<sup>258</sup>.

---

<sup>256</sup> LÓPEZ, María, ALBANESE, Diana y otros. Identificación de riesgos vinculados con el uso de Cloud Computing en la Gestión Organizacional. Aplicación de la Risk Breakdown Structure a Entidades Financieras de la República Argentina. Rio Janeiro: ANPAD [en línea] 4 de septiembre de 2011. Disponible en <<http://www.anpad.org.br/admin/pdf/ADI2220.pdf>>. [citado el 12 de abril de 2017], pág. 11.

<sup>257</sup> *ibidem*, pág. 11.

<sup>258</sup> *Ibidem*, pág. 12.

Del mismo modo, Hugo González<sup>259</sup> considera que mantener un alto nivel de seguridad y privacidad en la data que se deposita en el entorno *cloud* es un tema crítico para la institución financiera, así que, el proveedor debe garantizar medidas para cubrir la responsabilidad en el manejo y administración de los datos, cumplimiento de las regulaciones propias de cada país, de manera que se asegure la no afectación de la privacidad, seguridad y protección de la información.

Para el Instituto Nacional de Tecnología de la Comunicación (INTECO)<sup>260</sup> de España:

*La solución podría partir por reforzar la comprobación de seguridad de los clientes. Por ejemplo, los bancos empiezan a desarrollar medidas para que los navegadores de sus clientes aseguren los datos mediante el cifrado de las comunicaciones y aplicando mecanismos para evitar la interceptación de las pulsaciones de teclado.*

*Por su parte, la Agencia Europea de Seguridad de las Redes y de la Información<sup>261</sup> indica que:*

*Una característica común a todos los proveedores es que ofrecen la posibilidad de un escenario de «pánico bancario» para el proveedor en nube. Para este escenario, en caso de producirse una crisis de confianza en la situación financiera del proveedor en nube, tiene lugar una salida en masa y una retirada de contenido por orden de llegada. Entonces, en una situación en la que el proveedor limita la cantidad de «contenido» (código de aplicación y datos) que puede «retirarse» durante un período de tiempo dado, algunos clientes nunca podrán recuperar sus datos y sus aplicaciones.*

---

<sup>259</sup> GONZÁLEZ, Hugo. Implementación y uso de un *core bancario* para banca retail en la tecnología *cloud computing*. Trabajo de grado de Magister en Gerencia de Tecnología de la información, Quito: Pontificia Universidad Católica de Ecuador. Maestría en Gerencia de Tecnología de la información. [en línea], mayo de 2015. Disponible en <<http://repositorio.puce.edu.ec/bitstream/handle/22000/8539/CASO%20DE%20ESTUDIO%20-%20Hugo%20Gonzalez.pdf?sequence=1>> [citado el 12 de abril de 2017] Páginas 30, 31 y 32.

<sup>260</sup> INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN. (INTECO). Riesgos y amenazas en Cloud Computing. España: [en línea] marzo de 2011. Disponible en <[https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_riesgos\\_y\\_amenazas\\_en\\_cloud\\_computing.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf)>, [citado el 12 de abril de 2017], pág. 22.

<sup>261</sup> AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA). Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información, [e línea] Disponible en <<https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish>>, [citado el 20 de abril de 2017], pág. 30.

Respecto a la transferencia de datos, diversos países de la Unión Europea, limitan la transferencia de información hacia terceros países, cuando no ofrecen las garantías de un manejo adecuado de privacidad y confidencialidad de la información<sup>262</sup>. En Colombia es claro que los bancos transfieren constantemente información a otros países, pero también ha avanzado con las restricciones consagradas en la Ley 1480 de 2011, el Decreto 1074 de 2015 y ahora el proyecto de Circular de la Superintendencia de Industria y Comercio que consigna la lista de países a los cuales no se puede enviar información.

Otro conflicto que se puede presentar en la nube bancaria es el denominado *Phishing*, una técnica fraudulenta que utilizan los delincuentes al enviar correos electrónicos en nombre de entidades bancarias, para pedir los datos de acceso a las cuentas, con el argumento de que esta ha sido bloqueada o hackeada. Estos mensajes los remiten a un link de la entidad financiera, pero en realidad lo envía a una página falsa, igual a la del banco. Esta modalidad sucedió hace poco con la plataforma de Bancolombia y se relaciona con la nube ante la debida diligencia del proveedor y la entidad bancaria de aportar medidas de seguridad para corroborar la información en el acceso de usuarios a las cuentas y así, cumplir con la protección de datos<sup>263</sup>.

Por otro lado, respecto al conflicto de almacenamiento de la información falsa por parte de las entidades financieras, la Corte Constitucional ha indicado lo siguiente:

*Es claro que, si la información respectiva es falsa o errónea, no solamente se afectan los derechos a la honra y al buen nombre de la persona concernida, sino que, precisamente por el efecto multiplicador que tiene el informe negativo en las instituciones receptoras de la información incorporada al banco de datos o archivo, resulta notoriamente perjudicada en su actividad económica y en su situación patrimonial. No se pierda de vista que un cierre del crédito puede provocar una*

---

<sup>262</sup> Mesa sectorial cloud computing. Cloud computing una perspectiva para Colombia, [en línea] abril de 2010. Disponible en <[http://cintel.co/wp-content/uploads/2013/05/16.clud\\_computing\\_Cloud-Computing-Mesa-sectorial-1.pdf](http://cintel.co/wp-content/uploads/2013/05/16.clud_computing_Cloud-Computing-Mesa-sectorial-1.pdf)>, [citado el 24 de abril de 2017], pág. 35

<sup>263</sup> Sistemas. EN Dataware [en línea] Disponible en <<http://www.dwsistemas.com/es/index.php/noticias/27-peligro-pagina-bancolombia-phishing>> [citado el 14 de abril de 2017].

*cadena de incumplimientos forzados, la incapacidad de contraer nuevas obligaciones, la cesación de pagos y la quiebra*<sup>264</sup>.

En atención a lo cual, según el alto Tribunal las entidades bancarias tienen el deber de verificar los datos de los usuarios, pues en el caso de que existe información errónea, verbigracia: El usuario se encuentre en deuda con el banco, afecta los derechos fundamentales de éste y de ahí, la relación con el proveedor, quien además de verificar cualquier información, debe garantizar que la información del usuario no se ha mezclado con la información de otro usuario quien sí tiene pendiente una obligación financiera.

Por tanto, el contrato debe estipular esas obligaciones para el tratamiento de datos para el proveedor y el banco, pues según la Corte Constitucional las entidades administradoras de bases de datos financieros también son responsables de lo siguiente:

*(...) (i) el ejercicio de recolección, tratamiento y circulación de datos sea razonable y no lesione los derechos fundamentales de los titulares de la información; (ii) de la incorporación de los nuevos datos que les sean remitidos, en particular cuando de la inclusión de dichos datos se deriven situaciones ventajosas para el titular; (iii) de retirar los datos una vez se cumplan los términos de caducidad de los mismos; (iv) de mantener separadas las bases de datos que se encuentren bajo su cargo y de impedir cruces de datos con otros bancos de información; (v) de garantizar la integridad y seguridad de la información almacenada; (vi) de verificar que la entidad que le remite datos para divulgación, cuenta con autorización previa, expresa y escrita del titular del dato para el efecto, y (vii) de informar a este último que la información será incluida en su fichero*<sup>265</sup>.

Igualmente, el Tribunal Constitucional indicó que el reporte de datos negativos a centrales de información crediticia debe ser informado al titular del dato, con el fin de que este pueda ejercer sus derechos al conocimiento, rectificación y actualización de los datos, antes de que estos sean expuestos al conocimiento de terceros, toda vez que: *“(...) el derecho al habeas data resulta vulnerado en los eventos*

---

<sup>264</sup>COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T- 167 de 2015. (15 de abril de 2015) M.P Jorge Ignacio Pretelt Chaljub

<sup>265</sup> Ibidem.

en que la información contenida en un archivo de datos (i) sea recogida de forma ilegal, (ii) sea errónea, (iii) o verse sobre aspectos reservados de la esfera personal del individuo<sup>266</sup>.

#### **4.1 CONSECUENCIAS DE ANALIZAR LOS CONFLICTOS JURÍDICOS RELACIONADOS CON EL HABEAS DATA EN EL CLOUD BANKING.**

Una vez se determinan las fuentes y los conflictos jurídicos relacionados con el habeas data en los contratos entre Google y las entidades financieras se puede establecer que:

Los conflictos jurídicos dependen de con quien se provea la nube, es mejor buscar empresas reconocidas como Google, Amazon, Microsoft, porque si se adquiere los servicios con una empresa que no sea reconocida en el mercado, que no tenga una firma de seguridad digital, y de trayectoria va a ser complicado garantizar la confidencialidad de los archivos<sup>267</sup>.

Es necesario estandarizar los términos y condiciones en los contratos de los usuarios, con el desarrollo de modelos de buenas prácticas internacionales, de forma sencilla y legible<sup>268</sup>.

El proveedor *cloud* a través cláusulas de confidencialidad debe asegurar el no divulgar información estratégica de sus clientes finales que, en muchos casos por su naturaleza, puede ser de alto impacto, como es el caso de las instituciones financieras.<sup>269</sup>

---

<sup>266</sup> Ibidem.

<sup>267</sup> JAIMES, Leonardo, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

<sup>268</sup> EUROPA. PARLAMENTO EUROPEO. Dirección general de políticas interiores. Departamento temático, política, economía y científica. Computación en la nube, [en línea] mayo de 2012. Disponible en <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO\\_ET\(2012\)475104\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf)>, [citado el 15 de abril de 2017], pág. 103

<sup>269</sup> GONZÁLEZ, Hugo. Implementación y uso de un *core bancario* para banca retail en la tecnología *cloud computing*. Trabajo de grado de Magister en Gerencia de Tecnología de la información, Quito: Pontificia Universidad Católica de Ecuador. Maestría en Gerencia de Tecnología de la información. [en línea], mayo de 2015 Disponible en <<http://repositorio.puce.edu.ec/bitstream/handle/22000/8539/CASO%20DE%20ESTUDIO%20-%20Hugo%20Gonzalez.pdf?sequence=1>>, [citado el 12 de abril de 2017] pág. 28.

En el contrato de nube bancaria debe quedar la siguiente información del proveedor: domicilio, ubicación de sus centros de datos, ubicación del *software* utilizado, servidores subcontratados, etc. Además, resultaría esencial identificar a los subcontratados, estableciéndose con claridad los derechos sobre los datos y el uso de los mismos respecto del proveedor o sus posibles subcontratistas<sup>270</sup>.

La Ley Estatutaria 1581 de 2012 en el artículo 4<sup>271</sup>, consagra principios para la protección de los datos personales. A saber: principio de legalidad en materia de tratamiento de datos, principio de finalidad, principio de libertad, principio de veracidad o calidad, principio de transparencia, principio de acceso y circulación restringida, principio de seguridad y principio de confidencialidad que deberían estar incorporados en los contratos de nube bancaria en Colombia.

Los proveedores nube como *Google* y las entidades bancarias dentro de los contratos deben estipular una cláusula referida al control de la información, ya sea mediante la elaboración de Códigos de Ética que vinculen estos contratos y que tengan como objetivo evitar el reporte de información falsa.

La sostenibilidad del proveedor tiene que estar garantizada, ante fusiones, quiebras, cualquier cambio y, por tanto, se debe establecer un compromiso de continuidad a largo plazo en los propios términos del contrato<sup>272</sup>.

El proveedor debe obligarse a establecer un procedimiento con el fin de sistematizar la realización de copias de seguridad, identificando qué datos las requieren y su

---

<sup>270</sup>PÉREZ, Lorena. ¿Es confiable el cloud computing? [en línea] 17 de marzo de 2016. Disponible en <<https://lorenaperezcampillo.com/2016/03/17/es-fiabile-el-cloud-computing/>> [citado el 10 de abril de 2017]

<sup>271</sup> COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 de 2012 (octubre 17 de 2012) por la cual se dictan disposiciones generales para la protección de datos personales, Diario Oficial. Bogotá, D.C., 2012, art 4.

<sup>272</sup>JIMENEZ, Edwin. Modelo de Tarificación Software como Servicio Saas. Trabajo de grado de Magíster en ciencias de la información y las comunicaciones. Bogotá: Universidad Distrital Francisco José de Caldas. Facultad de Ingeniería. Maestría en ciencias de la información y las Comunicaciones, [en línea] 2015. Disponible en <http://repository.udistrital.edu.co/bitstream/11349/2765/1/JimenezGarzonEdwinAlfonso2015.pdf>, [citado el 24 de abril de 2017],pág. 35.

frecuencia, para ubicar estas copias de seguridad en un establecimiento diferente de la información original y así, evitar riesgos como la fuga o pérdida de datos<sup>273</sup>.

En las obligaciones del contrato estipular: presentar y solicitar auditorías y certificación de los sistemas de seguridad de los proveedores<sup>274</sup>, pues, el banco es el responsable ante los incumplimientos que ocurrieran y provocaran pérdida de datos o de disponibilidad. En ese sentido, es importante que el banco pueda auditar los sistemas y procedimientos del proveedor<sup>275</sup>.

En el contrato se debe dejar clara la obligación del proveedor y banco de notificar a las autoridades (Superintendencia de Industria y Comercio) de toda vulneración importante de la seguridad en la protección de datos<sup>276</sup>.

El proveedor de nube se debe obligar a proporcionar mecanismos eficientes para la generación de claves, el almacenamiento y la destrucción de la información<sup>277</sup>.

Además, definir mediante un documento escrito, la destrucción de los datos antes de que los medios de almacenamiento sean eliminados de la infraestructura, así como la política de copias de seguridad<sup>278</sup>.

---

<sup>273</sup> TIEMBLO, Alexandra. Seguridad y Cumplimiento Normativo en el Cloud Computing. Trabajo de grado para optar por el título de ingeniero Informático. Madrid: Universidad Carlos III de Madrid, [en línea] 15 de junio de 2012. Disponible en < [http://e-archivo.uc3m.es/bitstream/handle/10016/16232/tfg\\_alexandra\\_tiemblo\\_moreno\\_2012.pdf?sequence=1](http://e-archivo.uc3m.es/bitstream/handle/10016/16232/tfg_alexandra_tiemblo_moreno_2012.pdf?sequence=1)>, [citado el 12 de abril de 2017] página24.

<sup>274</sup>EUROPA. PARLAMENTO EUROPEO. Dirección general de políticas interiores. Departamento temático, política, economía y científica. Computación en la nube, [en línea] mayo de 2012. Disponible en <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO\\_ET\(2012\)475104\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf)>, [citado el 15 de abril de 2017], pág. 103

<sup>275</sup> TORO, Cristian, MURCIA, Johan y HERNÁNDEZ, Marien. Guía de auditoría para evaluar el aseguramiento de la disponibilidad de la información en un ambiente cloud computing IAAS, bajo la norma ISO 27001 de 2013. Trabajo de grado de especialistas en auditoría de sistemas de información, Bogotá: Universidad Católica de Colombia, Facultad de Ingeniería, Especialización en Auditoría de Sistemas de Información, [en línea], 2014. Disponible en <<http://repository.ucatolica.edu.co/bitstream/10983/1751/1/TRABAJO%20GRADO%20CLOUD%20COMPUTING%20IAAS.pdf>>, [citado el 11 de abril de 2017], pág. 45.

<sup>276</sup>EUROPA. PARLAMENTO EUROPEO. Dirección general de políticas interiores. Departamento temático, política, economía y científica. Computación en la nube, [en línea] mayo de 2012. Disponible en <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO\\_ET\(2012\)475104\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf)>, [citado el 15 de abril de 2017], pág. 104.

<sup>277</sup> INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN. (INTECO). Riesgos y amenazas en Cloud Computing. España: [en línea] marzo de 2011 Disponible en <[https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_riesgos\\_y\\_amenazas\\_en\\_cloud\\_computing.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf)>, [citado el 12 de abril de 2017], pág. 15

<sup>278</sup> Ibidem, pág. 15.

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<sup>279</sup>.

La adquisición de pólizas de cumplimiento, sobre todo, en el supuesto de que el contratista *cloud* se encuentre en otras jurisdicciones<sup>280</sup>.

Que las partes se obliguen a establecer medidas de seguridad con sus trabajadores, como controles previos al inicio de la relación laboral: identidad, nacionalidad, referencias de empleo, antecedentes, cláusula de confidencialidad, asunción de responsabilidades, aceptación del manual de seguridad; durante la vigencia de la relación laboral la política de seguridad para el personal debe contener: asignación y administración de responsabilidades, capacitación de manejo de datos, reporte de incidencias, información de cambios de las normas de seguridad, planes de formación y concienciación, campañas de mentalización, perfiles de usuarios y política de control de accesos y manuales de seguridad, los cuales deben ser claros, concisos y permanentemente actualizados, y tras la conclusión de la relación: revocación de los derechos de acceso a los datos, cambios de claves y la persistencia de responsabilidades legales<sup>281</sup>.

Evitar enviar información a países que no ofrezcan un adecuado tratamiento de datos, según los parámetros establecidos por la legislación colombiana.

---

<sup>279</sup> MORENO, GONZALO. Jurisdicción aplicable en materia de datos personales en los contratos de cloud computing: análisis bajo la legislación colombiana. Universidad de los Andes, Facultad de Derecho. Revista de Derecho, Comunicaciones y Nuevas Tecnologías. N°9 junio de 2013. ISSN 1909-7786, pág. 15.

<sup>280</sup> Ibidem, pág. 15.

<sup>281</sup> TIEMBLO, Alexandra. Seguridad y Cumplimiento Normativo en el Cloud Computing. Trabajo de grado para optar por el título de ingeniero Informático. Madrid: Universidad Carlos III de Madrid, [en línea] 15 de junio de 2012. Disponible en < [http://e-archivo.uc3m.es/bitstream/handle/10016/16232/tfg\\_alexandra\\_tiembre\\_moreno\\_2012.pdf?sequence=1](http://e-archivo.uc3m.es/bitstream/handle/10016/16232/tfg_alexandra_tiembre_moreno_2012.pdf?sequence=1)>, [citado el 12 de abril de 2017], pág. 22

Además, para mejorar en la elaboración del contrato se debe investigar sobre las experiencias, el comportamiento y la percepción del riesgo de los usuarios<sup>282</sup>.

Se deben crear reglas corporativas vinculantes, códigos de buenas prácticas de manera voluntaria, para asegurar las transferencias de datos personales entre empresas<sup>283 284</sup>.

El proveedor debe fomentar en las instituciones financieras una cultura de riesgos que involucre a toda la organización, intentando conseguir así, un eficiente y completo tratamiento de datos<sup>285</sup>.

También se deben desarrollar sistemas de intercambio de recursos y conocimientos en nube, para enseñar e intercambiar buenas prácticas por medio de foros, seminarios en línea y otros instrumentos de colaboración en nube<sup>286</sup>.

Que los controladores y los procesadores se obliguen a demostrar permanentemente que han adoptado todas las medidas para garantizar el cumplimiento de todas las normas y principios de protección de datos<sup>287</sup>.

---

<sup>282</sup>EUROPA. PARLAMENTO EUROPEO. Dirección general de políticas interiores. Departamento temático, política, economía y científica. Computación en la nube, [en línea] mayo de 2012. Disponible en <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO\\_ET\(2012\)475104\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf)>, [citado el 15 de abril de 2017], pág. 105

<sup>283</sup>GUASCH, Vicente, SOLER José. Cloud computing: cláusulas contractuales y reglas corporativas vinculantes. RDUNED. EN Revista de derecho UNED, ISSN 1886-9912, n. 14, [en línea] 2014. Disponible en <<http://revistas.uned.es/index.php/RDUNED/article/view/13300/12171>>, [citado el 22 de abril de 2017], pág. 265

<sup>284</sup> Los proveedores y bancos deben invertir en responsabilidad corporativa, realizar códigos de ética y prever los riesgos que generan la vulneración de los derechos de sus usuarios, puede tomar como referente: los Principios Rectores sobre las Empresas y los Derechos Humanos, redactados por el profesor de Harvard, John Ruggie, que ofrecen una guía muy útil sobre las obligaciones de los Estados y las empresas.

<sup>285</sup>SALIDO, Ruben, RODRIGUEZ, Mario y ARRANZ, ÁLVARO, Innovación y Multicanalidad en Banca. “La amenaza de las “FinTech Start Up,s”, Colegio Universitario de Estudios Financieros CUNEF, 2014-2015, [en línea] Disponible en <[http://biblioteca.cunef.edu/gestion/catalogo/doc\\_num.php?explnum\\_id=1360](http://biblioteca.cunef.edu/gestion/catalogo/doc_num.php?explnum_id=1360)>, [citado el 14 de abril de 2017] pág. 107

<sup>286</sup>EUROPA. PARLAMENTO EUROPEO. Dirección general de políticas interiores. Departamento temático, política, economía y científica. Computación en la nube, [en línea] mayo de 2012. Disponible en <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO\\_ET\(2012\)475104\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf)>, [citado el 15 de abril de 2017], pág. 105

<sup>287</sup> Ibidem, pág. 71

Que las entidades asuman la responsabilidad de la información que se recoge y que esté la obligación de rendir cuentas sobre la protección de la base de datos<sup>288</sup>.

Quizás las entidades financieras pueden encriptar la información antes de que se almacenen en un servicio de datos en nube, para reducir en gran medida la probabilidad de riesgo de dichos datos<sup>289</sup>.

El banco debe asegurarse de tener canales de comunicación, conexión de internet para el almacenamiento en la nube, para asegurar un buen nivel de servicio hacia su organización<sup>290</sup>.

Estipular en el contrato o por documento separado, la cláusula compromisoria, para que, cualquier controversia jurídica entre el proveedor y el banco se solucione a través del arbitraje.

---

<sup>288</sup> Ibidem, pág. 72

<sup>289</sup> Ibidem, pág. 69

<sup>290</sup> GONZÁLEZ, Hugo. Implementación y uso de un *core bancario* para banca retail en la tecnología *cloud computing*. Trabajo de grado de Magister en Gerencia de Tecnología de la información, Quito: Pontificia Universidad Católica de Ecuador. Maestría en Gerencia de Tecnología de la información. [en línea], mayo de 2015. Disponible en <<http://repositorio.puce.edu.ec/bitstream/handle/22000/8539/CASO%20DE%20ESTUDIO%20-%20Hugo%20Gonzalez.pdf?sequence=1>>, [citado el 12 de abril de 2017] páginas 28 y 29.

## **5. LA RESOLUCIÓN DE LOS CONFLICTOS DE HÁBEAS DATA EN EL *CLOUD BANKING* Y LA COMPETENCIA DEL ARBITRAJE EN DERECHO.**

En relación con los conflictos que pueden surgir con el almacenamiento de información en la nube, Martin Pablo Silva<sup>291</sup> argumenta que en el *Cloud Computing* hay incertidumbre en los usuarios para iniciar procesos judiciales, por lo cual es necesario un sistema de arbitraje internacional y cláusulas arbitrales compulsivas que aporten mejoras significativas en los conflictos planteados. Por consiguiente, los sistemas arbitrales permitirán que la internacionalidad genere menos conflictos respecto a la jurisdicción y el derecho aplicable para que los consumidores tengan acceso a la justicia.

Adicionalmente, propone un sistema de arbitraje común para que se unifique la multiplicidad de jurisdicciones; manejado por un organismo internacional del cual participen todos los Estados, como puede ser la Organización de Naciones Unidas ONU o la Organización Mundial del Comercio OMC, un sistema que contaría con un amplio plantel especializado de árbitros alrededor del mundo, lo cual contribuiría a la imparcialidad del laudo final, debido a que, la globalización atraviesa cada vez más los planos sociales y es inevitable recurrir a organizaciones internacionales para reubicar los roles de los Estados a fin de regular las relaciones de una forma efectiva y eficiente<sup>292</sup>.

Lo anterior, porque el arbitraje permite que quienes decidan sean especialistas en el tema, dependiendo de la materia del contrato, teniendo en cuenta que no es lo mismo un contrato de *Cloud Computing* sobre recursos financieros que sobre correo electrónico o almacenamiento de archivos personales. Por lo cual, en estos contratos se evitaría la especulación e incertidumbre al asegurarse que el sistema

---

<sup>291</sup> SILVA, Martín. El arbitraje y los contratos de adhesión en el Cloud Computing: una solución a los abusos en las relaciones asimétricas. Derecho, nuevas tecnologías, arte y otras yerbas. [en línea], 22 de junio de 2013. Disponible en< <http://derecho-e-internet.blogspot.com.co/2013/07/el-arbitraje-y-los-contratos-de.html>> [citado el 15 de abril de 2017]

<sup>292</sup> Ibidem.

que resuelva los problemas sea de fácil acceso y respetuoso de las normas que defienden al consumidor<sup>293</sup>. Esta es una idea que corrobora para los contratos de nube Lorena Pérez<sup>294</sup>, al indicar: *“son aconsejables las medidas alternativas de resolución de conflictos como la mediación o el arbitraje para desatascar a tribunales con vacíos normativos nacionales”*.

Además, al solucionar estas controversias mediante el arbitraje se van a beneficiar terceros, ya que de los conflictos contractuales entre el proveedor y la entidad financiera se deriva la afectación del habeas data de los clientes del banco y, por tanto, con este mecanismo se asegura que sean profesionales expertos en derecho civil, comercial, financiero y de telecomunicaciones quienes, con celeridad, neutralidad, confidencialidad profieren un laudo en derecho

## 5.1 EJEMPLO DE RESOLUCIONES INTERNACIONALES.

El presente ejemplo no involucra directamente un conflicto jurídico relacionado con el habeas data, como resultado de un contrato entre el proveedor y una entidad, pero sí evidencia un conflicto: infracción de derechos de propiedad intelectual que, surge por el hecho de almacenar información en la nube:

Viacom Intern, Inc<sup>295</sup>. vs. YouTube<sup>296</sup>: es un ejemplo respecto de la responsabilidad de un proveedor de servicios de nube en cuanto el almacenamiento y gestión de contenidos digitales<sup>297</sup>.

---

<sup>293</sup> ibidem

<sup>294</sup> PÉREZ, Lorena. ¿Es confiable el cloud computing? [en línea] 17 de marzo de 2016. Disponible en <<https://lorenaperezcampillo.com/2016/03/17/es-fiable-el-cloud-computing/>> [citado el 10 de abril de 2017]

<sup>295</sup> Viacom es el hogar de las principales marcas de entretenimiento del mundo que se conectan con el público a través de contenido atractivo a través de televisión, cine, Plataformas online y móviles en más de 160 países y territorios. Ver al respecto <http://www.viacom.com/pages/default.aspx>.

<sup>296</sup> Fue a inicios de 2005 cuando tres ex-empleados de la gran empresa internauta Paypal, Chad Hurley, Steve Chen y Jawed Karim, crearon un contenido que aparecía en forma de montajes de fotografías, cortes de televisión, vídeos musicales o clips de películas: YouTube, un invento que en el 2006 fue adquirido por Google, tras el pago de 1.650 millones de dólares en acciones. Ver al respecto <http://tendenciasweb.about.com/od/videos-y-fotos/a/La-Historia-De-Youtube.htm>

<sup>297</sup> GUASCH, Vicente, SOLER José. Cloud computing: cláusulas contractuales y reglas corporativas vinculantes. RDUNED. EN Revista de derecho UNED, ISSN 1886-9912, n. 14, [en línea] 2014. Disponible en <<http://revistas.uned.es/index.php/RDUNED/article/view/13300/12171>>, [citado el 22 de abril de 2017], pág. 240.

## **CASO**

YouTube reproducía y almacenaba obras a través de la página de internet *www.youtube.com*, sin autorización de sus titulares.

## **PRETENSIÓN.**

Viacom pretendía que se declarase la responsabilidad directa e indirecta de YouTube (de Google) por la infracción de derechos de propiedad intelectual, por la reproducción y almacenamiento de obras a través de la página de internet *www.youtube.com*, sin autorización de los titulares<sup>298</sup>.

## **CONTRATO DE YOUTUBE (de Google).**

YouTube es una empresa que permitía al usuario ver, cargar y compartir sus videos personales mediante una página de internet, luego del registro del usuario en el sitio web, en el que acepta las condiciones determinadas para el uso de la plataforma, entre las que se encuentra no infringir derechos de autor de terceros<sup>299</sup>

## **RESUELVE.**

En este caso, el Tribunal debía resolver si la conducta de *YouTube* estaba conforme a la excepción de responsabilidad dispuesta en Ley de Copyright de los Estados Unidos, que se refería a la ausencia de responsabilidad por parte del proveedor de servicios *YouTube*, cuando no tiene conocimiento de la infracción y al tenerlo toma las medidas necesarias para evitar que la infracción continúe cometiendo. Así, El Tribunal sostuvo que efectivamente *YouTube* era un proveedor de servicios que encontraba limitada su responsabilidad por lo dispuesto en la excepción de la Ley

---

<sup>298</sup> Ibidem, págs. 240 y 241.

<sup>299</sup> Ibidem, págs. 240 y 241.

de Copyright, en tanto que su actividad se circunscribe a las condiciones expuestas en la norma. En otra instancia, la Corte de Apelaciones del Segundo Circuito confirmó la decisión del Tribunal<sup>300</sup>.

Es decir, el Tribunal tomó la decisión según el contrato de *YouTube*, en el cual, el usuario acepta las condiciones determinadas para el uso de la plataforma, como no infringir derechos de autor de terceros, entendiéndose la presunción de que *YouTube* no tenía conocimiento de la infracción a la propiedad intelectual que se podría estar presentando.

## **5.2 EJEMPLO DE LAUDO ARBITRAL EN COLOMBIA.**

De los 742 laudos encontrados en la página de la Cámara de Comercio de Bogotá, sólo 1 se refiere a la computación en la nube, y contiene lo siguiente:

Datapoint de Colombia S.A.S Vs Comercializadora de Software Extensión de Colombia S.A.

### **CLÁUSULA COMPROMISORIA.**

*“CLÁUSULA UNDÉCIMA - RESOLUCIÓN DE CONFLICTOS: Toda controversia o diferencia relativa a este Contrato que resulten de su ejecución con excepción del cobro ejecutivo de obligaciones, se resolverá por un Tribunal de Arbitramento (el “Tribunal”), que se regirá por lo dispuesto en el Decreto 1818 de 1998 y demás normas vigentes que lo modifiquen o complementen, conforme a las siguientes reglas: 1. - El Tribunal estará integrado por tres árbitros designados de común acuerdo por las partes. A falta de acuerdo, total parcial, el o los árbitros respecto de los cuales no haya habido consenso será (n) designado (s) por el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá, a solicitud de cualquiera de las partes. 2. El Tribunal funcionará en el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá. 3. - El Tribunal decidirá”<sup>301</sup>.*

---

<sup>300</sup> Ibidem, págs. 240 y 241.

<sup>301</sup> COLOMBIA, TRIBUNAL ARBITRAL. Datapoint de Colombia S.A.S Vs Comercializadora de Software Extensión de Colombia S.A (16 de octubre de 2014). Árbitros: Luis Augusto Cangrejo Cobos, Marcel Tangarife Torres y Gustavo Suárez Camacho.

## CASO.

- El 15 de febrero de 2012, Extensión y Datapoint suscribieron un contrato, cuyo objeto fue la implantación, puesta en funcionamiento, capacitación y consultoría de una solución basada en la solución BMC Cloud LifeCycle Management y la provisión de escritorios virtuales por parte de Extensión. Contrato que fue varias veces modificado por las partes.
- Conforme a lo acordado entre las partes, Extensión celebró un contrato de seguro con la compañía Suramericana de Seguros S.A, para expedir la póliza de cumplimiento entre particulares.
- Mediante informe de Evaluación de Proyecto, Datapoint revisó el estado de la prestación y las inconsistencias respecto de los siguientes servicios: Portal de Servicios CLM, aprovisionamiento, monitoreo, seguridad, consola, integraciones, automatización, compatibilidad y administración.
- Desde el 12 de septiembre de 2012, Jorge Eduardo Gómez, Gerente de Datapoint, cerró el acceso de Extensión a las plataformas y servidores de aquél, particularmente los utilizados para la implementación de la nube.
- El 14 de septiembre terminó el Contrato de Servicios por decisión unilateral de Datapoint, por vencimiento de su plazo contractual, según la ampliación del cronograma concedida el 31 de julio del 2012<sup>302</sup>.

---

<sup>302</sup> Ibidem. Páginas 12, 18, 43

## PRETENSIONES

Entre las pretensiones se encuentran:

- *DECLARAR que entre DATAPOINT Y EXTENSIÓN, se celebró un Contrato de Prestación de Servicios y venta de software y equipos cuyo objeto era "(...) la implantación, puesta en funcionamiento, capacitación y consultoría de una solución basada en la solución BMC Cloud Lifecycle management provisión de escritorios virtuales (...)"*.
- *DECLARAR que el contrato de prestación de servicios celebrado entre DATAPOINT Y EXTENSIÓN, se terminó por vencimiento del plazo contractual.*
- *DECLARAR que la sociedad EXTENSION, incumplió el Contrato de prestación de servicios y venta de equipos y software.*
- *DECLARAR que como consecuencia del anterior el incumplimiento ha causado graves perjuicios a la Sociedad Convocante DATAPOINT.*
- *CONDENAR a EXTENSIÓN a pagar a favor de DATAPOINT las sumas que resulten probadas con respecto al daño emergente y el lucro cesante en los términos de Ley.*
- *Que se ORDENE que la totalidad de las condenas deberán ser pagadas dentro de los diez días (10) siguientes a la fecha en la cual quede ejecutoriado el Laudo, de forma indexada y actualizada, en los términos del artículo 16 de la ley 446 de 1998.*
- *CONDENAR en forma directa a SURAMERICANA DE SEGUROS S.A. al pago de las indemnizaciones a que hubiere lugar a favor de DATAPOINT hasta el monto de la cobertura constituida en la póliza de seguro.*
- *CONDENAR a la parte convocada a pagar las costas y las agencias en derecho que genere este proceso<sup>303</sup>.*

## SERVICIOS.

Implantación, puesta en funcionamiento, capacitación y consultoría de una solución basada en la solución BMC Cloud LifeCycle Management y la provisión de escritorios virtuales por parte de Extensión.

---

<sup>303</sup> Ibidem, páginas 5 y 6.

## LA CALIFICACIÓN DEL CONTRATO.

El contrato fue denominado por las partes como de “servicios”. Pero el Tribunal arbitral definió cuál era la calificación jurídica del contrato para establecer el régimen jurídico pertinente.

Desde el punto de vista doctrinal, tratándose de contratos cuyo propósito consiste en contratar una persona por su trabajo profesional, es necesario distinguir entre los contratos de obra o de arrendamiento de obra frente a los contratos de servicios o de arrendamiento de servicios inmateriales.

Así, se ha considerado que los contratos de servicios son aquellos que compromete una actividad profesional e involucra una obligación intangible de hacer, que se agota con su mismo consumo. Estos contratos se caracterizan por cuanto el contratista es un individuo quien tiene determinadas habilidades profesionales que suministra a su contratante a fin de conseguir un objetivo<sup>304</sup>.

De tal forma, el Tribunal considera que se enmarca en un contrato de prestación de servicios. En este caso, correspondía a Extensión como contratista de Datapoint, brindar asesoría profesional para las labores de instalación, configuración y puesta en marcha de la solución de nube.

Por otra parte, para el Tribunal, el Contrato se asimila a los que internacionalmente se han denominado “contratos de ingeniería”, pues, los profesionales en ingeniería prestan servicios para la elaboración de estudios o el diseño de proyectos y su ejecución.<sup>305</sup>

---

<sup>304</sup> Ibidem.

<sup>305</sup> Ibidem.

## RESUELVE

El Tribunal arbitral consideró que no hay duda de la existencia del contrato celebrado entre las partes, pero la conducta adelantada por Datapoint de dar por terminado unilateral y anticipadamente el contrato, y de impedir el acceso de Extensión a las instalaciones, corresponde a una conducta que se puede considerar dentro del abuso del derecho. Aunque, Extensión tampoco se encontraba en estricto cumplimiento de las obligaciones a su cargo, y tampoco razonablemente podría haber culminado a plenitud los servicios contratados dado el reducido término acordado.

Respecto a la responsabilidad por incumplimiento, según la doctrina ha de reunirse los presupuestos axiológicos que la identifican, así:

*“(i) un contrato válidamente celebrado; (ii) el incumplimiento de las obligaciones por alguna de las partes; (iii) el daño; y (iv) la atribución o relación de causalidad entre el incumplimiento y el daño, a la parte incumplida. Además, ha de recordarse que el daño, como requisito sine quo para derivar la obligación de su indemnización, debe ser cierto, de contenido patrimonial y probado”.*

Sin embargo, señaló el Tribunal que la ley colombiana no establece la distinción entre obligaciones de medio y de resultado. Por tal razón, para esclarecer la naturaleza de las obligaciones derivadas del Contrato, se debe recurrir a las cláusulas estipulaciones por las partes. Por tanto, el Tribunal estima que, según el contrato y la propuesta técnica, la obligación del servicio de Extensión era de medios en lo que respecta a las características y el funcionamiento de la solución de nube, y que su única obligación de resultado era efectivamente instalar y configurar el software suministrado por Datapoint.

De ahí que, según el acervo probatorio el Tribunal determinó: Declarar el incumplimiento del Contrato de Prestación de Servicios celebrado entre las partes únicamente en lo relativo a la elaboración de las listas de chequeo para la

aceptación de las soluciones durante la fase de ejecución del Contrato, circunstancia que no constituye un incumplimiento grave y que dentro de lo justo, equitativo y jurídico han de reconocerse los trabajos o labores hasta entonces realizados por Extensión.<sup>306</sup>

### 5.3 LA COMPETENCIA DEL ÁRBITRO.

Según el Reglamento del Colegio Profesional de Ingenieros Informáticos de la Comunidad de Madrid CPIICM, en lo que respecta al ámbito de la Ingeniería en Informática, los jueces y Tribunales tienen un evidente desconocimiento de las cuestiones técnicas que se plasman en los contratos desarrollados y firmados por las partes, consecuencia de que algunas resoluciones no correspondan con el verdadero espíritu que se quería reflejar en los documentos suscritos por las partes<sup>307</sup>.

Empero, en Colombia, la Constitución Política de 1991, artículo 116, consagra que los particulares pueden ser investidos transitoriamente de la función de administrar justicia en la condición de árbitros habilitados por las partes para proferir fallos en derecho o en equidad, en los términos que determine la ley<sup>308</sup>.

Según el principio *kompetenz-kompetenz*, el árbitro tiene el poder para decidir sobre su propia competencia, como uno de los fundamentos de la práctica arbitral moderna, en lo cual es pertinente mencionar el artículo 16 de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional-UNCITRAL, a través del cual adopta oficialmente este principio, estableciendo que “*el tribunal arbitral puede decidir acerca de su propia competencia, incluso sobre las excepciones relativas a*

---

<sup>306</sup> Ibidem.

<sup>307</sup> COLEGIO PROFESIONAL DE INGENIEROS EN INFORMÁTICA DE LA COMUNIDAD DE MADRID CPIICM. Reglamento de la Corte de Arbitraje (8 de junio de 2016). [en línea] Disponible en <http://cpiicm.es/wp-content/uploads/sites/3/2016/06/Reglamento-Corte-Arbitral-CPIICM.pdf> [citado el 06 de marzo de 2017]., pág. 3.

<sup>308</sup> COLOMBIA, CONSTITUCIÓN POLÍTICA DE 1991, Artículo 116.

*la existencia o a la validez del acuerdo de arbitraje*<sup>309</sup>. Por lo anterior, los árbitros tienen la potestad, legalmente conferida, de determinar si tiene competencia para conocer de una determinada pretensión relativa a una disputa entre las partes, en virtud del pacto arbitral que le ha dado fundamento<sup>310</sup>.

Por otro lado, de conformidad con la Ley 1563 de 2012, el pacto arbitral es un negocio jurídico por medio del cual las partes se obligan a someter a arbitraje controversias que surjan entre ellas, renunciando a hacer valer sus pretensiones ante los jueces ordinarios. Este pacto arbitral puede consistir en un compromiso o en una cláusula compromisoria.

Para el abogado César Quijano<sup>311</sup> el primer criterio que debe determinar el árbitro para saber si tiene competencia es:

*La manifestación inequívoca de las partes de acudir ante el arbitraje como una forma de solucionar sus diferencias, “principio de habilitación” ya sea porque se encuentra dicha manifestación en una cláusula compromisoria o en un contrato de compromiso.*

*Hay un momento en el trámite arbitral especial para esto, que es en la primera audiencia, en el primer auto se decreta si los árbitros son competentes para conocer del asunto; según la manifestación de las partes de acudir ante un tribunal de arbitramento para resolver sus diferencias.*

Como segundo criterio para definir la competencia plantea:

*Los límites materiales de los mecanismos alternativos de solución de conflictos, que según la doctrina, la ley y la jurisprudencia se refieren a que serán solucionados mediante el arbitraje aquellos conflictos susceptibles de transacción. Entonces, hay algunas diferencias que no pueden ser puestas a consideración de un tribunal, a modo de ejemplo, temas asociados a asuntos laborales, porque se trata de derechos mínimos e irrenunciables sobre los cuales no puede haber transacción, o*

---

<sup>309</sup> COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL UNCITRAL. Ley modelo de la CNUDMI sobre arbitraje comercial – internacional. Nueva York, [en línea] 2008. Disponible en <[https://www.uncitral.org/pdf/spanish/texts/arbitration/ml-arb/07-87001\\_Ebook.pdf](https://www.uncitral.org/pdf/spanish/texts/arbitration/ml-arb/07-87001_Ebook.pdf)> [citado el 7 de febrero de 2017] pág. 25.

<sup>310</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia SU174 del 2007, (14 de marzo de 2007). M.P Manuel José Cepeda Espinosa.

<sup>311</sup> QUIJANO, César abogado quien se ha desempeñado como árbitro de la Cámara de Comercio de Bucaramanga. Bucaramanga, 26 de abril de 2017.

*decretar la anulación de un acto administrativo, esa competencia recae exclusivamente sobre los jueces administrativos<sup>312</sup>.*

Finalmente, sobre la competencia del árbitro concluye:

*Esos dos criterios los debe tener en cuenta el árbitro: si las partes manifestaron inequívocamente que quieren acudir a un tribunal de arbitramento para dirimir sus controversias, y segundo, que el conflicto que van a conocer sea susceptible de ser tratado a través de una figura como el arbitraje<sup>313</sup>.*

De acuerdo a la anterior argumentación, Google y la entidad financiera deben manifestar su interés de recurrir al tribunal arbitral mediante la cláusula compromisoria o el contrato de compromiso, y el árbitro, además de analizar la habilitación de estas partes podrá definir que es competente ante el análisis del segundo criterio, pues los conflictos jurídicos del *cloud banking* anteriormente mencionados, son susceptibles de transacción.

En relación al conocimiento del árbitro sobre los contratos de computación en la nube, el abogado César Quijano afirma:

*Es importante precisar que cuando árbitro es designado, eventualmente puede no aceptar ante la posibilidad de un conflicto de intereses, de impedimento con alguna de las partes o porque tiene varios casos pendientes. Pero no alegando falta de conocimiento en el tema, pues las listas de árbitros estén distribuidas por especialidades, una de las bondades que tiene este mecanismo<sup>314</sup>.*

#### **5.4 LA CLÁUSULA COMPROMISORIA.**

La cláusula compromisoria, podrá formar parte de un contrato o constar en documento separado con el nombre de las partes y la indicación precisa del contrato

---

<sup>312</sup> Ibidem

<sup>313</sup> Ibidem.

<sup>314</sup> Ibidem.

a que se refiere. La inexistencia, ineficacia o invalidez del contrato no afecta esta cláusula<sup>315</sup>.

Ejemplo de la cláusula en Arbitraje Nacional<sup>316</sup>:

*Toda controversia o diferencia relativa a este contrato se resolverá por un Tribunal Arbitral que sesionará en el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bucaramanga, de acuerdo con las siguientes reglas:*

- 1. El Tribunal estará integrado por: 3 árbitros designados por las partes de común acuerdo. En caso de que no sea posible, los árbitros serán designados por el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bucaramanga, a solicitud de cualquiera de las partes.*
- 2. El procedimiento aplicable será el del Reglamento para Arbitraje Nacional del Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bucaramanga.*
- 3. El Tribunal decidirá en derecho.*

Ejemplo de Cláusula en Arbitraje Internacional<sup>317</sup>:

*Toda disputa relativa a este contrato o que derive del mismo, se resolverá por un tribunal arbitral que funcionará en el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá, de conformidad con las siguientes reglas:*

- 1. El tribunal se sujetará al Reglamento de Arbitraje Comercial Internacional del Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá.*
- 2. El tribunal estará integrado por tres árbitros designados por las partes. En caso de que no fuere posible, los árbitros serán designados por el Centro a solicitud de cualquiera de las partes.*
- 3. El tribunal decidirá en derecho.*
- 4. El idioma del arbitraje será español. La sede del arbitraje será en Chapinero (Calle 67 nro. 8-32).*
- 5. La legislación española será la aplicable para la solución de la controversia.*

La anterior cláusula, soluciona las controversias relacionadas con la jurisdicción competente y ley aplicable, ante cualquier conflicto jurídico que se presente por el contrato de computación bancaria, celebrado entre Google y la entidad financiera.

---

<sup>315</sup> COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1563 de 2012” Por medio de la cual se expide el Estatuto de Arbitraje Nacional e Internacional y se dictan otras disposiciones”. Diario Oficial. Bogotá, D.C., 2012, artículos 4 y 5.

<sup>316</sup> CÁMARA DE COMERCIO DE BOGOTÁ, Cláusulas compromisorias, [en línea]. Disponible en <<http://www.centroarbitrajeconciliacion.com/Servicios/Arbitraje/Clausulas-compromisorias>> [citado el 25 de abril de 2017]

<sup>317</sup> Ibidem.

## **5.5 EI COMPROMISO.**

El profesor Hernando Morales Molina distinguía el compromiso como aquel contrato por el que dos o más personas someten la decisión de una cuestión jurídica a particulares llamados árbitros<sup>318</sup>.

El compromiso podrá constar en cualquier documento, que contenga:

1. Los nombres de las partes.
2. La indicación de las controversias que se someten al arbitraje.
3. La indicación del proceso en curso, cuando a ello hubiere lugar<sup>319</sup>.

## **5.6 LAUDO EN DERECHO.**

Al involucrar los contratos de computación bancaria, es posible imaginarse que la controversia debe ser resuelta por árbitros expertos en informática para proferir un laudo técnico, pero la presente investigación plantea un laudo en derecho por la siguiente razón:

Según la Corte Constitucional el arbitraje técnico, no puede referirse a divergencias de índole jurídica derivadas de la estipulación y ejecución de un contrato, ni a su incumplimiento, ni a la definición de responsabilidad derivada de éste. Al calificar de técnico un tribunal de arbitramento, la ley restringe el sentido genérico del arbitraje a ese campo; de modo que un tribunal técnico profiere decisiones técnicas, lo que exige que lo integren técnicos, ingenieros, más no necesariamente abogados<sup>320</sup>.

---

<sup>318</sup> MORALES, Molina, Hernando. Curso de derecho procesal civil. Parte general. 4ª edición. Lerner. 1960. Pág. 51.

<sup>319</sup> COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1563 de 2012" Por medio de la cual se expide el Estatuto de Arbitraje Nacional e Internacional y se dictan otras disposiciones". Diario Oficial. Bogotá, D.C., 2012.

<sup>320</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-330 de 2012. (9 de mayo de 2012). M.P Humberto Antonio Sierra Porto.

Incluso, el arbitramento técnico difiere sustancialmente del arbitraje en derecho, por cuanto se busca dirimir divergencias de índole jurídica derivadas de la estipulación y ejecución de un contrato, su incumplimiento, o la definición de responsabilidad; en cambio, el arbitraje técnico tiende a dirimir cuestiones objetivas y de hecho referentes al cumplimiento y ejecución física de la obra, en lo atinente a las operaciones necesarias para la realización de las obligaciones resultantes de lo estipulado contractualmente<sup>321</sup>.

Para el abogado César Quijano<sup>322</sup>:

*Cuando hay un conflicto que su expresión básica se refiera a una diferencia entre dos o más personas, este puede tener alcances distintos, digamos que las controversias que le interesan al arbitraje en derecho son los conflictos jurídicos, entonces, si bien la génesis del conflicto puede ser de naturaleza tecnológica, es decir, donde exista un alto componente técnico en la solución de la controversia, ello no impide para que se solucione en derecho alguna diferencia sobre ese particular, porque puede estar asociada a la ejecución, terminación, interpretación de un contrato. Obviamente el componente técnico se soluciona con la posibilidad de acceder a peritos o a dictámenes técnicos que le sirvan al árbitro para el sustento de la decisión.*

## **5.7 EL ARBITRAJE INTERNACIONAL.**

El arbitramento, tanto el nacional como el internacional, tiene su fundamento en la autonomía de la voluntad, como lo reconoce expresamente la Constitución. Pero el laudo que profiera el tribunal internacional debe someterse al procedimiento del *exequátur*<sup>323</sup>, procedimiento que garantiza el respeto al ordenamiento jurídico nacional. Porque si bien pueden los árbitros aplicar una legislación extranjera, no

---

<sup>321</sup> Ibidem.

<sup>322</sup> QUIJANO, César, abogado quien se ha desempeñado como árbitro de la Cámara de Comercio de Bucaramanga. Bucaramanga, 26 de abril de 2017.

<sup>323</sup> *Exequátur*: es decir, de la autorización judicial para darle efecto jurídico y asegurar el efectivo cumplimiento de las referidas sentencias, es resultado de un proceso judicial dentro del cual deben observarse las reglas propias del debido proceso desarrolladas por el legislador con arreglo al marco normativo superior que comprenden básicamente las siguientes fases: demanda en forma; admisión y traslado al demandado y demás intervinientes, contestación de la demanda, probatoria, de alegaciones y decisoria. Ver al respecto: COLOMBIA, CORTE CONSTITUCIONAL, Sentencia T-716 de 1996 (16 de diciembre de 1996) M.P Antonio Barrera Carbonell.

podrán quebrantar normas de orden público vigentes en Colombia, excepto las de procedimiento.<sup>324</sup>

De acuerdo con la Ley 1563 de 2012, artículo 62<sup>325</sup>, las disposiciones contenidas en esta normatividad se aplicarán al arbitraje internacional, sin perjuicio de cualquier tratado multilateral o bilateral vigente en Colombia.

Empero, se entiende que el arbitraje es internacional cuando:

- a) Las partes en un acuerdo de arbitraje tengan, al momento de la celebración de ese acuerdo, sus domicilios en Estados diferentes<sup>326</sup>; o*
- b) El lugar del cumplimiento de una parte sustancial de las obligaciones o el lugar con el cual el objeto del litigio tenga una relación más estrecha, está situado fuera del Estado en el cual las partes tienen sus domicilios<sup>327</sup>;*
- c) La controversia sometida a decisión arbitral afecte los intereses del comercio internacional<sup>328</sup>.*

**5.7.1 El domicilio de las partes:** Para establecer si las partes tienen domicilio en Estados diferentes se analizará lo siguiente:

Domicilio de Google	Operación de Google en Colombia
1600 Amphitheatre Parkway Mountain View, CA 94043	Cr11 A 94-45 Bogotá, Colombia

<sup>324</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C-347 de 1997, (23 de julio de 1997). M.P Jorge Arango Mejía.

<sup>325</sup> COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1563 de 2012<sup>7</sup> Por medio de la cual se expide el Estatuto de Arbitraje Nacional e Internacional y se dictan otras disposiciones<sup>7</sup>. Diario Oficial. Bogotá, D.C., 2012, artículo 62.

<sup>326</sup> Este escenario es basado en la Ley Modelo UNCITRAL, artículo 1(3)(a). Ver al respecto: GAVIRIA, Juan. Comentarios sobre las nuevas normas colombianas en materia de arbitraje internacional. EN Revista de Derecho Privado. Universidad Externado de Colombia. [en línea] 2013. Disponible en <<http://revistas.uexternado.edu.co/index.php/derpri/article/view/3487/3473>> [citado el 13 de abril de 2017].

<sup>327</sup> Este escenario es basado en Ley Modelo UNCITRAL, artículo 1(3)(b) (ii) Ver al respecto: GAVIRIA, Juan. Comentarios sobre las nuevas normas colombianas en materia de arbitraje internacional. EN Revista de Derecho Privado. Universidad Externado de Colombia. [en línea] 2013. Disponible en <<http://revistas.uexternado.edu.co/index.php/derpri/article/view/3487/3473>> [citado el 13 de abril de 2017].

<sup>328</sup> Este escenario es basado en la Ley 315 de 1996, artículo 1.5 (que fue derogada por la Ley 1563<sup>13</sup>) y no en la Ley Modelo UNCITRAL Ver al respecto GAVIRIA, Juan. Comentarios sobre las nuevas normas colombianas en materia de arbitraje internacional. EN Revista de Derecho Privado. Universidad Externado de Colombia. [en línea] 2013. Disponible en <<http://revistas.uexternado.edu.co/index.php/derpri/article/view/3487/3473>> [citado el 13 de abril de 2017]

Estados Unidos	
Domicilio de un banco	Sucursal del banco
Plaza San Nicolás 4 480005 Bilbao, Viscaya, España.	Cra. 8 #13-42, Bogotá, Cundinamarca

Obsérvese que, sobre esta distinción, la árbitra Claudia Benavides Galvis<sup>329</sup> en una conferencia sobre aspectos esenciales del arbitraje Internacional afirma:

*(...) La sucursal es un establecimiento de comercio que no tiene personería jurídica independiente; no es una entidad separada, o diferente a la casa matriz extranjera.*

*Cita Supersociedades: "(...) el hecho de atribuir a la sucursal una cierta autonomía operativa, para fines jurídicos, tributarios y contables, no desdibuja su naturaleza, como parte de una organización que por esta vía se descentraliza sin lograr una personificación nueva y distinta a la de la sociedad".*

*Cita Supersociedades: el domicilio social "es uno solo, sin perjuicio que la administración o dirección coincida con aquél, o que para el desarrollo de sus negocios sociales habrá uno o más establecimientos de comercio o sucursales, dentro o fuera del domicilio de la sociedad".*

*"El domicilio de la sociedad extranjera está ubicado fuera de Colombia, aunque tenga una sucursal en el país".*

Se deduce que probablemente el contrato de nube bancaria se realizó entre las sociedades matriz de Google y el banco; y, por lo tanto, sus domicilios principales serán el lugar de notificación de la demanda.

<sup>329</sup> BENAVIDES, Claudia, Conferencia ICC YAF Aspectos esenciales del arbitraje internacional, [en línea]. Disponible en <<http://www.camaramedellin.com.co/site/Portals/0/Documentos/memorias%20random/Conferencia%20ICC%20YAF%20-%20Claudia%20Benavides.pdf>> [citado el 18 de abril de 2017], pág. 5.

**5.7.2 Lugar de cumplimiento de la obligación:** Respecto al segundo requisito, el lugar del cumplimiento de una parte sustancial de las obligaciones, estaría situado en Colombia, en el cual las partes tienen sus domicilios.

**5.7.3 Afectación de intereses comerciales:** En cuanto al tercer requisito, es difícil determinar si una controversia sujeta a arbitraje afecta los intereses del comercio internacional. Pues, la norma debería ser interpretada de manera amplia y, la jurisprudencia debe considerar cuáles intereses afectan los intereses del comercio internacional<sup>330</sup>.

**5.7.4 La ley aplicable:** El artículo 101 del Estatuto de Arbitraje Nacional e Internacional de Colombia, la Ley 1563 de 2012<sup>331</sup>, establece que el tribunal de arbitramento deberá resolver la controversia según la ley aplicable que las partes hayan estipulado. Omitir la estipulación de la ley aplicable en un acuerdo de arbitraje internacional no es recomendable puesto que los árbitros podrían aplicar normas que la parte vencida en el proceso habría preferido no escoger<sup>332</sup>.

A propósito, el artículo 92 de la Ley 1563 de 2012 estipula que las partes de un arbitraje también pueden estipular las reglas que regirán el procedimiento arbitral, ejemplo, las partes de un arbitraje internacional cuya sede es Colombia pueden excluir la aplicación de las normas de procedimiento colombianas. Pero, el laudo que profiera el tribunal internacional debe someterse al procedimiento del *exequatur*, que garantiza el respeto al ordenamiento jurídico nacional<sup>333</sup>.

---

<sup>330</sup> GAVIRIA, Juan. Comentarios sobre las nuevas normas colombianas en materia de arbitraje internacional. *EN Revista de Derecho Privado*. Universidad Externado de Colombia. [en línea] 2013. Disponible en <<http://revistas.uexternado.edu.co/index.php/derpri/article/view/3487/3473>> [citado el 13 de abril de 2017]

<sup>331</sup> COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1563 de 2012" Por medio de la cual se expide el Estatuto de Arbitraje Nacional e Internacional y se dictan otras disposiciones". Diario Oficial. Bogotá, D.C., 2012, artículo 92.

<sup>332</sup> GAVIRIA, Juan. Comentarios sobre las nuevas normas colombianas en materia de arbitraje internacional. *EN Revista de Derecho Privado*. Universidad Externado de Colombia. [en línea] 2013. Disponible en <<http://revistas.uexternado.edu.co/index.php/derpri/article/view/3487/3473>> [citado el 13 de abril de 2017]

<sup>333</sup> *Ibidem*.

## 5.8. LAS PRETENSIONES.

Las pretensiones comprenden la voluntad de la parte accionante ante el Tribunal de arbitral para que se resuelvan diferentes conflictos jurídicos, mediante peticiones declarativas, como el reconocimiento de la existencia o inexistencia de un contrato de computación en la nube, el incumplimiento contractual, la responsabilidad de las partes, la nulidad; o con pretensiones de condena que puede ser pecuniaria o no pecuniaria, pago de perjuicios, costas y condena a una obligación de hacer, no hacer o dar<sup>334</sup>

## 5.9 LAS MEDIDAS CAUTELARES INNOMINADAS.

El poder para ordenar las medidas cautelares le corresponde al Tribunal, ya sea por la decisión de las partes en el pacto arbitral o al escoger las reglas del procedimiento adoptadas, según la ley donde se encuentren, la ubicación del Tribunal arbitral o el lugar donde las medidas habrán de ser practicadas, según lo establecido en la cláusula compromisoria. Pero, en nuestra legislación, siguiendo el modelo UNCITRAL, consagra que, independientemente de que el trámite se adelante en Colombia o en el exterior, cualquiera de las partes podrá acudir a la autoridad judicial para que decrete las medidas cautelares, de conformidad con su ley procesal y el arbitraje internacional<sup>335</sup>.

Rafael Bernal Gutiérrez<sup>336</sup> indica que no todos los sistemas legales el tribunal arbitral tiene poderes para decretar medidas cautelares o, los que se le confieren, no son suficientes, además los poderes del tribunal arbitral se limitan, en cuanto al

---

<sup>334</sup>La pretensión como objeto del proceso. [en línea]. Disponible en <[https://rodas5.us.es/file/cafc4fdc-3a41-77f0-0038-e9674ec691fb/2/objeto\\_proceso\\_SCORM.zip/page\\_01.htm](https://rodas5.us.es/file/cafc4fdc-3a41-77f0-0038-e9674ec691fb/2/objeto_proceso_SCORM.zip/page_01.htm)> [citado el 24 de abril de 2017]

<sup>335</sup> BERNAL, Rafael. Medidas cautelares en el arbitraje nacional e internacional, una mirada comparada EN: XXXVII Congreso Colombiano de Derecho Procesal. Bogotá, Universidad Libre e Instituto Colombiano de Derecho Procesal, 2016, páginas 978 y 979.

<sup>336</sup>Ibidem, pág. 968.

destinatario, a las partes que están actuando en el trámite arbitral y, no tienen ninguna posibilidad de afectar a terceros o si sucede es de manera excepcional.

Igualmente, señala que, para decretar las medidas cautelares innominadas, el Tribunal habrá de apreciar la legitimación para actuar de las partes y la amenaza del derecho, la necesidad, efectividad y proporcionalidad de la medida, su alcance, duración y de oficio podrá determinar la modificación, sustitución o cese de la medida<sup>337</sup>.

Así mismo, cuando se trate de medidas cautelares sobre pretensiones pecuniarias, se podrá impedir la práctica, solicitar su levantamiento o modificación mediante una caución para garantizar el pago de los perjuicios y el cumplimiento de la sentencia favorable, también el demandante deberá prestar caución, cuando de medidas innominadas se trate, para responder por las costas y perjuicios derivados de su práctica<sup>338</sup>.

En Colombia, se conlleva la posibilidad de adoptar decisiones que afectan tanto a las partes como a terceros, mientras que, el arbitraje internacional, las medidas cautelares son en audiencia de la parte contra la cual se decretan y las conductas que pueden ser decretadas van dirigidas a quienes son partes en el trámite y no existe la eventualidad de dirigirla a los terceros afectados<sup>339</sup>.

Ante un litigio relacionado con las disposiciones contractuales sobre la seguridad de la información, se plantean las siguientes medidas cautelares innominadas:

- Se ordene la instalación de cámaras, chips, firmas criptográficas en los lugares donde se almacena la información del usuario.

---

<sup>337</sup> Ibidem, pág. 972.

<sup>338</sup> Ibidem, pág. 973.

<sup>339</sup> Ibidem, pág. 977

- Se realice por medio de un medio masivo de comunicación, la rectificación de la información del usuario.
- Se elimine totalmente de su centro de almacenamiento la información del usuario.

## 5.10 EL ANÁLISIS DE LA PRUEBAS.

El tribunal y las partes tendrán, respecto de las pruebas, las mismas facultades y deberes previstos en el Código General del Proceso y las normas que lo modifiquen o complementen<sup>340</sup>.

Sin embargo, ante las controversias jurídicas presentadas en el desarrollo del contrato de nube bancaria, las partes muy seguramente van a presentar el contrato, manuales del funcionamiento de la nube, testigos y pruebas relacionadas con el uso de las Tecnologías de la Información, avance que está consagrado en la Ley 527 de 1999 y el Código General del Proceso, permitiendo métodos de estudio más complejos en el análisis de las pruebas.

En ese sentido, la Corte Constitucional en la Sentencia T 916 de 2008 indicó:

*(...) uno de los medios de comunicación privada que e importancia en la actualidad con el surgimiento de la informática es el correo electrónico, sobre el cual, dada la complejidad de la realidad actual exige una aproximación a la intimidad que tenga en cuenta los diversos aspectos que la contempla, entre los cuales se halla el derecho a controlar la información acerca de uno mismo. Por tratarse entonces de un dispositivo que tiene un ámbito privado, es que la regla constitucional prevista en el artículo 15 Superior, referida a la inviolabilidad de la correspondencia y demás formas de comunicación privada, tiene total aplicabilidad cuando se trata de correos electrónicos, pues se trata de una forma de comunicación entre personas determinadas, siendo solamente posible su interceptación o registro, (i) mediante*

---

<sup>340</sup> COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1563 de 2012” Por medio de la cual se expide el Estatuto de Arbitraje Nacional e Internacional y se dictan otras disposiciones”. Diario Oficial. Bogotá, D.C., 2012.

*orden de autoridad judicial, (ii) en los eventos permitidos en la ley y (iii) con observancia estricta de las formalidades que la misma establezca*<sup>341</sup>.

No obstante, los inconvenientes al aportar estas pruebas al proceso, es dudar que las evidencias informáticas son fácilmente creadas, modificadas o destruidas y que por ello difícilmente podrían ser utilizadas en un proceso judicial, Aunque, todo hecho acaecido en un sistema informático puede ser objeto de experticia para promoverse un medio probatorio a los efectos de su incorporación procesal, los peritos en la materia, utilizan entre otros el método de la reconstrucción relacional, es decir, la ubicación en los ordenadores de los datos vinculados al caso, el rastreo y determinación de la propiedad, administración, y datos de contactos relacionados con un dominio en Internet y/o servidores de almacenamiento, así como la fecha de creación y modificaciones realizadas en página Web para establecer responsabilidades y de ser posible establecer el tiempo y concatenación de estos hechos a efectos de dar a conocer al sentenciador los elementos básicos<sup>342</sup>.

Según Andrés Felipe Contreras<sup>343</sup> en la valoración probatoria, la evidencia digital no se abstrae controles inmediatos de cualquier otro elemento del acervo probatorio de todo proceso. Toda vez que, la utilidad, conducencia y pertinencia deben estar presentes en cualquier juicio de admisibilidad de evidencia, a fin, de evitar un desgaste inútil de la administración de justicia y proteger la formalidad de la prueba y evitar que se obstruya y dificulte la actividad probatoria, con evidencias que no prestarán servicio alguno al proceso. Además, es preponderante al evaluar la evidencia digital la confiabilidad en la forma en la que se haya generado, archivado, comunicado y conservado; es decir, al igual que en cualquier otra prueba, lo importante es verificar que la cadena de custodia cumpla con todas sus directrices

---

<sup>341</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-916 de 2008. (18 de septiembre de 2008). M.P Clara Inés Vargas Hernández.

<sup>342</sup> Informática Forense como medio de pruebas. [en línea]. Disponible en <<http://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.html>> [citado el 15 de abril de 2017].

<sup>343</sup> CONTRERAS, Andrés. Evidencias digitales y su valor probatorio. [en línea] 22 de julio de 2015. Disponible en <<http://derinformatico.uexternado.edu.co/evidencias-digitales-y-su-valor-probatorio/>> [citado el 10 de abril de 2017]

y refuerce la convicción que el juzgador debe tener sobre la autenticidad, integridad y autoría de la evidencia.

### **5.11 MOTIVACIÓN DEL LAUDO.**

Según el alto Tribunal Constitucional en la Sentencia T- 214 de 2012 *“la motivación de los fallos judiciales es un deber de los jueces y un derecho fundamental de los ciudadanos, como posición jurídica concreta derivada del debido proceso”*. La motivación es en un ejercicio argumentativo por medio del cual el juez establece la interpretación de las disposiciones normativas, según el acervo probatorio y la regla jurídica aplicable al caso conforme a la Carta Política, que le permita, mediante la argumentación tomar en cuenta factores relevantes y administrar el pluralismo de los principios constitucionales<sup>344</sup>.

Si bien, en Colombia casi no existe doctrina sobre los contratos de computación en la nube y no existen precedentes de los altos Tribunales, es necesario, que aunque sean temas complejos relacionados con las tecnologías de la información, los árbitros motiven el laudo, con los presupuestos procesales, la determinación del tipo de contrato, los hechos probados, el análisis de cada pretensión, el análisis de las pruebas aportadas y la doctrina jurídica civil o mercantil respecto a las cláusulas establecidas en el contrato, según la ley aplicable y los motivos del resuelve.

### **5.12 RESUELVE.**

Es la decisión que emite el árbitro y que soluciona la controversia sometida a su conocimiento, según las disposiciones jurídicas aplicables. Por tanto, el resuelve da

---

<sup>344</sup> COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-214 de 2012. (16 de marzo de 2012). M.P Luis Ernesto Vargas Silva.

respuesta a cada pretensión del accionante, según los hechos, el análisis de las pruebas, los fundamentos jurídicos etc.

Si bien, los contratos realizados con proveedores son de adhesión e incorporan cláusulas leoninas, se plantea en esta investigación que el árbitro dentro de su facultades de analizar las cláusulas del contrato, decreta que, la cláusula es abusiva por ir en contra de los principios generales del derecho, la ley, el orden público y las buenas costumbres a pesar de no tener regla expresa que lo autorice, entendiendo que en el orden público se encuentran incorporados, el derecho a la dignidad humana, la protección especial a los consumidores y la buena fe<sup>345</sup>.

En efecto, Verónica Echeverry considera que,

*Los jueces son temerosos de decretar que una cláusula es abusiva, pero en Colombia, se pueden encontrar supuestos aislados de cláusulas que no son toleradas por el ordenamiento con diferentes sanciones que pueden ser la inexistencia, la nulidad, la ineficacia, que se tengan por no escritas o la nulidad. En caso de que un juez encuentre una cláusula que tenga el carácter de abusiva pero que no tenga una sanción expresa en la legislación, aun así podría descartar su aplicación en un caso determinado, decretando la inexistencia (en caso de que el adherente no haya conocido y aceptado la cláusula); la nulidad absoluta cuando considere que por ir en contra del principio de la buena fe es contraria al orden público y, en consecuencia, tiene objeto y causa ilícita o la nulidad relativa, en caso de considerar que esa es la sanción aplicable en los casos que la ley no consagre expresamente una sanción diferente<sup>346</sup>.*

En ese sentido, estos contratos son una muestra de la reinterpretación de los principios de la buena fe, la voluntad de las partes, los derechos fundamentales que resultan vulnerados por disposiciones contractuales y de la conmutatividad en los contratos.

---

<sup>345</sup> ECHEVERRY, Verónica. El control a las cláusulas abusivas en los contratos de adhesión con consumidores. Medellín: Universidad de Medellín, Opinión Jurídica, Vol. 10, N° 20, ISSN 1692-2530, [en línea] julio-diciembre de 2011. Disponible en <http://www.scielo.org.co/pdf/ojum/v10n20/v10n20a08.pdf>, [citado el 26 de abril de 2017].

<sup>346</sup> Ibidem, pág. 140.

## 6. CONCLUSIONES.

- El *cloud computing* abre un nuevo modelo en las Tecnologías de la Información y la Comunicación, que se adapta a cada empresa, con costes predecibles, acceso desde cualquier lugar, fórmula de pago por uso y el autoservicio a la carta o la rápida elasticidad<sup>347</sup>.
- Al establecer el tipo de contrato de computación en la nube, se concluye que los grandes proveedores, con amplia trayectoria en el mercado como Google, Amazon, Apple, entre otros, elaboran unilateralmente el contrato con condiciones que no pueden ser discutidas previamente por la entidad bancaria, dado que, sólo se limita a dar su aceptación o rechazo, es decir, celebran un contrato de adhesión. Empero, si se contrata con otros proveedores se les da la oportunidad a las entidades financieras de modificar, agregar o eliminar las cláusulas del contrato; y al tratarse de servicios profesionales que realizan las empresas proveedoras para una labor específica, por ejemplo: almacenamiento de datos, corresponde a un contrato de prestación de servicios.
- - Google es una de las empresas más exitosas en el mundo de la tecnología y su buscador es el sitio más usado de la Internet, cuenta con altos niveles de seguridad de la información como la identificación biométrica, cámaras, sistemas de detección de intrusos basados en láser, firmas criptográficas. Pero, esta empresa ha aceptado subvenciones del gobierno estadounidense para el desarrollo de servicios de computación en la nube, a cambio de colaboración en la identificación de usuarios y contenidos, así como de

---

<sup>347</sup> TORRES, Jordi. Del Cloud Computing al Big Data, visión emprendedora de jóvenes emprendedores. FUOC 2012, Disponible en [http://www.jorditorres.org/wp-content/uploads/2012/03/Del.Cloud\\_.Computing.al\\_.Big\\_.Data\\_.JordiTorres.ES\\_.pdf](http://www.jorditorres.org/wp-content/uploads/2012/03/Del.Cloud_.Computing.al_.Big_.Data_.JordiTorres.ES_.pdf), pág. 20.

acceso generalizado sin orden judicial a los archivos depositados por los usuarios de sus servicios y en varias ocasiones Gmail y su buscador han sufrido fallas, dejando a sus usuarios fuera de servicio por un buen tiempo.

- El Acuerdo de licencia de Google presenta un desequilibrio jurídico relevante entre las obligaciones contraídas y los derechos adquiridos por cada contratante, para el caso, con las entidades financieras. Así mismo, se exonera de la responsabilidad frente al tratamiento de datos, evidenciándose el debido cuidado que debe mantener los bancos para proteger los datos de sus clientes, respecto a cualquier anomalía.
- En los contratos de computación en la nube, se pueden presentar varios conflictos jurídicos, relacionados con la vulneración de un derecho como el habeas data, como por ejemplo: el incumplimiento de las cláusulas que determinan la separación de la información de otros usuarios, reportándose la información inequívoca, la transferencia de datos a países donde no existe una protección de datos personales, indebida migración de la información, falta de auditoría y medidas de seguridad, uso de los datos con fines publicitarios, que derivan otro tipo de conflictos relacionados con el desconocimiento de la jurisdicción y ley aplicable para que los bancos puedan solucionar estas controversias ante un juez y no vulnerar los derechos de terceros.
- Los contratos de almacenamiento de nube con grandes proveedores son una muestra de la reinterpretación de los principios de la buena fe, la voluntad de las partes, los derechos fundamentales que resultan vulnerados por disposiciones contractuales, la necesidad de buenas prácticas corporativas y de la conmutatividad en los contratos.

- La realización de un buen contrato, disminuye los conflictos jurídicos, razón por la cual en su redacción se debe asegurar la protección de datos personales, con la obligación de establecer medidas de seguridad, pólizas de cumplimiento, cláusulas de confidencialidad para los empleados, y la redacción de códigos de ética que mejoren las prácticas corporativas de las empresas.
  
- La incorporación de la cláusula compromisoria, no representa una inserción abusiva, porque, tanto como el proveedor como la entidad financiera contarían con los medios para solucionar la controversia de manera rápida, efectiva y precisa ante el Tribunal arbitral, ya que en la redacción de esta disposición se puede establecer el lugar donde se solucionaría el litigio, el reglamento del Tribunal, el idioma y cual ley sería la aplicable, en el caso de que las partes sean de diferentes Estados.
  
- Aunque, los grandes proveedores no van a modificar las condiciones de sus servicios, sólo porque la otra parte desea que se cambien algunas estipulaciones del contrato, este trabajo planteó como solución que el árbitro según las pretensiones del accionante, verbigracia, la nulidad absoluta del contrato, pueda analizar las cláusulas y resolver con la respectiva sanción, si dichas disposiciones se ajustan a la ley, al orden público y las buenas costumbres y decretar que la cláusula es vejatoria o no.
  
- El laudo que profiera el árbitro será en derecho, teniendo en cuenta que se van a analizar las cláusulas del contrato y no aspectos técnicos, ya que, pese a que es un tema complejo, los abogados deben ajustarse a las necesidades del mercado, los avances tecnológicos, la evolución de la doctrina respecto a los bienes intangibles, la protección de derechos fundamentales en el contrato y los nuevos conflictos de las partes y para el juez competente quien los va a resolver.

- La resolución sobre las disposiciones contractuales, permite que los terceros perjudicados por la vulneración del habeas data, en este caso, los consumidores financieros se beneficien de manera expedita, imparcial, sin complicaciones a través del arbitraje.

## BIBLIOGRAFÍA.

- AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA). Computación en nube: beneficios, riesgos y recomendaciones para la seguridad de la información, [en línea]. Noviembre de 2009. [Citado el 20 de abril de 2017]. Disponible en <<https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish>>.
  
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Glosario de términos, [en línea]. 2014. [Citado el 13 de abril de 2017]. Disponible en <[https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion\\_ficheros/preguntas\\_frecuentes/glosario/index-ides-idphp.php](https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/glosario/index-ides-idphp.php)>.
  
- AREITIO BERTOLÍN, Javier. Protección del cloud computing en seguridad y privacidad. Revista española de electrónica, ISSN 0482-6396, n. 666, [en línea]. 2010. [Citado el 12 de abril de 2017]. Disponible <en [http://www.redeweb.com/\\_txt/666/42.pdf](http://www.redeweb.com/_txt/666/42.pdf)>.
  
- ASOCIACIÓN LATINOAMERICANA DE INSTITUCIONES FINANCIERAS PARA EL DESARROLLO (ALIDE). La Experiencia de Bancoldex. Core bancario: tecnología al servicio de la banca de desarrollo [en línea]. Octubre-diciembre 2011. [Citado el 24 de abril de 2017]. Disponible en <[http://www.alide.org.pe/fn11\\_fin\\_rev4\\_coreBancoldex.asp](http://www.alide.org.pe/fn11_fin_rev4_coreBancoldex.asp)>.
  
- ÁVILA, Oscar. Computación en la nube, [en línea]. 19 de mayo de 2011, p. 45–52 [Citado el 12 de abril de 2017]. Disponible en <<http://www.izt.uam.mx/newpage/contactos/anterior/n80ne/nube.pdf>>.

- BANCO PICHINCHA. Banca electrónica, [en línea]. [Citado el 23 de abril de 2017]. Disponible en <<https://www.pichincha.com/portal/Canales-de-atencion/Banca-Electronica>>.
  
- BBVA. Innovation Edge. Banca Móvil: una nueva experiencia en la era post PC, [en línea] abril de 2012. [Citado el 16 de abril de 2017]. Disponible en <[http://www.centrodeinnovacionbbva.com/sites/default/files/mobilebanking\\_spanish.pdf](http://www.centrodeinnovacionbbva.com/sites/default/files/mobilebanking_spanish.pdf)>.
  
- BENAVIDES, Claudia. Conferencia ICC YAF Aspectos esenciales del arbitraje internacional, [en línea]. 21 de Agosto de 2015. [Citado el 18 de abril de 2017]. Disponible en <<http://www.camaramedellin.com.co/site/Portals/0/Documentos/memorias%20random/Conferencia%20ICC%20YAF%20-%20Claudia%20Benavides.pdf>>.
  
- BERNAL, Rafael. Medidas cautelares en el arbitraje nacional e internacional, una mirada comparada EN: XXXVII Congreso Colombiano de Derecho Procesal. Bogotá, Universidad Libre e Instituto Colombiano de Derecho Procesal, 2016.
  
- BLAZHESKI, Filip. ¿Banca en la nube o banca en las nubes? EN: BBVA. Observatorio Económico EEUU, [en línea]. 2016, P. 1. [Citado en 8 de enero de 2017]. Disponible en <[https://www.bbvaesearch.com/wpcontent/uploads/2016/05/160510\\_CloudBanking\\_esp.pdf](https://www.bbvaesearch.com/wpcontent/uploads/2016/05/160510_CloudBanking_esp.pdf)>.
  
- BUSTAMANTE DONAS, Javier. Ética en la nube: dilemas éticos y políticos en el modelo de "Computación en nube (Cloud computing)". Argumentos de razón técnica: Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología, ISSN 1139-3327, n. 16, [en línea]. 2013. [Citado el 13 de abril de 2017]. Disponible en <[http://institucional.us.es/revistas/argumentos/16/art\\_2.pdf](http://institucional.us.es/revistas/argumentos/16/art_2.pdf)>.

-CÁMARA DE COMERCIO DE BOGOTÁ, Cláusulas compromisorias, [en línea]. [Citado el 25 de abril de 2017]. Disponible en <<http://www.centroarbitrajeconciliacion.com/Servicios/Arbitraje/Clausulas-compromisorias>>.

- CASTRO, Jorge, et al. Cloud computing una perspectiva para Colombia. Mesa Sectorial sobre Cloud Computing, organizada por CINTEL y presidida por NEC de Colombia [en línea] abril de 2010. [Citado el 24 de abril de 2017]. Disponible en <[http://cintel.co/wp-content/uploads/2013/05/16.clud\\_computing\\_Cloud-Computing-Mesa-sectorial-1.pdf](http://cintel.co/wp-content/uploads/2013/05/16.clud_computing_Cloud-Computing-Mesa-sectorial-1.pdf)>.

- CERDÁ, Hugo. 'Cloud computing': informática en la nube, llega la tormenta. Técnica industrial, [en línea] 2009. ISSN 0040-1838. N. 282. [Citado el 18 de abril de 2017]. Disponible en <<http://www.tecnicaindustrial.es/TIAdmin/Numeros/64/46/a46.pdf>>.

- COLEGIO PROFESIONAL DE INGENIEROS EN INFORMÁTICA DE LA COMUNIDAD DE MADRID CPIICM. Reglamento de la Corte de Arbitraje, [en línea]. 8 de junio de 2016. [Citado el 06 de marzo de 2017]. Disponible en <<http://cpiicm.es/wp-content/uploads/sites/3/2016/06/Reglamento-Corte-Arbitral-CPIICM.pdf>>.

- COLOMBIA. CORTE CONSTITUCIONAL. Constitución Política de 1991. Artículo 116. Gaceta Constitucional. Bogotá D.C. 20 de julio de 1991. No. 116.

-COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 de 2012 (octubre 17 de 2012) por la cual se dictan disposiciones generales para la protección de datos personales, Diario Oficial. Bogotá, D.C., 2012.

-COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 de 2008, (diciembre 31 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. Bogotá, D.C., 2008.

- COLOMBIA. PRESIDENTE DE LA REPÚBLICA, Decreto 1227 de 2005, por el cual se reglamenta parcialmente la Ley 909 de 2004 y el Decreto-ley 1567 de 1998. (abril 21 de 2005), [en línea]. [Citado el 04 de abril de 2017]. Disponible en <<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=16313>>.

- COLOMBIA. PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. Decreto 1074 DE 2015 (mayo 26 de 2015) “Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo”. [Citado el 04 de abril de 2017]. Disponible en <<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62508>>.

- COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1341 de 2009, (julio 30 de 2009), por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2009.

- COLOMBIA. Ley 57 de 1887. Código Civil, [en línea]. [Citado el 24 de abril de 2017]. Disponible en <<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=39535>>.

- COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 2952 de 2010, Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008 (agosto 6 de 2010),

[en línea]. [Citado el 21 de abril de 2017]. Disponible en <<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=40120>>.

- COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1563 de 2012” Por medio de la cual se expide el Estatuto de Arbitraje Nacional e Internacional y se dictan otras disposiciones”. Diario Oficial. Bogotá, D.C., 2012.

-COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 76434 de 2012 (diciembre 4 de 2012) Diario Oficial. Bogotá, D.C. No. 48.635 de 5 de diciembre de 2012.

- COLOMBIA. SUPERINTENDENCIA FINANCIERA. Circular 052 de 2007 (octubre de 2007), [en línea]. [citado el 24 de marzo de 2017]. Disponible en <<https://www.bancodebogota.com/wps/themes/html/banco-de-bogota/pdf/nuestra-organizacion/transparencia/circular-052.pdf>>.

- COLOMBIA, SUPERINTENDENCIA FINANCIERA. Concepto 2015019296-001, contratación en la nube, contratación de servicios de terceros (16 de abril de 2015), [en línea]. [Citado el 21 de abril de 2017]. Disponible en <<https://en.superfinanciera.gov.co/jsp/loader.jsf?IServicio=Publicaciones&ITipo=publicaciones&IFuncion=loadContenidoPublicacion&id=10084637&dPrint=1>>.

- COLOMBIA, SUPERINTENDENCIA FINANCIERA. Circular Básica Jurídica, Circular Externa 029 (2014), [en línea]. [Citado el 21 de abril de 2017]. Disponible en <<https://www.superfinanciera.gov.co/jsp/loader.jsf?IServicio=Publicaciones&ITipo=publicaciones&IFuncion=loadContenidoPublicacion&id=10083443&reAncha=1>>.

- COLOMBIA, SUPERINTENDENCIA FINANCIERA. Expediente 2013 -0063. No. 2013015100 (julio 31 de 2013).

- COLOMBIA, SUPERINTENDENCIA FINANCIERA. Concepto 2016070922-001, banca móvil, banca por internet, normatividad (11 de agosto de 2016), [en línea]. [Citado el 30 de marzo de 2017]. Disponible en <<https://www.superfinanciera.gov.co/jsp/loader.jsf?IServicio=Publicaciones&ITipo=publicaciones&IFuncion=loadContenidoPublicacion&id=10087124&dPrint=1>>.
  
- COLOMBIA, SUPERINTENDENCIA FINANCIERA. Expediente 2013 -0211. No. 2013041561(noviembre 20 de 2013).
  
- COLOMBIA, SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Proyecto de Circular Externa, Bogotá, [en línea]. [Citado el 25 de marzo de 2017]. Disponible en <[http://www.sic.gov.co/sites/default/files/normatividad/Proyecto\\_Circular\\_Adiciona\\_capitulo\\_3\\_al\\_titulo\\_5\\_transferencia\\_internacional\\_de\\_datos.pdf](http://www.sic.gov.co/sites/default/files/normatividad/Proyecto_Circular_Adiciona_capitulo_3_al_titulo_5_transferencia_internacional_de_datos.pdf)>.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-443 de 1994. (12 de octubre de 1994) M. P Eduardo Cifuentes Muñoz.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia SU-082 de 1995 (1 de marzo de 1995) M.P Jorge Arango Mejía.
  
- COLOMBIA, CORTE CONSTITUCIONAL, SentenciaT-716 de 1996 (16 de diciembre de 1996) M.P Antonio Barrera Carbonell.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C-347 de 1997, (23 de julio de 1997). M.P Jorge Arango Mejía.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C-1147 de 2001. (13 de octubre de 2011) M.P Manuel José Cepeda Espinosa.

- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-464 de 2002. (13 DE JUNIO DE 2002). M.P Marco Gerardo Monroy Cabra.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T- 160 de 2005 (24 de febrero de 2005) M.P Marco Gerardo Monroy Cabra.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia SU174 del 2007, (14 de marzo de 2007). M.P Manuel José Cepeda Espinosa.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-916 de 2008. (18 de septiembre de 2008). M.P Clara Inés Vargas Hernández.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C-748 de 2011, (6 de octubre de 2011) Jorge Ignacio Pretelt Chaljub.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-330 de 2012. (9 de mayo de 2012). M.P Humberto Antonio Sierra Porto.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-833 de 2013 (diciembre 3 de 2013) M.P Luis Guillermo Guerrero Pérez.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-246 de 2014 (abril 11 de 2014) M.P Mauricio González Cuervo.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-943 de 2006. (16 de noviembre de 2006) M.P Álvaro Tafur Galvis.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-900 de 2008, (16 de septiembre de 2008), M.P Humberto Antonio Sierra Porto.

- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T-214 de 2012. (16 de marzo de 2012). M.P Luis Ernesto Vargas Silva.
  
- COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T- 167 de 2015. (15 de abril de 2015) M.P Jorge Ignacio Pretelt Chaljub.
  
- COLOMBIA, TRIBUNAL ARBITRAL. Datapoint de Colombia S.A.S Vs Comercializadora de Software Extensión de Colombia S.A (16 de octubre de 2014). Árbitros: Luis Augusto Cangrejo Cobos, Marcel Tangarife Torres y Gustavo Suárez Camacho.
  
- COLOMBIA INN. IBM inaugura el mayor centro de datos en nube de Colombia [en línea]. [Citado el 25 de febrero de 2017]. Disponible en <<http://colombia-inn.com.co/ibm-inaugura-el-mayor-centro-de-datos-en-nube-de-colombia-3/>>.
  
- CNN. El internet es un derecho según la ONU, [en línea] 9 de junio de 2011. [Citado el 24 de abril de 2017]. Disponible en <<http://cnnespanol.cnn.com/2011/06/09/el-acceso-a-internet-un-derecho-humano-segun-la-onu/>>.
  
- COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL UNCITRAL. Ley modelo de la CNUDMI sobre arbitraje comercial - internacional. Nueva York, [en línea] 2008. [Citado el 7 de febrero de 2017]. Disponible en <[https://www.uncitral.org/pdf/spanish/texts/arbitration/ml-arb/07-87001\\_Ebook.pdf](https://www.uncitral.org/pdf/spanish/texts/arbitration/ml-arb/07-87001_Ebook.pdf)>.
  
- CONTRERAS, Andrés. Evidencias digitales y su valor probatorio, [en línea] 22 de julio de 2015. [Citado el 10 de abril de 2017]. Disponible en <<http://derinformatico.uexternado.edu.co/evidencias-digitales-y-su-valor-probatorio/>>.

-DATAWARE. Sistemas [en línea] 2015 [citado el 14 de abril de 2017]. Disponible en <http://www.dwsistemas.com/es/index.php/noticias/27-peligro-pagina-bancolombia-phishing>.

- DEL VECCHIO, José, PATERNINA, Fabián. La computación en la nube: Un modelo para el desarrollo de las empresas, [en línea]. Vol. 13, No. 2, Julio-diciembre de 2015, págs. 81-87 [citado el 02 de abril de 2017]. Disponible en <http://www.scielo.org.co/pdf/prosp/v13n2/v13n2a10.pdf>.

- DINERO.COM. Los negocios de la “nube” viven una verdadera danza de los millones, [en línea]. 3 de marzo de 2016 [citado el 8 de marzo de 2017]. Disponible en <http://www.dinero.com/edicion-impres/a/negocios/articulo/crecimiento-de-los-negocios-en-la-nube-o-cloud-en-el-2016/220999>.

- DRAGONJAR. Informática Forense como medio de pruebas, [en línea]. [citado el 15 de abril de 2017]. Disponible en <http://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.xhtml>

- ECHEVERRY, Verónica. El control a las cláusulas abusivas en los contratos de adhesión con consumidores. Medellín: Universidad de Medellín, Opinión Jurídica, Vol. 10, N° 20, ISSN 1692-2530, [en línea]. Julio-diciembre de 2011 [citado el 26 de abril de 2017]. Disponible en <http://www.scielo.org.co/pdf/ojum/v10n20/v10n20a08.pdf>

- ENTREVISTA con Leonardo JAIMES, Ingeniero Electrónico de la Universidad Industrial de Santander. Bogotá D.C., 18 de febrero de 2017.

- ENTREVISTA con César Augusto QUIJANO QUIROGA, abogado, Asesor Jurídico en Universidad Industrial de Santander, quien se ha desempeñado como árbitro de la Cámara de Comercio de Bucaramanga. Bucaramanga, 26 de abril de 2017.

- EUROPA. PARLAMENTO EUROPEO. Dirección general de políticas interiores. Departamento temático, política, economía y científica. Computación en la nube, [en línea] mayo de 2012 [citado el 15 de abril de 2017]. Disponible en <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO\\_ET\(2012\)475104\\_ES.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf)>
  
- EL PAÍS. Fiscalía buscará tener acceso al WhatsApp de los judicializados [en línea]. Marzo 30 de 2017 [citado el 15 de abril de 2017]. Disponible en <<http://www.elpais.com.co/colombia/fiscalia-buscara-tener-acceso-al-whatsapp-de-los-judicializados.html>>.
  
- EL PAÍS. Google amplía a todo el mundo su sistema de verificación de noticias falsas [en línea]. Marzo 7 de 2017 [citado el 22 de abril de 2017]. Disponible en <[http://tecnologia.elpais.com/tecnologia/2017/04/07/actualidad/1491552626\\_830458.html](http://tecnologia.elpais.com/tecnologia/2017/04/07/actualidad/1491552626_830458.html)>
  
- FAJARDO, Daniel. Pasión por los negocios: por qué los bancos y la industria financiera se están entusiasmando en la nube híbrida. EN Revista Pulso, [en línea]. Disponible en <<http://www.pulso.cl/noticia/tech/industria/2015/05/76-64216-9-por-que-los-bancos-y-la-industria-financiera-se-estan-entusiasmando-en-la-nube.shtml>>, [citado el 21 de abril de 2017].
  
- FINANZAS PERSONALES ¿Qué son las centrales de riesgo y para qué sirven? [en línea]. [Citado el 25 de abril de 2017]. Disponible en <<http://www.finanzaspersonales.com.co/credito/articulo/que-centrales-riesgo-para-que-sirven/51380>>
  
- FONS, Fernando. Cloud Computing: caracterización de los impactos positivos obtenidos por la utilización del modelo Cloud Computing por las pymes, basado en

la tipología de Modelos de Negocio de este tipo de empresas, [en línea]. Julio 17 de 2014 [citado el 4 de abril de 2017].

Disponible en:  
<<https://riunet.upv.es/bitstream/handle/10251/38864/Cloud%20Computing%20y%20Modelo%20de%20Negocio%20para%20pymes%20-%20TFM%20de%20Fernando%20Fons.pdf?sequence=1>>

-GALEÓN. Conceptos de hardware y software, [en línea]. [Citado el 22 de abril de 2017]. Disponible en <<http://engendros.galeon.com/U1T6.htm>>

- GASTÓN, Bruno. Cloud computing en la industria financiera, [en línea]. Octubre 2013 [citado el 22 de abril de 2017]. Disponible en <[http://www.palermo.edu/ingenieria/pdf2014/13/CyT\\_13\\_05.pdf](http://www.palermo.edu/ingenieria/pdf2014/13/CyT_13_05.pdf), 2013>

- GASSER URS y O'BRIEN DAVID. Governments and Cloud Computing: Roles, Approaches, and Policy Considerations [en línea]. Agosto 2013. Universidad de Harvard. [citado el 22 de abril de 2017]. Disponible en <<https://dash.harvard.edu/bitstream/handle/1/16460373/Gasser2014-6.pdf?sequence=1>>

- GAVIRIA, Juan. Comentarios sobre las nuevas normas colombianas en materia de arbitraje internacional. EN Revista de Derecho Privado. Universidad Externado de Colombia, [en línea]. 2013 [citado el 13 de abril de 2017]. Disponible en <<http://revistas.uexternado.edu.co/index.php/derpri/article/view/3487/3473>>.

- GONZÁLEZ, Hugo. Implementación y uso de un *core bancario* para banca retail en la tecnología *cloud computing*. Trabajo de grado de Magíster en Gerencia de Tecnología de la información, Quito: Pontificia Universidad Católica de Ecuador. Maestría en Gerencia de Tecnología de la información, [en línea]. Mayo de 2015 [citado el 12 de abril de 2017]. Disponible en

<<http://repositorio.puce.edu.ec/bitstream/handle/22000/8539/CASO%20DE%20ESTUDIO%20-%20Hugo%20Gonzalez.pdf?sequence=1>>.

-GOOGLE CLOUD PLATAFORM. Google Infraestructura Security Design Overview, [en línea]. Febrero 24 de 2017 [citado el 25 de abril de 2017]. Disponible en <<https://cloud.google.com/security/security-design/>>

- GOOGLE CLOUD PLATAFORM. *Google Cloud Platform Terms of Service*, [en línea]. Marzo 7 de 2017 [citado el 22 de abril de 2017]. Disponible en <<https://cloud.google.com/terms/>>.

- GOOGLE CLOUD PLATAFORM. Google Cloud Platform Blog, Google shares data center security and design best practices, [en línea]. Marzo 24 de 2016 [citado el 20 de abril de 2017]. Disponible en <[https://docs.google.com/document/d/17am-dv9UmarT7HQiuqM\\_NfWeyhhKi1sfExPI4IsRwOE/edit#>](https://docs.google.com/document/d/17am-dv9UmarT7HQiuqM_NfWeyhhKi1sfExPI4IsRwOE/edit#>)

- GOUJON, André. ¿Qué es y cómo funciona una VPN para la privacidad de la información?, 10 de septiembre de 2012, [en línea]. Septiembre 10 de 2012 [citado el 23 de abril de 2017]. Disponible en <<http://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/>>.

- GUASCH, Vicente, SOLER José. Cloud computing: cláusulas contractuales y reglas corporativas vinculantes. RDUNED. EN Revista de derecho UNED, ISSN 1886-9912, n. 14, [en línea] 2014 [citado el 22 de abril de 2017]. Disponible en <<http://revistas.uned.es/index.php/RDUNED/article/view/13300/12171>>.

- INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR (ICBF). Proceso servicios administrativos. Procedimiento saneamiento de inmuebles. Definiciones. Colombia, [en línea], 2016 [citado el 20 de abril de 2017]. Disponible en <<http://www.icbf.gov.co/portal/page/portal/PortalICBF/procesos/apoyo/servicios>>.

- INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN. (INTECO). Riesgos y amenazas en Cloud Computing. España: [en línea] marzo de 2011 [citado el 12 de abril de 2017]. Disponible en <[https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_riesgos\\_y\\_amenazas\\_en\\_cloud\\_computing.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf)>

- JARA, Jairo. Guía para el análisis de factibilidad en la implantación de tecnologías de cloud computing en empresas del Ecuador. Trabajo de grado para optar por el título de Ingeniero en Sistemas Informáticos y de computación. Quito: Escuela Politécnica Nacional, Facultad de Ingeniería de Sistemas, mayo de 2012 [citado el 25 de febrero de 2017]. Disponible en <<http://bibdigital.epn.edu.ec/bitstream/15000/4649/1/CD-4281.pdf>>.

- JIMENEZ, Edwin. Modelo de Tarificación Software como Servicio SaaS. Trabajo de grado de Magíster en ciencias de la información y las comunicaciones. Bogotá: Universidad Distrital Francisco José de Caldas. Facultad de Ingeniería. Maestría en ciencias de la información y las Comunicaciones, [en línea] 2015 [citado el 24 de abril de 2017]. Disponible en <<http://repository.udistrital.edu.co/bitstream/11349/2765/1/JimenezGarzonEdwinAlfonso2015.pdf>>.

-LARA, Pablo y MANIEGA, David. Conocimiento en la nube: evolución de las intranets. El profesional de la información, [en línea], marzo-abril 2011, v. 20, n. 2, [citado el 14 de abril de 2017]. Disponible en <<http://www.elprofesionaldelainformacion.com/contenidos/2011/marzo/07.pdf>>.

- LÓPEZ, David. La “Computación en la nube o “cloud computing” examinada desde el ordenamiento jurídico español.EN: Revista de Derecho de la Universidad Católica de Valparaíso. N° 40 agosto de 2013 ISSN 0718-685, pp. 689 – 709 [en

línea]. Disponible en <<http://www.scielo.cl/pdf/rdpucv/n40/a21.pdf>>, [citado el 20 de abril de 2017].

- LÓPEZ, María, ALBANESE, Diana y otros. Identificación de riesgos vinculados con el uso de Cloud Computing en la Gestión Organizacional. Aplicación de la Risk Breakdown Structure a Entidades Financieras de la República Argentina. Rio Janeiro: ANPAD [en línea] 4 de septiembre de 2011 [citado el 12 de abril de 2017]. Disponible en <<http://www.anpad.org.br/admin/pdf/ADI2220.pdf>>.

- MACHADO, Jesús. Blogs Computación en la nube: Conceptos y recomendaciones, marzo 4 de 2015, [en línea]. Marzo 4 de 2015 [citado el 24 de febrero de 2017]. Disponible en <<https://blogs.vmware.com/latam/2015/03/computacion-en-la-nube-conceptos-y-recomendaciones.html>>.

- MATIAS, CAMARGO. La política pública de liberalización y privatización de las telecomunicaciones en Colombia. Bogotá DC: Universidad Libre de Colombia, Facultad de Derecho Centro de Investigaciones Socio Jurídicas. 2011 ISBN 978-958-85-34-63-3.

- MINISTERIO DE JUSTICIA. Programa Nacional de Arbitraje. Arbitraje internacional, [en línea]. 2017 [citado el 25 de marzo de 2017]. Disponible en <<https://conciliacion.gov.co/portal/Arbitraje/-Qu%C3%A9-es-Arbitraje/Arbitraje-Internacional>>.

- MIRÓ ECHEVARNE, Manuel. Valoración financiera de recursos intangibles, [en línea] 2006 [citado el 25 de enero de 2017]. Disponible en <<http://www.ub.edu/iafi/Recerca/Seminaris/miro.pdf>>.

- MOLINA, Alberto. ¿Qué es eso de OpenStack y por qué debería conocerlo? [en línea]. 25 de noviembre de 2013 [citado el 23 de abril de 2017]. Disponible en <<https://openwebinars.net/blog/que-es-eso-de-openstack-por-que-deberia-conocerlo/>>.

- MOLINA, José. Aproximación jurídica al ciberespacio. Instituto Español de Estudios Estratégicos. EN: Instituto Español de Estudios Estratégicos, [en línea] Junio 8 de 2015 [citado el 22 de abril de 2017]. Disponible en <[http://www.ieee.es/Galerias/fichero/docs\\_opinion/2015/DIEEEO572015\\_Aproximacion\\_Juridica\\_Ciberespacio\\_MolinaMateos.pdf](http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO572015_Aproximacion_Juridica_Ciberespacio_MolinaMateos.pdf)>.

-MONROY, C.R., Arias, C.A., GUERRERO, Y.N. El nuevo paradigma de la computación en la nube: el camino hacia la TI visto como una utilidad. EN: Revista Latinoamericana y del Caribe de Educación en Ingeniería, [en línea]. 2013 [citado el 15 de enero de 2017]. Disponible en <<https://riunet.upv.es/bitstream/handle/10251/38864/Cloud%20Computing%20y%20Modelo%20de%20Negocio%20para%20pymes%20-%20TFM%20de%20Fernando%20Fons.pdf?sequence=1>>.

- MORALES, Molina, Hernando. Curso de derecho procesal civil. Parte general. 4ª edición. Lerner. 1960.

- MORENO, Gonzalo. Jurisdicción aplicable en materia de datos personales en los contratos de cloud computing: análisis bajo la legislación colombiana. Universidad de los Andes, Facultad de Derecho. Revista de Derecho, Comunicaciones y Nuevas Tecnologías. N°9 junio de 2013. ISSN 1909-7786.

-MUÑOZ, Ana, ¿Qué es Startup? [en línea]. Diciembre 24 de 2016 [citado el 24 de abril de 2017]. Disponible en <<http://computerhoy.com/noticias/internet/que-es-startup-56074>>.

- MUSEO DE INFORMÁTICA. Historia de Google, EN: Blog historia de la informática [en línea]. 11 de enero del 2011 [citado el 20 de febrero de 2017]. Disponible en <<http://histinf.blogs.upv.es/2011/01/11/historia-de-google/>>.
  
- NOCETI, Héctor Y FREIJO, Aníbal. Cloud computing. Su aplicación en la banca privada Argentina. Buenos Aires, Argentina: Universidad Argentina de la Empresa (UADE) Facultad de Ingeniería y Ciencias Exactas, [en línea]. 2015. ISSN: 2451-7631 [citado el 23 de abril de 2017]. Disponible en <<http://44jaiio.sadio.org.ar/sites/default/files/sts264-276.pdf> >.
  
- ORTEGA, Francisco. Derecho y TIC. Bogotá D.C: Temis S.A. ISBN 978-958-35-0863-9.
  
- PÉREZ, Lorena. ¿Es confiable el cloud computing? [en línea]. 17 de marzo de 2016 [citado el 10 de abril de 2017]. Disponible en <<https://lorenaperezcampillo.com/2016/03/17/es-fiable-el-cloud-computing/>>.
  
- PÉREZ, Manuel. Manual de Informática y Derecho. Barcelona: Ariel, 1996. ISBN 84-344-1598-4, [citado el 25 de febrero de 2017].
  
- POSADA TORRES, Camilo. Las cláusulas abusivas en los contratos de adhesión en el derecho colombiano. EN: Revista de la Universidad Externado. Núm. 29 [en línea] 14 de diciembre de 2015. Disponible en <<http://revistas.uexternado.edu.co/index.php/derpri/article/view/4328/5081>>, [citado el 24 de abril de 2017].
  
- PORTAFOLIO.CO. Empresas le apuestan a estar en la nube. Más compañías en Colombia invertirán en esta herramienta, [en línea]. 14 de diciembre de 2011 (citado

el 22 de abril de 2017). Disponible en <<http://www.portafolio.co/tendencias/empresas-le-apuestan-nube-133834>>.

- PRUCOMMERCIALRE.COM ¿Qué es el Consejo Federal de Instituciones Financieras examen? [en línea]. 12 de septiembre de 2010 [citado el 22 de enero de 2017]. Disponible en <<http://www.prucomercialre.com/que-es-el-consejo-federal-de-instituciones-financieras-examen/>>.

- REMOLINA, Nelson, 'Cloud computing' y protección de datos personales. Aunque la información esté en la nube, la responsabilidad se asume en la tierra. EN: Periódico Ámbito Jurídico, [en línea] 20 de septiembre de 2011 [citado el 14 de abril de 2017]. Disponible en <[www.ambitojuridico.com/BancoConocimiento/Educacion-y-Cultura/noti-110920-12-cloud-computing-y-proteccion-de-datos-personales-aunque-la-informacion-este-en](http://www.ambitojuridico.com/BancoConocimiento/Educacion-y-Cultura/noti-110920-12-cloud-computing-y-proteccion-de-datos-personales-aunque-la-informacion-este-en)>.

- RENGIFO GARCÍA, Ernesto. Computación en la nube. Revista la propiedad inmaterial, ISSN 1657- 1959. N. 17, [en línea] 2013 [citado el 15 de abril de 2017]. Disponible en <<http://dialnet.unirioja.es/servlet/articulo?codigo=4775097>>.

- RIVERO, Marcelo, ¿Qué es el phishing? [en línea]. [Citado el 22 de abril de 2017]. Disponible en <<https://www.infospymware.com/articulos/que-es-el-phishing/>>.

- SALIDO, Ruben et., al. Innovación y Multicanalidad en Banca. “La amenaza de las “FinTech Start Up,s”, Colegio Universitario de Estudios Financieros CUNEF, 2014-2015, [en línea]. [citado el 14 de abril de 2017]. Disponible en <[http://biblioteca.cunef.edu/gestion/catalogo/doc\\_num.php?explnum\\_id=1360](http://biblioteca.cunef.edu/gestion/catalogo/doc_num.php?explnum_id=1360)>.

- SILVA, Martín. El arbitraje y los contratos de adhesión en el Cloud Computing: una solución a los abusos en las relaciones asimétricas: Derecho, nuevas tecnologías, arte y otras yerbas. [en línea], 22 de junio de 2013 [citado el 15 de abril de 2017].

Disponible en < <http://derecho-e-internet.blogspot.com.co/2013/07/el-arbitraje-y-los-contratos-de.html>>.

- SOFTONIC NEWS LETTERS. Google vs las mentiras [en línea]. Visto en softonic.es [citado el 22 de abril de 2017].

- SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Manual de protección de los datos personales en los servicios de contratación en la nube (cloud computing), [en línea]. 10 de diciembre de 2015 [citado el 3 de marzo de 2017]. Disponible en <[https://issuu.com/quioscosic/docs/cartilla\\_proteccion\\_datos](https://issuu.com/quioscosic/docs/cartilla_proteccion_datos)>.

- TELESUR. Facebook ya advierte a sus usuarios sobre noticias falsas [en línea]. 22 de marzo de 2017 [citado el 11 de abril de 2017]. Disponible en <<http://www.telesurtv.net/news/Facebook-ya-advierte-a-sus-usuarios-sobre-noticias-falsas-20170322-0082.html>>.

- TELESUR. Creador de la web advierte de manipulación con noticias falsas. [En línea] 16 de marzo de 2017 [citado el 12 de abril de 2017]. Disponible en <<http://www.telesurtv.net/news/Creador-de-la-web-advierte-de-manipulacion-con-noticias-falsas-20170316-0054.html>>.

- TEMENOS. Banca en la nube: la computación en la nube es el futuro de la tecnología bancaria, [en línea]. [Citado el 24 de abril de 2017]. Disponible en <<https://www.temenos.com/es-mx/productos-y-servicios/banca-en-la-nube/>>.

-TIEMBLO, Alexandra. Seguridad y cumplimiento normativo en el cloud computing. Trabajo de grado para optar por el título de ingeniero Informático. Madrid: Universidad Carlos III de Madrid, [en línea] 15 de junio de 2012 [citado el 12 de abril de 2017]. Disponible en <[144](http://e-</a></p></div><div data-bbox=)

archivo.uc3m.es/bitstream/handle/10016/16232/tfg\_alexandra\_tiemblo\_moreno\_2012.pdf?sequence=1>.

- TORRES, Jordi. Del Cloud Computing al Big Data, visión emprendedora de jóvenes emprendedores. FUOC 2012. Primera ed.: septiembre 2012, [en línea]. [Citado el 25 de febrero de 2017]. Disponible en <[http://www.jorditorres.org/wp-content/uploads/2012/03/Del.Cloud\\_.Computing.al\\_.Big\\_.Data\\_.JordiTorres.ES\\_.pdf](http://www.jorditorres.org/wp-content/uploads/2012/03/Del.Cloud_.Computing.al_.Big_.Data_.JordiTorres.ES_.pdf)>.

- TORO, Cristian, MURCIA, Johan y HERNÁNDEZ, Marien. Guía de auditoría para evaluar el aseguramiento de la disponibilidad de la información en un ambiente cloud computing IAAS, bajo la norma ISO 27001 de 2013. Trabajo de grado de especialistas en auditoría de sistemas de información, Bogotá: Universidad Católica de Colombia, Facultad de Ingeniería, Especialización en Auditoría de Sistemas de Información, [en línea], 2014 [citado el 11 de abril de 2017]. Disponible en <<http://repository.ucatolica.edu.co/bitstream/10983/1751/1/TRABAJO%20GRADO%20CLOUD%20COMPUTING%20IAAS.pdf>>.

- UNIVERSIDAD DE NAVARRA, IESE. Las nuevas tecnologías y su impacto en la competitividad empresarial, [en línea], 20 de marzo de 2013. [Citado el 24 de abril de 2017]. Disponible en <<http://www.iese.edu/es/conoce-iese/prensa/noticias/noticias/2013/marzo/las-nuevas-tecnologias-y-su-impacto-en-la-competitividad-empresarial/>>.

- VÁSQUEZ, Eduardo. Google lanza globos al espacio para dar internet gratis al mundo, EN Sophimania, esa manía por saber, [en línea] 24 de junio de 2013. [Citado el 12 de abril de 2017]. Disponible en <<http://www.sophimania.pe/espacio-y-cosmos/cosmos/google-lanza-globos-al-espacio-para-dar-internet-gratis-al-mundo/>>.

-VELASCO & CALLE D'ALEMAN. Contratación en la Nube, Privacidad y Recomendaciones de la Autoridad colombiana. Parte 2 [en línea]. 10 de agosto de 2006. [Citado el 1 de abril de 2017]. Disponible en <<http://velascocalle.co/blog/contratacion-en-la-nube-privacidad-y-recomendaciones-de-la-autoridad-colombiana-parte-2/>>.

- VELASCO & CALLE D'ALEMAN. Incertidumbre en Colombia por Transferencia Internacional de Datos Personales con Estados Unidos, [en línea] 15 de marzo de 2017. [Citado el 12 de abril de 2017]. Disponible en <<http://velascocalle.co/blog/incertidumbre-en-colombia-por-transferencia-internacional-de-datos-personales-con-estados-unidos/>>.

- WAYER, Fayer. Computación en la Nube. Guatemala, [en línea] 2012. [Citado el 24 de abril de 2017]. Disponible en <<http://todosobrelanube.blogspot.com.co/p/historia.html>>.

- ZAUZICH, Ivanna. Cloud banking: de qué se trata la banca en la nube y cómo implementarla. EN: Cobiscorp blog, [en línea]. 22 de marzo de 2016. [Citado el 23 de marzo de 2017]. Disponible en <<http://blog.cobiscorp.com/banca-en-la-nube-cloud-banking>>.

- ZAUZICH, Ivanna. La Importancia del Core Bancario en Bolivia. EN: COBIS, [en línea] 16 de junio de 2016. [Citado el 24 de abril de 2017]. Disponible en <<http://blog.cobiscorp.com/como-tener-core-bancario-bolivia>>

- (n.f.) La pretensión como objeto del proceso, [en línea]. [Citado el 24 de abril de 2017]. Disponible en <[https://rodas5.us.es/file/cafc4fdc-3a41-77f0-0038-e9674ec691fb/2/objeto\\_proceso\\_SCORM.zip/page\\_01.htm](https://rodas5.us.es/file/cafc4fdc-3a41-77f0-0038-e9674ec691fb/2/objeto_proceso_SCORM.zip/page_01.htm)>.