FACULTAD DE DERECHO Y CIENCIAS SOCIALES

El DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL ECUATORIANO ANALIZADO A PARTIR DE LA RELACIÓN B2C (BUSINESS TO CONSUMER) EN LA PRESTACIÓN DE SERVICIOS DE *CLOUD COMPUTING*: CASO DE POLÍTICAS DE PRIVACIDAD DE DROPBOX

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de Abogada de los Tribunales y Juzgados de la República

Profesor Guía
Ms. Lorena Naranjo Godoy

Autor
Eugenia Patricia Novoa Zubiría

Año
2015

DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido este trabajo a través de reuniones periódicas con la estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

_____

Lorena Naranjo Godoy
Master en Derecho de las Nuevas Tecnologías
C.I.: 170829378-0

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____

Eugenia Patricia Novoa Zubiría

C.I.: 171338934-2

AGRADECIMIENTO

A mi amado y omnipotente Dios.

A mi hijo, por la luz que sus sonrisas dan a mi vida.

A mis padres por formarme y permitirme ser quien soy.

A quien dirigió este trabajo con la entrega, exigencia y amor propios de una madre, mi mentora y buena amiga Lorena Naranjo.

Al cuerpo docente de mi querida facultad, por forjar en mí esta pasión por estudio del derecho.

A las TIC, por sus retos.

Eugenia

DEDICATORIA

A mi Dios, porque con su amor eterno guía mi existir.

Eugenia

RESUMEN

El *cloud computing* o nube de cómputo es un paradigma de Internet a través del cual se ofrecen servicios agiles, efectivos y fáciles de utilizar, lo que genera beneficios económicos y sociales a nivel mundial. Sin embargo, muchos ignoran lo que es el *cloud computing* y las variadas implicaciones de su utilización.

En aquellos casos de relaciones business to consumer (B2C) usuarios de servicios de *cloud computing*, incluso sin haberse percatado, son signatarios de contratos de adhesión. Estos contratos en sus cláusulas facultan a dichos proveedores para dar tratamiento a la información personal de sus usuarios. Muchas veces el contenido de estos contratos es abusivo y desencadena en un manejo inescrupuloso de la información, lo que genera afectaciones irreparables para los usuarios.

En relación a lo manifestado, la Constitución de la República de Ecuador reconoce el derecho a la protección de datos de carácter personal, derecho que ampara a las personas para no ser víctimas de un inadecuado tratamiento y manejo de información. Este trabajo busca esclarecer cómo la prestación de servicios de *cloud computing* puede afectar al derecho a la protección de datos personales reconocido a los consumidores ecuatorianos, y qué medidas debe establecer el Estado para que este derecho ampare de forma preventiva a los usuarios de servicios de cómputo en la nube.

ABSTRACT

Cloud computing is a paradigm through which Internet services are offered agile, effective and easy to use, thus generating economic and social benefits worldwide. However, many ignore what is cloud computing and its implications generated by its use.

In business to consumer (B2C) cases users of cloud services, even without being noticed, are signatories of adhesion contracts. The clauses in their contracts entitle such providers to treat the personal information of its user's. Indeed these contracts are abusive and trigger an unscrupulous management of information causing irreparable damages to users.

The Constitution of the Republic of Ecuador recognizes the right of personal data protection, a right that protects the victims from bad processing of information. This paper seeks to establish how the provision of cloud computing can affect the consumer's recognized right of personal data protection and what measures should be taken by the State to optimize this protection in a preventive way for users of computing services in the cloud.

ÍNDICE

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La tecnología que nuestros padres consideran mágica está evolucionando, lo que el día de ayer era novedoso, hoy en día es normal, y mañana será obsoleto. Todos hemos pagado por un iPod con más espacio de almacenamiento, ahora eso no es necesario, tenemos Spotify; hemos adquirido USB para transportar nuestra información, ahora tenemos Dropbox. Podríamos hacer innumerables reflexiones respecto a los cambios que ha generado el *cloud computing*, pero es mejor solo definirlo con unas cuantas palabras: el *cloud computing* posibilita la independencia entre nuestros datos y nuestra PC, ubicándolos en la WEB; este paradigma de internet es la herramienta más efectiva para lograr interoperabilidad, el cloud es la es la innovación de la innovación.

El *cloud computing* o nube de cómputo es un paradigma de Internet que, sin lugar a dudas, facilita y optimiza su funcionamiento; su existencia responde a la necesidad de brindar servicios en la red cuando los usuarios cuenten con una limitada plataforma local de almacenamiento (Cerda, 2012). Los servidores de Internet a través de la nube ofrecen servicios ágiles, efectivos y amigables con el usuario. Gracias a la nube tenemos acceso a nuestra información a cualquier hora o desde cualquier lugar. Pero no todo lo referente al *cloud computing* es maravilloso, y mucho menos cuando se trata del manejo de información.

Con el avance de la tecnología crecen las problemáticas jurídicas; se despliegan en el caso particular de la nube de cómputo, diversas situaciones para las que el derecho debe dar respuestas. Nacen, junto con el *cloud computing*, problemas en el área de propiedad intelectual, en el Derecho Penal, en aspectos del Derecho al Consumidor, violaciones a derechos intrínsecos de los particulares, como el de protección de datos personales; el presente estudio se centrará en el último punto enunciado.

Este trabajo se centra en el derecho a la protección de datos personales principalmente debido a las crecientes problemáticas y las desastrosas

consecuencias que se están evidenciando a nivel mundial por el mal manejo de información de los usuarios de internet. En los últimos tiempos este derecho ha adquirido popularidad en casos famosos con los que se han demostrado la posibilidad de poner un alto a actuaciones de empresas gigantescas como Dropbox, Google o Facebook.

Es importante mencionar que esta investigación intenta vislumbrar la posibilidad de proteger a los usuarios ecuatorianos comunes y corrientes que viven en estado de indefensión, de un incesante y enigmático avance tecnológico. Enfatizamos el hecho de que los datos de la mayoría de usuarios de Internet están en la nube, lo que ha despertado la pasión de la autora por entender más a fondo el tema del *cloud computing*, ligándolo con un derecho novedoso y complejo como el de la protección de datos personales.

Analizaremos en este trabajo de titulación específicamente la relación business to consumer (en adelante B2C) generada por las políticas de privacidad en las que Dropbox, como un ejemplo de proveedor de servicios de *cloud computing*, estipula la utilización y tratamiento de datos personales de consumidores ecuatorianos, sin que estos estén informados del hecho. Las cláusulas de dichas políticas de privacidad desde un inicio no son acordes a los principios del sistema preventivo de protección de datos personales, que consideramos elemental para precautelar este derecho.

La Constitución de la República de Ecuador reconoce el derecho a la protección de datos de carácter personal de las personas. Para que este derecho sea precautelado, el Estado ecuatoriano deberá implementar normativa que expresamente reconozca principios para el manejo de la información, y genere un sistema preventivo de protección de datos personales. Solo así se podrá amparar el derecho a la protección de datos personales de los ecuatorianos en casos particulares como el de la relación B2C con proveedores de servicios de *cloud computing*.

Por lo enunciado el presente estudio se centrará en establecer cómo la prestación de servicios de *cloud computing* en relaciones B2C puede afectar al derecho a la protección de datos personales reconocido a los ecuatorianos en el artículo 66 numeral 19 de la Constitución de la República del Ecuador. Considerando que al no existir normativa específica en la que se recojan principios para la protección de datos de carácter personal en el Ecuador, se crea una laguna jurídica en el derecho ecuatoriano. Este hecho puede dejar en indefensión a las personas frente al tratamiento abusivo de datos que podrían generar los prestadores de servicios de *cloud computing* en relaciones B2C, como se buscará evidenciar en el caso de Dropbox.

El presente trabajo entonces se estructurará de la siguiente forma: En el capítulo primero se definirá y explicará el modelo de prestación de servicios que constituye el *cloud computing*, estableciendo fases en relación con el tratamiento de datos personales. El capítulo segundo, generará un marco teórico que definirá y brindará pautas estandarizadas para comprender el derecho a la protección de datos personales y su aplicabilidad en la normativa ecuatoriana. Finalmente, el capítulo tercero desarrollará un análisis práctico que empate la teoría de los capítulos primero y segundo con el fin de dilucidar la necesidad de implementar en Ecuador normativa específica de protección de datos personales, que prevenga y ampare a los usuarios ecuatorianos en relaciones B2C, frente a los riesgos que genera el uso del *cloud computing*, riesgos que serán analizados a partir de las políticas de privacidad que rigen en el caso específico de Dropbox.

1 EL *CLOUD COMPUTING*

1.1 Antecedentes históricos del *cloud computing*

El término "*cloud computing"* es un anglicismo muy utilizado a nivel mundial que hace alusión a su equivalente en el castellano "nube de cómputo"; muchos utilizan las abreviaturas de *"el cloud"* o *"la nube"* para referirse a lo mismo.

La famosa "nube" surge como una metáfora de los diagramas de flujo de red utilizados para ilustrar al Internet, (Tellez, 2013, p. 1), y el término específicamente se refiere a "la forma de ver a una red de computadoras como proveedor de servicios de *software* y datos", (Cruz, 2012, p. 52). Comprender la razón de ser de este término es preponderante para entender que aunque imaginamos a nuestra información almacenada en una "nube", la misma siempre precisará de un soporte físico (*hardware*) de acopio.

El *cloud computing* revoluciona el concepto de internet que conocemos, gracias a este paradigma tecnológico la interoperabilidad de sistemas cada vez es más palpable para el usuario. Pero los servicios en la nube a los que hoy en día accedemos son producto de un devenir de antecedentes que llegaron a configurar lo que conocemos como *cloud computing.* Por lo enunciado es importante dar al lector una idea de los antecedentes históricos del cómputo en la nube, estos pueden resumirse en varios eventos de los que destacan los siguientes:

- Inicia de forma fehaciente a finales del siglo veinte; sin embargo, su concepto fue desarrollado con anterioridad a partir de los años sesenta con ideas desarrolladas por pensadores como J.C.R. Licklider, quien formuló la concepción de una *"red galáctica"* de computadoras capaz de comunicar a usuarios (Mohamed, 2009); o, John McCarthy, quien expuso la idea de la computación como una tecnología de tiempo compartido que podría venderse como un servicio público, conforme desprende de su famosa

frase *"algún día la computación se organizará como un servicio público".* (Tecayehuatl, 2012). Consideramos que ideas abstractas como las enunciadas son las que fomentan el avance de las tecnologías y su crecimiento durante el siglo XXI.

Por otro lado, la historia de los servicios de cómputo en la nube tiene sus inicios en el año 1999 con *Salesforce.com*, donde se ofertaban aplicaciones empresariales por medio de una página web. (Tecayehuatl, 2012). La existencia de este sitio web da la pauta para el posterior desarrollo de servicios de *cloud computing* a nivel mundial.

- Cuando el equipo técnico de Amazon a finales de los años 90, se percató que, de la inmensa infraestructura informática con que contaba únicamente utilizaba el 15% de su capacidad; desarrolló sistemas como el AWS (*Amazon Web Services*) en el año 2002. En el año 2006, Amazon creó el término *Elastic Compute Cloud (EC2)* referido a un servicio comercial que permite a pequeñas y medianas empresas alquilar servidores donde pueden poner a funcionar sus aplicaciones. (Mazuecos, 2013). En el año 2006, también apareció el famoso *Google docs*, con el que se socializó el *cloud computing.* (Tecayehuatl, 2012). Sin embargo, desde la misma existencia del correo electrónico (que data al año 1971) ya se aplicaban ideas que dieron nacimiento a la nube de cómputo.

- Finalmente, durante los años 2007 y 2008, compañías como IBM conjuntamente con universidades estadounidenses iniciaron una investigación acerca del *cloud computing*. Fruto de dicha investigación, en enero de 2009 salió a la luz la plataforma de código abierto *Eucalyptus.* (Escamilla, 2012). A partir de la existencia de *Eucalyptus* se difunde mucho más la nube de cómputo.

El surgimiento del *cloud computing* tiene su fundamento en el desarrollo paulatino de diferentes arquitecturas tecnológicas que se evidencia a nivel

mundial desde los años sesenta (Escamilla, 2012), mismas que se especifican a continuación:

- ***Mainframes.-*** Fueron las primeras computadoras lanzadas al mercado por IBM a principios de los años 60, estos ordenadores presentaban deficiencias debido a su alto costo y dificultades para su utilización y mantenimiento. Debido a esto, IBM desarrolló nuevos equipos más económicos e interconectados entre sí. (Aalbers, 2013). Los *mainframes* fueron computadoras inmensas que no llegaron a ser difundidas al público en general.

- ***Utilitycomputing.-*** Debido al alto precio de los *mainframes*, las empresas pensaron en pagar únicamente por el tiempo de uso de estos ordenadores. Bajo este concepto nace Electronic Data Systems en 1962, este modelo de negocio se desarrolló por un tiempo, pero debido a la flexibilidad de la informática y baja de precios, no se generalizó. (Aalbers, 2013). Con la difusión de los ordenadores personales, los *mainframes* fueron despojados del mercado, desarrollándose paulatinamente el mercado de ordenadores personales.

- ***Gridcomputing.-*** Este modelo nace de la idea de varias universidades de resolver problemas complejos a través del uso de grandes cantidades de equipos económicos, con arquitectura *hardware* estándar. Las ideas macro de este modelo hoy en día perduran con el *cloud computing,* de las que destaca la del "uso de un *hardware* económico y *software* estándar para resolver problemas complejos, abaratando de esta forma costos". (Aalbers, 2013). Con la actuación conjunta de estudiantes universitarios a través de interconexión de muchos ordenadores personales, fue posible el desarrollo de productos tecnológicos inimaginables, un ejemplo claro de es la película de *Toy Story*, la que fue producida gracias al desarrollo de ideas de *gridcomputing*.

Es evidente que al *cloud computing* le anteceden ideas de avance tecnológico y crecimiento empresarial, por un lado, la optimización de los servicios de cómputo y arquitecturas tecnológicas; y, por otro, la eficiencia en negocios y baja de costos para las empresas que utilizan sistemas de cómputo.

1.2 Concepto de *cloud computing* o nube de cómputo

En realidad no existe un concepto exclusivo que defina al *cloud computing* en su amplitud, sin embargo, una de las definiciones más amplias y con mayor aceptación global es la brindada por el Instituto Nacional de Estándares y Tecnología NIST que señala lo siguiente:

> "El cómputo en la nube es un modelo que permite el acceso oblicuo, conveniente y bajo demanda de red a un conjunto de recursos informáticos configurables (por ejemplo redes, servidores, almacenamiento, aplicaciones y servicios) que puedan ser rápidamente proveídos con esfuerzos mínimos de administración o interacción con el proveedor de servicios. Este modelo en la nube promueve la disponibilidad y se compone de cinco características esenciales, tres modelos de servicios y cuatro modelos de implementación." (2011)

Varios autores se basan en la anterior definición para configurar una propia, este es el caso de Tellez, quien termina definiendo al cómputo en la nube como "[…] un ecosistema de recursos tecnológicos de la información y la comunicación, que ofrece servicios escalables, compartidos y bajo demanda en diferentes modalidades y a diversos usuarios a través de Internet." (2013, p. 5)

Para la Agencia Española de Protección de Datos el *cloud computing* es "[…] una nueva forma de prestación de los servicios de tratamiento de la información, válida tanto para una empresa como para un particular y, también, para la Administración Pública." (2013, p. 5)

Una definición más técnica es la que brindan los autores Hurwitz, Kaufman y Harper al indicar:

> "*Cloud computing* es un método para proveer un conjunto de recursos de computación compartida que incluye aplicaciones, computación, almacenamiento, creación de redes, desarrollo, y plataformas de desarrollo así como procesos de negocio. El *cloud computing* convierte a los tradicionales silos activos informáticos en un grupo compartido de recursos basados en la fundación subyacente del Internet." (2012, p. 6)

Para Joyanes la nube no es solamente Internet aunque se fundamente en este, es un conjunto de *hardware*, *software* e interfaces que conjuntamente facilitan el tratamiento de la información como un servicio. Los servicios que se ofrecen a través de la nube incluyen *software*, infraestructura y almacenamiento en la red, como componentes independientes o como una plataforma completa, basados en la demanda del usuario. El autor también hace referencia a los actores y participantes de la nube, entre los que están: los proveedores, quienes proporcionan la tecnología y servicio; los socios, que crean servicios para la nube facilitando el acceso de los clientes; los líderes de negocio que evalúan los servicios para adoptarlos con posterioridad en sus compañías; y, los usuarios finales que utilizan los servicios. (2012a, pp. 11-12)

Conforme a las definiciones brindadas, se puede concluir que el *cloud computing* o nube de cómputo es un modelo innovador compuesto por un conjunto de *hardware*, *software* e interfaces destinados a la prestación de servicios TIC, modelo mediante el cual sus proveedores brindan acceso a gran escala y bajo demanda a sus usuarios finales, aportando beneficios sociales y económicos para todos sus actores.

Como se ha mencionado los conceptos que trae consigo el *cloud computing* revolucionan la Web que todos conocemos. Hoy en día la interoperabilidad de sistemas cada vez es más palpable para los usuarios, las facilidades que se ofertan son bastante atractivas al consumidor. Son innegables las facilidades que la nube brinda a las personas, lo que repercute, sin lugar a dudas, incluso en el desarrollo de la sociedad.

Finalmente, Huibert hace una reflexión muy interesante respecto a la conceptualización del *cloud computing* definiéndolo como el resultado de buscar la mayor eficiencia posible en la asignación de recursos informáticos. Para especificar dicho enunciado, el autor realiza una analogía entre lo que fue la línea de producción para la industria automotriz del siglo XX con lo que el *cloud computing* supondrá para la industria informática en el futuro. Nosotros consideramos que esta analogía no solo predice lo que será el *cloud computing* en un futuro próximo, sino que confirma la necesidad del mundo entero de extender la industria informática y sacar frutos de la misma.

En el contexto de este trabajo es importante tener en cuenta que independientemente de sus novedosas características y de los cambios radicales que pueda generar el *cloud computing,* existe en Ecuador el derecho a la protección de datos personales, que sin importar las innovaciones tecnológicas, impondrá obligaciones a los responsables de tratamiento de datos para prevenir posibles afectaciones a los usuarios.

1.3 Funcionamiento del *cloud computing*

Para entender la forma en que funciona la arquitectura de la nube de cómputo, es importante estar al tanto de que, no existe una regla que generalice una definición aplicable para toda la dinámica técnica inmersa dentro de dicho sistema. Por lo tanto, comprender el funcionamiento del *cloud computing,* solo será posible al relacionar las tecnologías que dan vida a este modelo de prestación de servicios informáticos.

Igualmente, sería inútil estancar el presente estudio en tecnicismos que describan a cabalidad cada tecnología y sistema inmersos en el modelo de *cloud computing.* Para la el entendimiento del *cloud computing* basta atender a los parámetros brindados por Jonathan Strickland (2008) en su artículo titulado "*how cloud computing works",* quien didácticamente divide a este sistema en dos secciones: el *"front end"* y el *"back end".*

El *"front end"* (Véase Figura 1) está compuesto del usuario final, quien accederá a los servicios que se proporcionan en la nube de cómputo a través de distintos dispositivos que naveguen en red; ya que, en la actualidad tener acceso a Internet es un requisito indispensable para utilizar varios servicios en la nube.

El *"back end"*, por otro lado, está conformado por toda la arquitectura inmersa detrás de la idea de la nube de cómputo. Dicha arquitectura es una combinación de redes de computadores, servidores, bases de datos, que se valen de sistemas de virtualización para ser controladas. Las órdenes que son enviadas del *"front end"* son procesadas y atendidas de forma casi automática, sin necesidad de interacción entre seres humanos, esto se da gracias al nodo de control de los sistemas virtualizados en el *"back end"*.

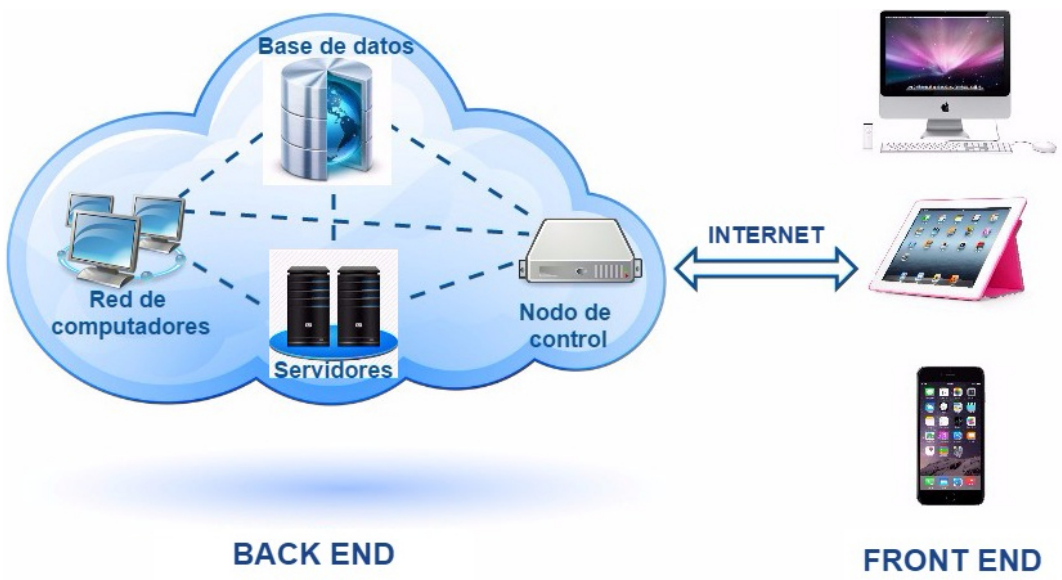

Figura 1. **Funcionamiento del *cloud computing***

Adaptado de "*How Cloud Computing Works*", por Strickland, 2008, p. 1.

Es importante mencionar que el sistema descrito en la realidad tiene una dimensión incalculable, es más, las compañías proveedoras de servicios *cloud computing* más conocidas en la actualidad como Dropbox o Google, cuentan con muchas plantas de *"back end",* también conocidas como "granjas informáticas".

Dichas granjas informáticas están ubicadas indistintamente al rededor del mundo, pero pueden ser controladas de forma central gracias a la virtualización.

Debido a que el *cloud computing* nace de la idea de reemplazar lo físico por lo virtual, para concebir su funcionamiento también es importante tener claro que todo *software* precisa de un *hardware* para existir, aunque el segundo sea imperceptible para los que somos usuarios de servicios en la nube. Es así que el "*back end"* al que se refiere Strickland representa toda la arquitectura de *hardware* que manejan los proveedores de cómputo en la nube para ofertar sus servicios en el mercado.

1.4 Características distintivas del *cloud computing*

Con las características de la nube nos referimos a las peculiaridades que distinguen y particularizan, al modelo de *cloud computing*. Al igual que en la definición, existen varias posturas al respecto, sin embargo la generalidad de autores concuerda con las cinco características que han sido planteadas por el Instituto Nacional de Estándares y Tecnología (NIST), que son las siguientes:

- Auto servicio bajo demanda (*On-demand self-service*)
- Acceso ubicuo a la Red (*Broad network access*)
- Reservas de recursos en común (*Resource pooling*)
- Rápida elasticidad (*Rapid elasticity*)
- Servicio supervisado (*Measured service*). (2013)

1.4.1 Autoservicio bajo demanda

Varios autores tratan a esta característica con distintas denominaciones (auto servicio, pago por uso, etc.) pero bajo el mismo precepto. Básicamente, un usuario de *cloud computing* puede auto proveerse (no hay interacción humana con el proveedor) de servicios TIC acorde a sus necesidades, es decir, conforme vayan evolucionando estas necesidades, el usuario tendrá que pagar

únicamente por la cantidad de servicio que consume del proveedor. Al respecto, NIST ha manifestado lo siguiente:

"Un consumidor se puede provisionar unilateralmente de capacidades de computación, como tiempo de servicio, almacenamiento en red, dentro de sus necesidades de forma automática sin requerir interacciones humanas con cada proveedor de servicios." (NIST, 2013)

Gracias a esta característica, el usuario de *cloud computing,* para provisionarse de servicios en la nube únicamente deberá solicitarlos en línea (la mayoría de veces el servicio es proveído de forma automática) y realizar el respectivo pago del mismo.

Para mayor comprensión del lector, en el caso de Dropbox, cuando la persona natural "X" tiene una cuenta gratuita con 2 GB de capacidad de almacenamiento, y desea contratar más espacio en un plan de 1 TB. Para que "X" tenga 1 TB de espacio en Dropbox deberá realizar el pago por el servicio en internet, y automáticamente se estará proveyendo del plan de 1 TB que Dropbox oferta en la nube. La forma de abastecerse de servicios de *cloud computing* ejemplificada es la razón por la que al cómputo en la nube se lo caracteriza como un "autoservicio bajo demanda".

1.4.2 Acceso ubicuo a la Red

Con "ubicuo" se hace referencia al acceso que se tiene a los datos desde cualquier lugar y en cualquier momento, evidentemente, será necesario estar conectado a la red para disfrutar de los servicios de *cloud computing.* (INTECO, 2011, p. 14). Los mecanismos de acceso a la red son heterogéneos, no es necesario contar con aplicaciones o programas destinados específicamente al acceso a los servicios de *cloud computing*.

Tellez expone "las capacidades están disponibles en la red y se accede a ellas a través de mecanismos estándar que promueven el uso de plataformas

heterogéneas tanto ligeras como pesadas (por ejemplo, teléfonos móviles, computadoras portátiles y otros dispositivos).” (2013, p. 6). Es primordial considerar que esta característica se encuentra ampliamente ligada la convergencia tecnológica, o a principios del comercio electrónico, como el de neutralidad tecnológica o el de equivalencia funcional.

El cómputo en la nube existe gracias al Internet; los servicios que se ofertan hallan su sustento en la existencia de una red de redes mundial, a la que se puede acceder por medio de diversos dispositivos y en cualquier lugar. Donde se pueda acceder a la web será posible disfrutar de los beneficios del *cloud computing*.

La característica de acceso ubicuo a la red se puede ejemplificar claramente en el caso de Dropbox. Si el usuario “X” almacena archivos en la nube por medio de su cuenta Dropbox, todos estos archivos serán accesibles desde cualquier lugar, dispositivo y en cualquier momento. Lo único que “X” necesitará será ingresar a su cuenta de Dropbox (para lo cual será necesario que tenga conexión a internet).

1.4.3 Reservas de recursos en común

Esta característica es, sin lugar a duda, la más compleja e innovadora de todas, y constituye el pilar del *cloud computing*. La infraestructura que utiliza un proveedor de servicios de cómputo en la nube para el tratamiento y almacenaje de información de sus usuarios es compartida entre todos ellos (multi-tenencia). (Barnitzke, Corrales y Forgó, 2011, p. 18)

El funcionamiento de dicha infraestructura está basado en varias tecnologías de virtualización, que asignan y reasignan dinámicamente los recursos físicos conforme a la demanda del consumidor. (Joyanes, 2012b, p. 94). Estas tecnologías son utilizadas por los proveedores para ofrecer sus servicios, por lo que es imposible determinar a ciencia cierta la localización de la información de sus usuarios. (INTECO, 2011, p. 15)

Respecto a esta característica Barnitzke y otros consideran, por un lado, que “los datos se transfieren de un lugar a otro, dependiendo de donde haya recursos disponibles” y, por otro lado, que “el proveedor del servicio de nube (no el consumidor del servicio) determina la ubicación de los datos, el estándar del servicio y el estándar de la seguridad.” (2011, p. 18)

Es importante considerar que la mayoría de dificultades que despliega el *cloud computing* respecto a la aplicabilidad del derecho a la protección de datos personales, emergen particularmente de esta característica, porque debido al dinamismo con que viaja la información, es muy complicado determinar la ubicación exacta de los datos personales; quiénes efectivamente tienen acceso al tratamiento de los mismos, y los estándares de seguridad que deberán implementar para cada caso.

Así que, resultará complejo determinar a ciencia cierta el ámbito de aplicación de la normativa así como establecer responsabilidades a los actores, esto debido a que los lugares físicos en que se almacenan los datos podrán ser asignados y reasignados constantemente entre varios actores, en atención a una diversidad de propósitos (mantenimiento, requerimiento de más espacio, descargas que realiza el usuario, etc.).

Para ejemplificar la característica de reservas de recursos en común se utilizará el siguiente caso: por un lado el usuario “X” que vive en India, tiene almacenados archivos (fotos, documentos, videos) que pesan 2 GB en su cuenta con Dropbox. Por otro lado, el usuario “Y” que vive en Ecuador también tiene archivos que pesan 2 GB almacenados en su cuenta Dropbox. Imaginemos que al igual que “X” y “Y”, millones de personas de Canadá, Brasil, Colombia, Honduras y muchos otros países tienen los mismos 2 GB de archivos almacenados en su cuenta Dropbox.

Para el proveedor de servicios de *cloud computing* sería imposible asignar un espacio determinado a cada uno de sus usuarios (a “X” solo se le concederá espacio en el *data center* de India), ya que maneja tanta información de sus

usuarios a nivel mundial, y recibe tantas solicitudes de espacio diarias, que simplemente le sería inmanejable conocer a ciencia cierta dónde están los archivos de cada uno. Para poder dar recursos de forma automática y a tantas personas en el mundo entero, Dropbox utiliza tecnologías que le permiten asignar y reasignar espacio de almacenamiento a cualquier persona y en cualquier lugar indistintamente. Es decir, si "X" tiene 2 GB de archivos en la nube, puede ser que 1 GB esté almacenado en un *data center* de Estados Unidos y el otro 1 GB en India junto con 1GB de datos de "Y". La ubicación del *data center* no será de importancia, pues "X" no dejará de tener acceso ubicuo a sus archivos subidos a la nube por medio de su cuenta Dropbox.

Esta forma de almacenar los datos, ejemplificada en el caso de Dropbox, es la razón por la cual al *cloud computing* se le atribuye la característica esencial de "reservas de recursos en común", sin la cual no constituiría un servicio de cómputo en la nube.

1.4.4 Rápida elasticidad

Los servicios de *cloud computing* son proporcionados a sus usuarios de forma rápida (muchas veces automática), y elástica debido su adaptabilidad y facilidad de implementación. Un ejemplo claro de esto se da cuando un usuario precisa más espacio en la nube, para lo cual, sólo deberá realizar el pago en línea y automáticamente lo recibirá. Esta característica para Joyanes da la impresión de que los servicios de *cloud computing* son ilimitados y pueden ser adquiridos en cualquier momento. (2012b, p. 94)

Esta característica va de la mano con la de "reservas de recursos en común", debido a que frente a un requerimiento de espacio para almacenar, dichos recursos físicos serán asignados de forma automática respondiendo a la multi-tenencia del *cloud computing*.

Para comprender la agilidad y dinámica de los servicios de *cloud compiting*, hay que interrelacionar sus características, que responden a un tipo de

funcionamiento específico. Así pues, la atención rápida que brinda el *cloud computing* a los requerimientos de sus usuarios tiene su fundamento en la asignación dinámica de sus recursos físicos.

Para ejemplificar lo expuesto se plantea el siguiente ejemplo: El usuario "X", desea almacenar en su cuenta Dropbox una carpeta de fotografías que pesa 2GB. El servicio de *cloud computing,* por su naturaleza, de forma automática permitirá que dicho usuario suba los archivos a la nube. Detrás de esta acción existe una asignación automática de 2GB en espacio físico que oferta Dropbox, estas fotografías serán accesibles al dueño de la cuenta en cualquier momento pues están archivadas en la nube. Sin embargo, el *hardware* que almacena los archivos será siempre un incógnito para su dueño, los que siempre estarán circulando alrededor de varios *data centers* conforme a la disponibilidad de espacio que exista (podrán darse casos en que en el *Data center* de China existía disponibilidad de 1GB, y en el de India de 1GB; los 2GB estarán ubicados en ambos países, pero serán accesibles al usuario en cualquier momento que ingrese a su cuenta Dropbox).

1.4.5 Servicio supervisado

Los sistemas de cómputo en la nube controlan el uso de recursos para hacerlos óptimos de forma automática. (NIST, 2013). Esta característica brinda transparencia a los servicios de *cloud computing,* tanto para sus *usuarios,* como para sus *proveedores.* Debido a este control, el uso de sistemas de cómputo en la nube, puede seguirse, controlarse y notificarse, contribuyendo así a la transparencia. (Alcocer, s.f.)

Para Melaños (2013, p. 23) por medio de los sistemas de *cloud computing* se controla y optimiza automáticamente el uso de los recursos, con lo que se aprovecha la capacidad de medición que posibilita su monitoreo y control, lo que brinda transparencia del servicio ante el proveedor y el usuario.

Para que el sistema de cómputo logre optimizar los recursos de manera automática, será necesario tratar la información de sus usuarios relacionando al número de sus cuentas activas, información como: los recursos de almacenamiento que demandan, el tipo de procesamiento de información que realizan o el ancho de banda que manejan. En definitiva, información que permita perfilar a sus usuarios para de esta forma brindarles un servicio óptimo y transparente acorde a sus necesidades.

Si bien el usuario se mantendrá informado de los servicios que ha contratado, y el proveedor realizará una mejora continua de sus servicios, acrecentando su negocio, no se puede negar que el proveedor estaría realizando tratamiento de la información relativa a sus usuarios, y por lo tanto, debe cumplir con las obligaciones que le impone el derecho a la protección de datos personales, para el buen desempeño de sus actividades.

Estas características brindan una visión amplia de las razones por las cuales los servicios en la nube han aumentado considerablemente los últimos años y de los evidentes beneficios que brindan al usuario.

Nosotros consideramos que la fusión de las cinco características enunciadas, ofrece un servicio diferente, ágil y económico; y, a pesar de que estas no son innovadoras al evaluarse disyuntivamente, en conjunto conforman la esencia del paradigma tecnológico del cómputo en la nube. Para los fines de este trabajo, es preciso comprender a cabalidad las características expuestas, que, por constituir en conjunto los pilares del *cloud computing*, también generan las problemáticas en la aplicación de normativa destinada a resguardar de manera preventiva el derecho a protección de datos personales.

1.5 Actores partícipes en el *cloud computing*

Para esclarecer el funcionamiento del *cloud computing*, es necesario definir los actores que participan en este modelo de prestación de servicios. (Research Centre on IT and Law [CRID], 2010, p. 11)

1.5.1 El proveedor

Persona natural o jurídica que oferta servicios de computación en la nube (IaaS, PaaS y SaaS) a nivel mundial a través del Internet. Los proveedores de servicio, para fines de aplicación preventiva de la normativa de protección de datos personales deben distinguirse entre:

1.5.1.1 Responsable de tratamiento (*data controller*)

La figura de responsable de tratamiento hace alusión a aquella persona (en la mayoría de casos jurídica) que determina el fin del tratamiento de los datos, es decir, decide sobre las cuestiones de fondo que lo legitiman, y por ende, es quien se responsabiliza frente a los titulares de la información. (Grupo del artículo 29 sobre protección de datos, 2010, p. 16)

En el *cloud computing* dependerá del tipo de servicios que se presten y los actores involucrados para determinar responsabilidades. En el caso específico de esta investigación, en que se analiza la relación directa B2C (buisness to consumer) entre el proveedor de servicios de *cloud* y el usuario final, será el proveedor quien cumpla con las funciones de responsable de tratamiento.

1.5.1.2 Encargado de tratamiento (*data procesor*)

El encargado de tratamiento presta servicios externos de negocio y tecnología al responsable de tratamiento, con la finalidad de apoyarlo en el cumplimiento de sus labores. (Cloud Security Alliance [CSA], 2011, p. 26). Para que una persona actúe como encargado del tratamiento deberán concurrir dos condiciones básicas: por una parte, ser una entidad jurídica independiente del responsable del tratamiento y, por otra, realizar el tratamiento de datos personales por cuenta de éste. (Grupo del artículo 29 sobre protección de datos, 2010, pp. 36-37). Esta figura en el derecho a la protección de datos personales no ha sido tratada a fondo y siempre se la ha subordinado a un responsable de tratamiento.

Para el tratamiento de datos en *cloud computing*, será preciso que se realice un análisis preventivo pormenorizado del papel que cumplen tanto el responsable como el encargado de tratamiento, ya que la actuación de estos actores puede resultar hasta cierto punto confusa, y en dichos casos una solución podría ser asignar obligaciones específicas para cada uno de los actores. Para el desarrollo del presente estudio la figura de encargado de tratamiento pasa a tomar un papel secundario en el análisis, puesto que nos centraremos en el proveedor de servicios de *cloud computing* en relaciones B2C, caso en el cual este pasará a ser el responsable de tratamiento.

1.5.2 El usuario

Son las personas naturales o jurídicas que contratan servicios de computación en la nube con los proveedores de servicio; el usuario, en la mayoría de casos es el destinatario final del servicio, aunque en otros puede no serlo. (CRID, 2010, p. 11). Para fines de aplicación preventiva de la normativa de protección de datos personales, será preciso identificar los siguientes tipos de usuarios que podrían presentarse:

1.5.2.1 El suscriptor

Este actor puede, como puede no ser la misma persona que el usuario, esto dependerá del caso. Por ejemplo, cuando el usuario de *cloud computing* es una empresa, y sus empleados son quienes se suscriben al servicio contratado, el suscriptor del servicio de *cloud computing* será el empleado, mientras que la empresa continuará siendo usuaria del servicio (pues es quien lo contrató con el proveedor).

1.5.2.2 Los interesados (*data subject*)

La propuesta de Reglamento General de Protección de datos de la Unión Europea define a los interesados en su artículo segundo como:

> "Toda persona física identificada o que pueda ser identificada, directa o indirectamente, por medios que puedan ser utilizados razonablemente por el responsable del tratamiento o por cualquier otra persona física o jurídica, en particular mediante un número de identificación, datos de localización, identificador en línea o uno o varios elementos específicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona." (Propuesta RGPD, art. 2)

En definitiva, si por medio del tratamiento de sus datos personales, una persona puede ser identificada por el responsable o encargado del fichero, esta persona será el interesado. En el caso del *cloud computing*, los usuarios o suscriptores podrían ser identificados como interesados, para lo cual será preciso determinar las circunstancias de cada caso concreto.

1.5.3 Los terceros

Se conoce como "terceros" a todas aquellas personas naturales o jurídicas que no forman parte del acuerdo para la prestación de servicios de *cloud computing*; y, por ende, no tienen legitimidad o autorización específica para tratar datos personales del usuario. En el contexto de la protección de datos personales los terceros no son ni interesados, ni responsables de tratamiento, ni encargados de tratamiento. (Grupo del artículo 29 sobre protección de datos, 2010, p. 34-35). Sin embargo, si un tercero recibe legítima o ilegítimamente datos personales y llega a cumplir de facto las condiciones para que pueda considerarse responsable del tratamiento, se verá obligado a cumplir con las obligaciones que se le imponen a dicho actor

Para efectos de la presente investigación, debido a que la misma se centra en la relación B2C entre usuarios ecuatorianos y proveedores de servicios de cómputo en la nube, es importante señalar que, en el contexto de la protección de datos personales, el proveedor de servicios de *cloud computing* será el responsable de tratamiento y el usuario del servicio será el interesado.

1.6 Clasificación de los modelos de servicio e implementación del *cloud computing*

La clasificación del *cloud computing* se divide en tres modelos de servicio y cuatro modelos de implementación, conforme se desprende de la información brindada por NIST. (2013, p. 9). Es importante considerar que conforme a los servicios específicos que brinde cada proveedor, podrán combinarse modelos de servicio con modelos de implementación, es decir no son excluyentes los unos de los otros.

1.6.1 Modelos de servicio del *cloud computing*

También conocidos como *niveles de servicio* o "*Modelo SPI"*, se refieren al cómo y para qué utilizarán los usuarios de *cloud computing* estos servicios. (Acevedo, 2010). Los proveedores de *la nube* ofertan acceso a recursos informáticos a través de la red, adaptando estos a las necesidades de cada cliente, brindando soluciones de Infraestructura como Servicio, Plataforma como Servicio y *Software* como Servicio. (Agencia Española de Protección de Datos [AGPD], 2013). Cada modelo de servicio se refiere a una forma de utilización del *cloud compunting*, sin embargo, para estos tres aplican indistintamente las ideas y características esenciales de este modelo de prestación de servicios, independientemente del nivel de almacenamiento y el nicho de mercado al que se proyecten.

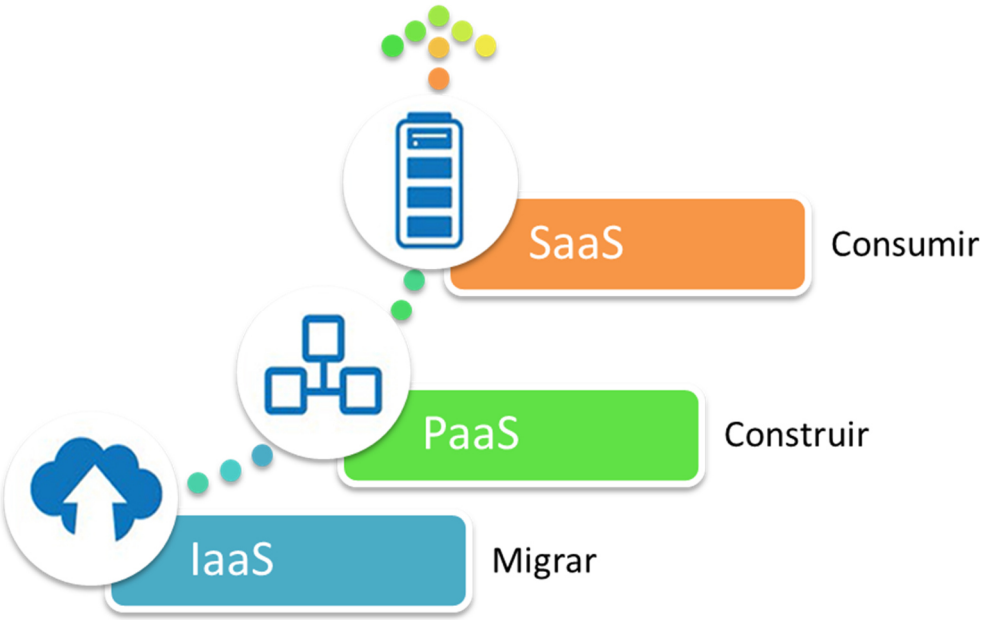

Figura 2. **Modelos de servicio del *cloud computing***

Adaptado de "*Cloud computing solutions*: iaas, paas, saas", por Khang, 2014

1.6.1.1 Infraestructura como Servicio (IaaS)

El proveedor de servicios de cómputo en la nube a través del nivel IaaS ofrece una vasta infraestructura, que le permite al usuario manejar un amplia gama de recursos de computación, tales como: capacidad de almacenamiento, procesamiento, y desarrollo de aplicaciones en máquinas virtuales. (Salas y Colombo, 2012, p. 54)

Este modelo de prestación de servicios es el más ejemplificativo de los tres para describir al *cloud computing,* pues el usuario se provee únicamente de los recursos informáticos que necesita, y, en lugar de comprarlos e instalar su propio centro de datos, los alquila. (Joyanes, 2012a, p. 76)

Para algunos autores este nivel puede llegar a representar una evolución de los Servidores Privados Virtuales (o sus siglas en inglés VPS) que ofrecen los proveedores de servicio de alojamiento (INTECO, 2011, p. 9); esto debido a que el IaaS es el nivel más básico de *cloud computing*, y dio la pauta para su posterior

avance a niveles más complejos como el PaaS o el SaaS. En concordancia con lo antes expuesto, es importante considerar la definición brindada por NIST del IaaS:

> "La infraestructura como servicio es la capacidad que se da al consumidor al proporcionarle procesamiento, almacenamiento, redes y otros recursos de computación en los que es capaz de desplegar y ejecutar *software*s específicos que pueden incluir sistemas operativos y aplicaciones. El consumidor no gestiona ni controla la infraestructura fundamental de la nube, sin embargo, tiene el control sobre los sistemas operativos, almacenamiento, aplicaciones desplegadas y, en su caso, control limitado sobre ciertos componentes específicos de redes." (NIST, 2013, p. 9)

A continuación, para mayor entendimiento de lo que comprende el modelo de prestación de servicios de *cloud computing* IaaS, se expone una figura en el que se puede observar que en base al funcionamiento general del *cloud computing.* Con el modelo IaaS los usuarios tendrán acceso a una infraestructura de almacenamiento en la nube que podrán administrar por sí mismos, de este tipo de servicio existen ejemplos como Amazon Web Services, con servicios como EC2, Wmware, GoGrid, etc. (Joyanes, 2012a, p. 75)

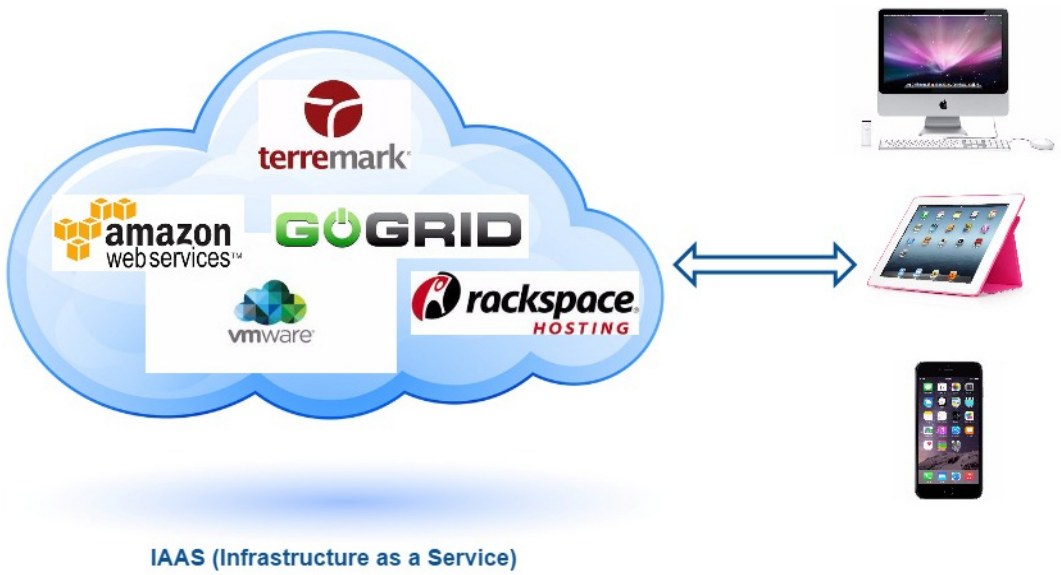

Figura 3. **El modelo IaaS de *cloud computing***

Adaptado de "Computación en la nube: estrategias del *cloud computing* en las empresas", por Joyanes, 2012a, p. 75

El nivel IaaS, por su naturaleza y complejidad, está direccionado a un mercado compuesto en su mayoría de personas jurídicas. Generalmente son las empresas las que precisan tener infraestructuras completas, que les permitan poner en funcionamiento sus sistemas operativos, y considerando el alto coste que significa adquirir, actualizar y mantener servidores, optan por contratar servicios IaaS en la nube.

Cuando un proveedor de servicios de *cloud computing* presta servicios a empresas o compañías, generalmente se negocian las cláusulas principales del contrato y estos dejan de ser de adhesión (como en los casos de SaaS y PaaS). Por lo mencionado, es evidente que la mayoría de contratación electrónica de servicios IaaS se da en relaciones B2B, aunque esto no es una regla general y también podrán existir casos de contratación B2C.

Cuando las relaciones son B2B, igual deberá precautelarse de forma preventiva el derecho a la protección de datos personales, las responsabilidades de los actores partícipes serán distintas a las que se generan en relaciones B2C, es importante recordar al lector que este trabajo se centra únicamente en las segundas.

1.6.1.2 Plataforma como Servicio (PaaS)

Los proveedores de servicios de *cloud computing* al nivel de PaaS proporcionan a sus usuarios una plataforma de desarrollo virtual alojado en la nube, (Joyanes, 2012a, p. 74), evitando así gastos de compra y mantenimiento del *hardware* y *software*. Las aplicaciones en este modelo de servicios se despliegan utilizando un conjunto determinado de lenguajes y herramientas de programación, (Salas y Colombo, 2012, p. 52). Una desventaja que podría presentar ese modelo es que el usuario estará limitado a utilizar únicamente las herramientas y lenguajes que prestan los proveedores, (Skytap, 2011), manteniendo así el control de la aplicación, pero no el de la infraestructura subyacente a esta. (Joyanes, 2012b,

p. 95). Para aclara de mejor forma el funcionamiento del PaaS, podemos observar el siguiente criterio:

> "En la plataforma como servicio, la capacidad proporcionada al consumidor es para desplegar en la infraestructura de nube aplicaciones adquiridas o creadas por el consumidor, utilizando lenguajes y herramientas de programación soportadas por el proveedor. El consumidor no administra la infraestructura de nube subyacente que incluye la red, servidores, sistemas operativos o de almacenamiento, pero tiene el control sobre las aplicaciones desplegadas y la posibilidad de controlar las configuraciones de entorno del hosting de aplicaciones." (Tellez, 2013, p. 7)

La siguiente figura ejemplifica el modelo de prestación de servicios PaaS de cómputo en la nube, a través del que se brinda a los usuarios la facilidad de gestionar sus aplicaciones en una plataforma ubicada en la nube, para este caso se pueden brindar ejemplos como lo es el famoso Facebook, Google Apps Engine o Microsoft Azure.

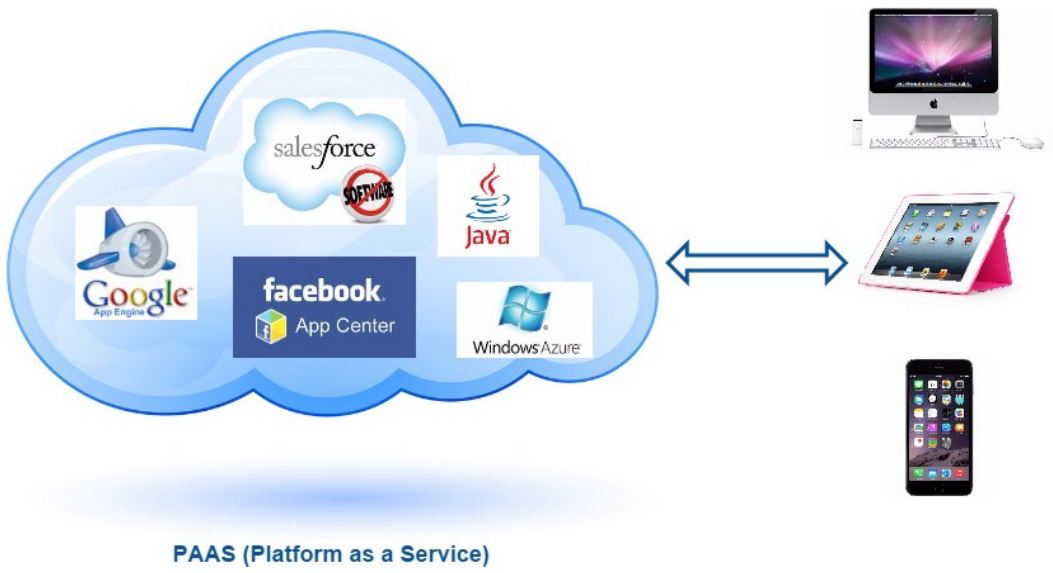

Figura 4. **El modelo PaaS de *cloud computing***

Adaptado de "Computación en la nube: estrategias del *cloud computing* en las empresas", por Joyanes, 2012a, p. 74

Este nivel de prestación de servicios del PaaS es intermedio, por un lado el usuario del servicio tiene el control de las aplicaciones que oferta por medio de la nube, sin embargo, no puede administrar la infraestructura de *cloud computing* inmersa detrás (*"back end")* de sus aplicaciones.

Estos servicios están direccionados a un mercado compuesto por personas jurídicas y naturales indistintamente, existirán tanto relaciones B2C, como B2B.

En el PaaS también con un solo *"click"* el cliente acepta los términos y condiciones que establezca el proveedor. Sin embargo, en los casos de PaaS el usuario paga por el servicio y, la mayoría de veces, está consciente de lo que está contratando. En el caso de PaaS, el usuario de los servicios no tiene el mismo nivel de desconocimiento de lo que implica su contratación, como en el nivel SaaS; esto debido a que este nivel de prestación de servicios es más complejo y precisa de cierto nivel de comprensión por parte del usuario para acceder al mismo. Aunque con independencia del nivel SaaS o PaaS, el proveedor de servicios de *cloud computing* siempre deberá observar los estándares del derecho a la protección de datos personales para prevenir posibles riesgos al derecho a la protección de datos personales de sus usuarios.

1.6.1.3 Software como Servicio (SaaS)

Este modelo es el más difundido de los tres, por la comodidad que ofrece y, además, porque muchas veces es gratuito. Con este modelo se ofrece a los usuarios aplicaciones ya creadas, que se ejecutan en la infraestructura de la nube, prescindiendo de una plataforma personal; así se elimina la necesidad de instalar y operar la aplicación únicamente en la computadora del usuario. (Salas y Colombo, 2012, p. 50). Tellez desarrolla más a fondo la definición de este modelo de servicios cuando expresa:

> "En el *software* como servicio, la capacidad proporcionada al consumidor consiste en utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura de nube. Puede accederse a las aplicaciones desde varios dispositivos del cliente a través de una interfaz de cliente ligero como un navegador de Internet (por

> ejemplo, correo web). El consumidor no gestiona la infraestructura de nube subyacente que incluye la red, servidores, sistemas operativos, almacenamiento o incluso capacidades de aplicaciones individuales, con la posible excepción de unos parámetros de configuración de la aplicación específica del usuario." (2013, p. 5)

Nosotros consideramos, que al ser esta la expresión más avanzada de *cloud computing,* hay variedad de ejemplos de SaaS en la red, y debido a su amplitud suelen ofrecerse de forma gratuita. La figura siguiente enumera algunos programas muy conocidos por el público en general que pertenecen al modelo de prestación de servicios SaaS del *cloud computing.* Es importante considerar que dichos *software* se caracterizan por precisar de conexión a internet para ser ejecutados, es así que de este modelo de servicios destacan ejemplos como: iCoud, Google docs, Gmail, Dropbox, etc.

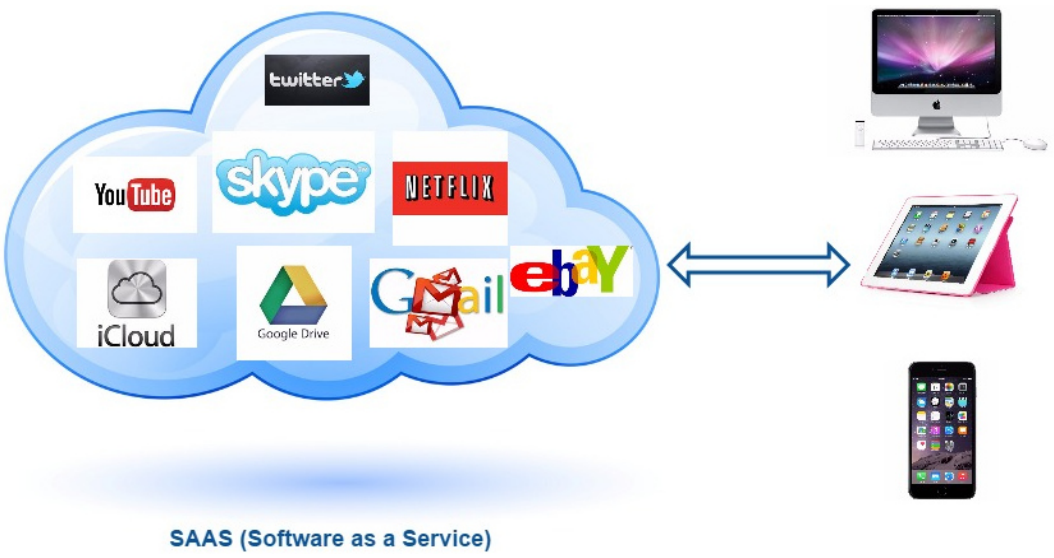

Figura 5. **El modelo SaaS de *cloud computing***

Adaptado de "*Lex cloud computing",* por Tellez, 2013, p. 5

El nivel SaaS ofrece una variedad de servicios direccionados a un mercado compuesto de personas naturales y jurídicas; sin embargo, por su sencillez, popularidad y a veces gratuidad, muchos de sus usuarios son personas naturales.

En la actualidad la mayoría de personas cuentan con un correo electrónico o una cuenta en redes sociales, es más, tener una incluso se ha vuelto imprescindible en la actualidad. Las personas que sin darse cuenta, hicieron "*click*" para aperturar una cuenta de correo electrónico, ya son usuarios de servicios de *cloud computing;* y sus datos están siendo tratados bajo términos y condiciones que ignoran totalmente. Este trabajo tiene como objeto estudiar más a detalle este tipo de relación B2C, para evidenciar la necesidad de desarrollar en Ecuador un sistema preventivo de protección de datos personales, que precautele derechos de consumidores ecuatorianos.

1.6.1.4 Análisis de modelos de servicio de *cloud computing* en el derecho a la protección de datos personales

Podemos evidenciar entonces con los modelos de servicio de *cloud computing* enunciados la dimensión del tema de estudio y su complejidad. El presente trabajo se centrará en el análisis específico del derecho a la protección de datos personales de los ecuatorianos usuarios de servicios de cómputo en la nube en relaciones B2C; para realizar dicho análisis, como caso ejemplificativo, se estudiarán las políticas de privacidad de Dropbox, empresa que oferta servicios SaaS en la Web.

Se ha elegido analizar un caso del nivel de servicio SaaS, porque este es el más popularizado en la actualidad entre los usuarios, y permite comprender de forma más amplia y didáctica la necesidad de precautelar preventivamente el derecho a la protección de datos personales que se reconoce a nivel constitucional en Ecuador.

Es menester mencionar que aunque el análisis práctico del presente estudio se centre en casos en que exista relación B2C en el modelo SaaS, las conclusiones a las que se llegará también serán aplicables para cualquiera de los niveles de prestación de servicios en el *cloud computing*, siempre que estos servicios sean proporcionados directamente por el proveedor de servicios de nube de cómputo al *e-consumer* (relación B2C).

Tanto para el IaaS, el PaaS y el SaaS son aplicables los mismos criterios técnicos de manejo, procesamiento y almacenamiento de información conforme al ciclo de vida de los datos en la nube. Así pues, el usuario al momento de contratar cualquier nivel de servicio de *cloud computing*, independientemente del tipo de prestación y el mercado al que se encuentren proyectados los servicios en la nube, deberá observar las cláusulas relativas al manejo de la información que estipule el proveedor y podrían violentar *a priori* su derecho a la protección de datos personales.

1.6.2 Modelos de implementación del *cloud computing*

También conocidos como "modelos de despliegue", hacen referencia a la forma en que el proveedor pone a disposición del público sus servicios de cómputo en la nube, (Acevedo, 2010), respecto a la localización y gestión de su infraestructura. (Joyanes, 2012b, p. 94). Los modelos de despliegue descritos anteriormente son independientes de estos y, por lo tanto, se pueden implementar indistintamente. Para NIST existen cuatro modelos de despliegue, sin embargo, la nube comunitaria no ha tenido mucha aceptación de los expertos en tecnología. (Joyanes, 2012a, p. 76). Es importante mencionar que las nubes híbrida y comunitaria constituyen simplemente combinaciones entre las nubes pública y privada.

1.6.2.1 Nube privada

En este modelo de implementación el *datacenter* es de propiedad exclusiva de la organización usuaria de los servicios de cómputo en la nube. La arquitectura puede o no ser administrada por dicha organización, pero ésta siempre decidirá quienes tienen acceso a la misma. Sus recursos informáticos pueden ser *"on-premise",* dentro de las instalaciones de la compañía, u *"off-premise"* fuera de dichas instalaciones. (Tellez, 2013, p. 8). En el caso de contar con recursos "*off-premise",* el *datacenter* siempre estará localizado dentro de un perímetro de seguridad (cortafuegos) de la compañía. (Joyanes, 2012a, p. 77)

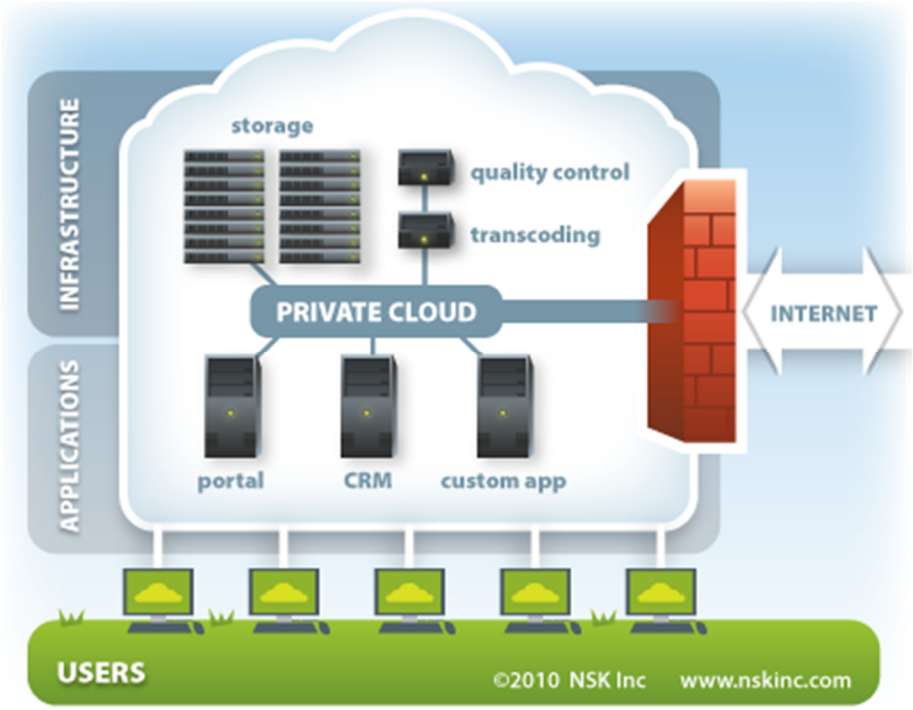

Figura 6. **Representación de la nube privada**

Tomado de "*Cloud Computing* 101: Public Vs Private Clouds", por Briggette, 2011

El tratamiento de datos en este tipo de nube no debería implicar tantas afectaciones al derecho a la protección de datos personales como en el caso de una nube publica, porque resultaría contraproducente que la compañía dueña de la información, violente sus datos propios o los de sus empleados. Sin embargo, en la nube privada también es factible que existan trasgresiones al derecho a la protección de datos personales, como en el caso de que el dueño de una compañía realize tratamiento de datos de sus empleados (quienes terminan siendo usuarios del servicio).

1.6.2.2 Nube pública

Con este tipo de modelo de implementación de *cloud computing* el proveedor de estos servicios, pone sus recursos a disposición del público en general. (Joyanes, 2012a, p. 77). Para Tellez la nube pública "significa que la

infraestructura de la nube es disponible al público en general o a un gran sector industrial y es detentada por una organización que provee servicios en la nube." (2013, p. 8)

En los casos de contrataciones B2C de servicios de *cloud computing* realizadas dentro de la nube pública, se pueden originar ejemplos claros de trasgresión al derecho a la protección de datos personales de los usuarios que han contratado con un proveedor de servicios de cómputo en la nube.

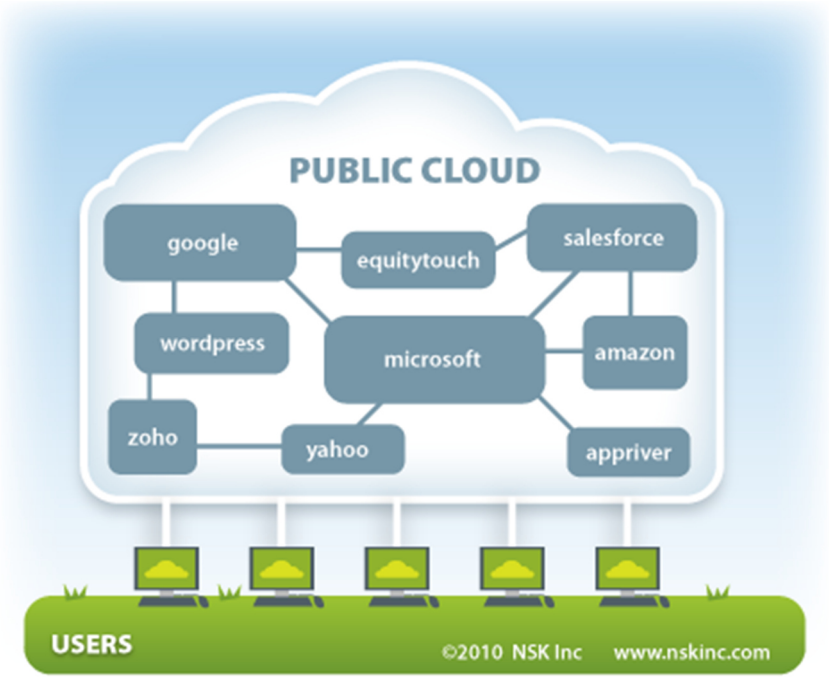

Figura 7. **Representación de la nube pública**
Tomado de "*Cloud Computing* 101: Public Vs Private Clouds", por Briggette, 2011.

1.6.2.3 Nube híbrida

Cuando se habla de nube híbrida se hace referencia a aquellas nubes privadas que pueden tener acceso a nubes públicas, esto en caso de presentarse períodos de máxima demanda de recursos para las compañías, períodos en los cuales su arquitectura propia resulta insuficiente para satisfacer su demanda.

(Joyanes, 2012a, p. 77). Para Tellez este tipo de nube implica: "[…] la infraestructura de la nube está compuesta de una o más nubes (privada, comunitaria o pública), que se mantienen como entidades individuales, pero que están unidas por tecnología estándar o propietaria que permite la portabilidad de datos y aplicaciones." (2013, p. 8)

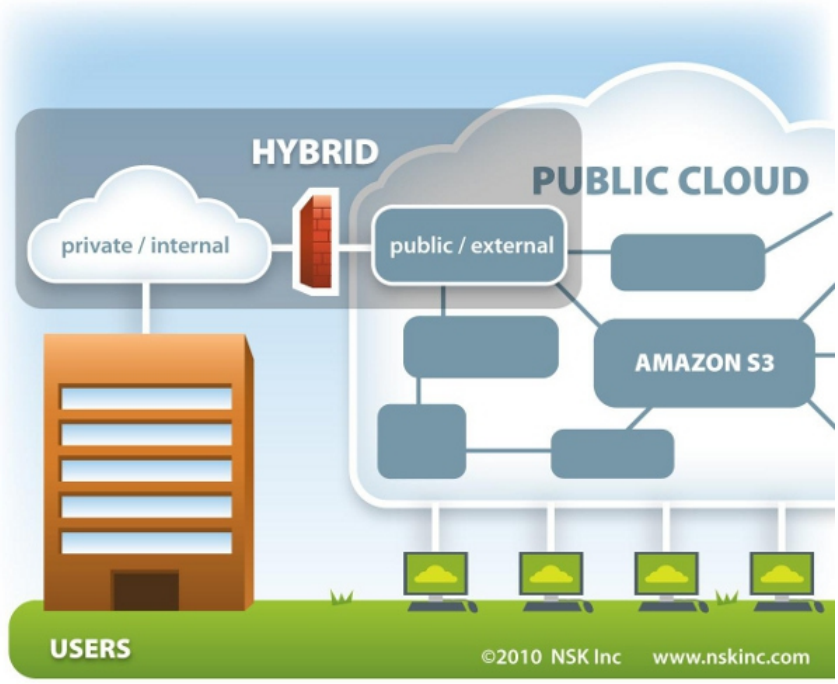

Figura 8. **Representación de la nube híbrida**
Tomado de "Hybrid Clouds-The Best of Both Worlds", por IT Consultants' Insight On Business Technology, s.f.

1.6.2.4 Nube comunitaria

Este tipo de nube se crea con el objeto específico de servir a una función o propósito común. La misma puede ser administrada por terceros o por las organizaciones que las constituyen. (Joyanes, 2012b, p. 95). Tellez hace referencia a la nube comunitaria diciendo lo siguiente:

> "Significa que la infraestructura de la nube es compartida por diversas organizaciones usuarias, que usualmente dan servicio a una comunidad en

> particular, que comparten requerimientos o propósitos comunes (ya sea de misión, requerimientos de seguridad, políticas, consideraciones de cumplimiento normativo, etcétera). La nube puede ser administrada por dichas organizaciones o por un tercero y puede existir *on-premise* u *off-premise*." (Tellez, 2013, p. 8)

Conforme desprende de los criterios antes expuestos, que rigen los modelos de implementación del *cloud computing*, en los casos de contrataciones realizadas en nubes híbridas y comunitarias se podrían producir quebrantamientos al derecho de protección de datos de las personas usuarias de los servicios, en la medida en que estos sean parte de nubes públicas aumentarán las probabilidades de violación al derecho a la protección de datos. Así pues, es menester señalar que independientemente del modelo de despliegue de *cloud computing* que se utilice, el derecho a la protección de datos personales siempre deberá ser resguardado, puesto que el peligro continuará latente.

1.7 Ciclo de vida y tratamiento de los datos en el *cloud computing*

Las formas en que se da tratamiento a los datos relativos a los usuarios de servicios de *cloud computing*, varían conforme a las políticas y sistemas que maneje cada proveedor. Debido a la naturaleza económica de este modelo de prestación de servicios, es improbable que los proveedores de servicios de *cloud computing* se rijan a un proceso uniforme de tratamiento de datos, por lo que resulta fuera de contexto, e incluso imposible tratar de definir uno de forma generalizada.

Sin embargo, para fines de la presente investigación y para comprender la forma en que los datos se movilizan en la nube, se ha considerado necesario atender a las diversas pautas brindadas por el Instituto Nacional de Tecnologías de la Comunicación (INTECO), entidad española creada con el fin de desarrollar la ciberseguridad y dar confianza digital de los ciudadanos. Con estas pautas se podrá concebir en contexto el ciclo de vida de los datos dentro de la nube de cómputo:

> "El ciclo de vida que siguen los datos que son procesados en la nube es el siguiente:
>
> - Los datos son preparados para poder adaptarse a la nube adaptando su formato o creando un fichero que contenga toda la información necesaria.
> - Los datos "viajan" a la nube a través de una conexión a Internet, mediante un correo electrónico, una aplicación específica para importarlos o la transferencia a la nube de la copia de seguridad obtenida de un servidor en la organización.
> - Los datos son procesados en la nube, desde su almacenamiento hasta el cálculo de complejas operaciones matemáticas. Es importante mencionar que los datos pueden almacenarse en copias de seguridad en la nube para facilitar futuros accesos.
> - Los datos finales "viajan" de vuelta al usuario. Una vez terminado el procesamiento, el resultado debe volver al usuario con el valor añadido de la información generada en la nube" (INTECO, 2011, pp. 40-41)

Para que los datos inicialmente puedan recogerse en un fichero, deberá adaptarse su formato, así los datos pasarán a ser almacenados en la nube. Una vez en la nube, la información será procesada y tratada por el proveedor de servicios de cómputo en la nube. El tratamiento de datos que realizan los proveedores se basa en cálculos econométricos, destinados muchas veces a desarrollar perfiles generales de comportamiento del público en general. Finalmente, siempre que el usuario precise acceder a sus datos almacenados en la nube, estos viajarán de vuelta al mismo.

1.7.1 Fases del ciclo de vida de los datos en el *cloud computing*

Expertos en el tema de *cloud computing* han intentado desarrollar más a fondo el tema de seguridad de datos en la nube a través del "ciclo de vida de seguridad de los datos." (véase Securosis, 2011). Existen varias formas de definir este ciclo de vida, pero éste en particular hace énfasis en las funciones que podrá realizar el proveedor de servicios de *cloud computing,* y por ende, se puede definir a partir de sus fases, de mejor manera las responsabilidades y obligaciones que establece el derecho a la protección de datos personales para el responsable de tratamiento de datos.

Aunque la finalidad de este trabajo no es la de realizar un estudio detallado de la seguridad de los datos en el *cloud computing* Cloud Security Alliance desarrolla algunas recomendaciones para la seguridad de los datos que recomendamos revisar. (Véase CSA, 2009, pp. 26-27). Para comprender la forma en que se tratan los datos personales en este modelo de prestación de servicios, es preciso atender a las fases del ciclo de vida de los datos en la nube. Para este caso particular se ha considerado pertinente considerar las siguientes fases basadas en los criterios de Securosis. (2011)

- **Fase 1: Creación.-** También se la puede llamar creación/actualización, pues a través de la misma se puede generar un nuevo contenido digital, o también un contenido ya existente puede ser actualizado o modificado.

- **Fase 2: Almacenamiento.-** Esta fase generalmente ocurre prácticamente de forma simultánea a la fase de creación, y en la misma los datos son ubicados en un repositorio de almacenamiento.

- **Fase 3: Uso.-** En esta fase los datos se visualizan, procesan, o utilizan conforme al tipo de actividad del proveedor de servicios de *cloud computing*. Es importante tener en cuenta que en esta fase no existe modificación alguna de los datos, sin embargo, con la información recabada, en esta fase los proveedores de servicios de cómputo en la nube elaboran perfiles de sus usuarios.

- **Fase 4: Compartición.-** La información es compartida entre varios actores, como usuarios, clientes, y colaboradores.

- **Fase 5: Archivado.-** Para el inicio de esta fase los datos ya habrán dejado de ser usados activamente, y se los archiva por largo plazo.

- **Fase 6: Destrucción.-** Esta fase final supone la destrucción de los datos con medios físicos o digitales.

Es importante tener en cuenta que las fases expuestas no son una regla generalizada para todos los casos de tratamiento de datos en el *cloud computing*, es decir, existirán casos en los que, por ejemplo, los datos sean destruidos antes de haber pasado por las fases 4 y 5. A continuación una figura que detalla las fases expuestas para mejor comprensión del lector.

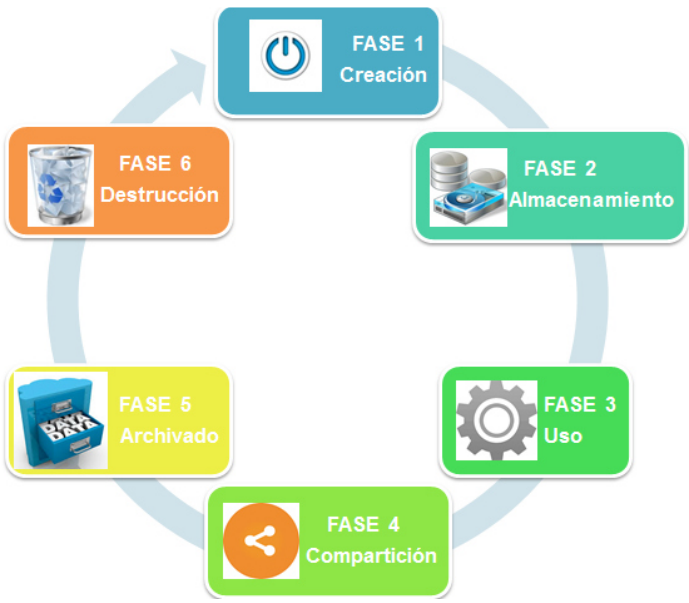

Figura 9. **Ciclo de vida de los datos en el *cloud computing***
Adaptado de "Data Security Lifecycle 2.0", por Securosis, 2011.

También se considera necesario entender las distintas funciones que los actores en el sistema de *cloud computing* podrán realizar conforme a cada fase explicada. Para el efecto hay tres tipos de operaciones que los actores pueden realizar con los datos (Securosis, 2011), es importante considerar que estas operaciones no forman parte de las fases del ciclo de vida de los datos ya detalladas:

- **Acceso:** Consiste en ver o acceder a la información, lo que incluye copiarla, transferirla o intercambiarla.

- **Procesamiento:** Constituye la realización de operaciones en los datos tales como: actualización, organización, y utilización en operaciones de

negocios para elaborar perfiles personales y de preferencias de sus usuarios, para así mejorar el marketing empresarial o vender sus bases de datos a distintas empresas.

- **Almacenamiento:** Consiste en almacenar la información, por ejemplo en archivos o una base de datos.

Conforme a las fases del ciclo de vida de los datos detalladas previamente, la siguiente figura detalla qué funciones pueden ser desempeñadas por los actores del *cloud computing* en cada una de estas:

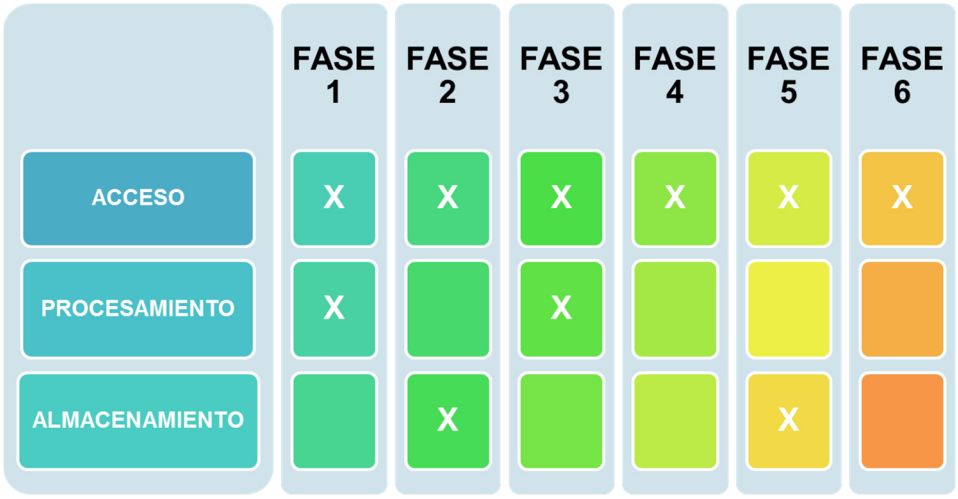

Figura 10. **Funciones que los actores pueden desempeñar de acuerdo al ciclo de vida de los datos en el *cloud computing***

Adaptado de “Data Security Lifecycle 2.0”, por Securosis, 2011

Entonces constatamos que en cualquiera de las seis fases será factible para los actores del cómputo en la nube acceder a la información. Sin embargo, estos datos solo podrán ser procesados en las fases 1 y 3; y almacenados en las fases 2 y 5.

Además para fines de la presente investigación es importante poner atención a las fases que brindan funciones de procesamiento a los proveedores de servicios

de *cloud computing,* pues será en estas fases cuando se elaboren perfiles de sus usuarios. A demás es elemental destacar que en el *cloud computing* si existe tratamiento de datos personales de los usuarios y que se elaboran perfiles de estos, por lo que el derecho a la protección de datos de los titulares de la información debe ser precautelado por el Estado.

1.7.2 Circulación de datos personales entre distintos actores del *cloud computing*

Para entender cómo el ciclo de vida de los datos del *cloud computing* pasa a tener relevancia para el derecho a la protección de datos personales, hay que concebir que, con independencia de las fases que existan, los datos siempre circularán por manos de varios actores (titular de los datos, responsable de tratamiento, encargado de tratamiento, etc.). Es así que en concordancia con las pautas ya brindadas, para hacer más específicos, la siguiente figura proyecta una idea general del flujo de datos en la nube de cómputo:

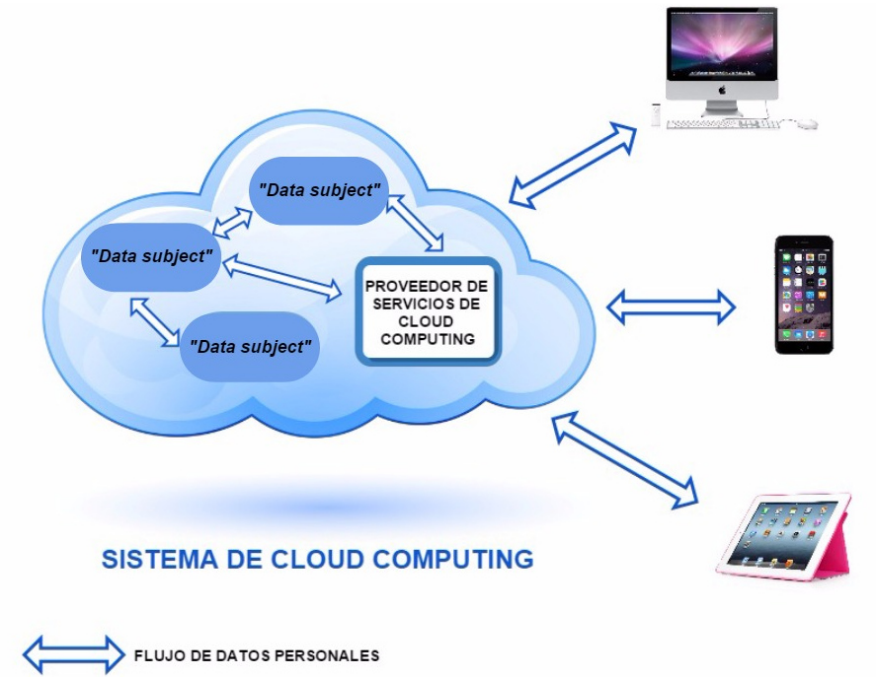

Figura 11. **Flujo de datos personales en el *cloud computing***

Adaptado de "*Cloud computing and its implications on data protection*", por CRID, 2010, p. 10

Conforme desprende de la figura, las pautas brindadas por INTECO, y los criterios del ciclo de vida de seguridad de los datos, se evidencia que, no es posible delimitar un único proceso de tratamiento de datos al que se rijan los proveedores de servicios de *cloud computing,* pues incluso para ellos resulta muy complejo determinar a ciencia cierta en qué lugar específico están almacenados los datos de cada uno de sus usuarios, esto compagina con las características de "reservas de recursos en común" y "rápida elasticidad", expuestas en el capítulo primero del presente trabajo.

Sin embargo, aunque no se puede definir a ciencia cierta qué actores tendrán acceso a los datos y la forma en que estos serán tratados, si se pueden puntualizar fases que ayudarán a comprender las funciones que podrán realizar los proveedores de servicios de *cloud computing* en general. Es decir, aunque los proveedores no realicen efectivamente dichas funciones, éstos al tratar la información de sus usuarios y elaborar perfiles, conforme a las distintas fases de sus actividades, deberán implementar preventivamente las debidas seguridades observando y aplicando los principios del derecho a la protección de datos personales.

1.8 Ventajas y desventajas para los actores del *cloud computing*

El cómputo en la nube es un tema muy amplio que da cabida a investigaciones en varios aspectos del derecho, sin embargo, el tema de esta investigación está encaminado a profundizar y examinar exclusivamente los aspectos del *cloud computing* que pueden coartar el derecho de protección de datos personales de usuarios ecuatorianos, debido al tratamiento de datos que realicen sus proveedores.

El mayor aporte doctrinario acerca de *cloud computing* hace referencia a los beneficios económicos que este modelo de prestación de servicios representa para las empresas. Sin embargo, los peligros que podrían afectar a los usuarios de dichos servicios en muchos casos llegan a ser muy graves, esto debido a la

magnitud de personas que contratan servicios de *cloud computing* sin haberse percatado del hecho.

1.8.1 Ventajas y desventajas para los proveedores de servicios de *cloud computing*

Las ventajas para los proveedores de servicios son innumerables, pero se pueden mencionar algunas a continuación. (Melaños, 2013, pp. 23-24):

- Debido a la información que obtienen de sus usuarios, pueden optimizar continuamente sus servicios generando eficiencias que les permitan desarrollarse.

- La afluencia tecnológica apunta al crecimiento de demanda de este tipo de servicios a futuro, lo que beneficia a los proveedores actuales.

- Por las características del *cloud computing*, es factible que compartan plataformas de almacenamiento con otros proveedores, lo que acrecentaría su negocio, disminuyendo costos.

- Debido a la fórmula de "pago por consumo", siempre tendrán la seguridad de obtener el dinero a tiempo, lo que disminuye el riesgo del negocio y favorece inversiones a futuro.

- Por la naturaleza del servicio, es complejo que sus usuarios migren a otros proveedores, por lo que existe estabilidad de clientela.

Las desventajas que podrían presentarse para los proveedores son las siguientes (Melaños, 2013, pp. 24-25):

- En caso de que sus sistemas no funcionen adecuadamente, esto puede implicar una perdida inmensa para su empresa, incluso podría llevarlos a la quiebra.

- Están expuestos a casos de fuerza mayor, como un apagón de luz, que podría representar pérdidas de dinero, información e incluso de clientela.

- En caso de que no utilicen sistemas de seguridad amplios, podrían ingresar hackers a su sistema. Este hecho podría acarrear el inicio de acciones civiles o penales en su contra, por negligencia en el cuidado de los datos de sus clientes.

1.8.2 Ventajas y desventajas para los usuarios de servicios de *cloud computing*

Algunas de las ventajas que se generan para los usuarios de servicios de cómputo en la nube se enuncian a continuación (Melaños, 2013, pp. 23-24):

- Al utilizar servicios de *cloud computing*, los usuarios no van a necesitar preocuparse por instalar *software* o dar mantenimiento a las máquinas que utilicen (*hardware*), lo que resulta sumamente conveniente pues implica ahorro de tiempo y de coste.

- Debido a que los proveedores de computo en la nube deben mantener actualizadas constantemente las aplicaciones o programas que ofertan, el usuario no debe preocuparse por realizar las actualizaciones, lo que implica un inmenso ahorro de tiempo y, por consiguiente, de dinero.

- Al utilizar servicios en la nube, generalmente se ahorrará los costos que le implicarían al usuario adquirir toda la plataforma para el funcionamiento y almacenamiento de sus programas.

- Al utilizar servicios de *cloud computing*, los usuarios son parte de la convergencia tecnológica, que hoy en día es tan buscada, pues implica una interconexión de tecnologías.

- A través del *cloud computing* tienen acceso a su información desde cualquier dispositivo, independientemente del lugar en que se encuentren, solo necesitarán conexión a Internet.

Entre algunas de las desventajas que se presentarían para los usuarios se pueden enunciar las siguientes (Melaños, 2013, pp. 24-25):

- Al aceptar cláusulas de contratos de adhesión abusivas, se podrían violentar sus derechos como consumidor.

- Debido a su falta de conocimiento del sistema que se maneja en el *cloud computing*, estarían expuestos a que se realice un manejo abusivo de sus datos.

- En caso de que sus derechos sean quebrantados, podrían tener una gran incertidumbre respecto a las acciones que les amparen, hallándose en total indefensión.

- Se podrían crear bases de datos de sus preferencias, manipulando erróneamente la información que los perfila, lo que causaría graves daños a la persona.

1.9 Conclusiones previas

La presente investigación tiene la finalidad de definir y comprender en general lo que es y lo que representa el *cloud computing* para el desarrollo de la tecnología a nivel mundial, por esto ha sido preciso brindar referencias de sus antecedentes, las características que distinguen a este modelo de otros, los actores que participan en la prestación de estos servicios, los tipos de servicios a los que se puede acceder en la nube, los tipos de nube existentes y las ventajas y desventajas que pueden generarse para los proveedores y usuarios de los servicios de *cloud computing.*

Se ha evidenciado en el presente capítulo la importancia del cómputo en la nube para el desarrollo de las TIC, y también la gran difusión que han ido adquiriendo los servicios de *cloud computing* en los últimos años. En definitiva, estamos en la nube sin siquiera estar enterados del hecho, lo que es positivo para el avance social y tecnológico del Estado ecuatoriano. Aunque también es preciso recordar que los ecuatorianos tenemos derechos y estos deben ser tutelados.

El presente estudio busca identificar las implicancias que el *cloud computing* trae consigo para el debido amparo preventivo que el Estado debe dar al derecho a la protección de datos personales reconocido por vía constitucional a los ecuatorianos. Es así que una vez esclarecido lo que es el *cloud computing* y sus elementos distintivos, el capítulo segundo planteará un marco teórico del derecho a la protección de datos personales y su aplicabilidad preventiva en el caso ecuatoriano.

Posteriormente, en el capítulo tercero, se contrastará el contenido de los capítulos primero y segundo para proponer la implementación de normativa preventiva de protección de datos personales que acoja en la legislación ecuatoriana principios estándares de este derecho, que regulen los diversos riesgos que se pueden generar a partir de relaciones B2C entre los usuarios ecuatorianos y proveedores de servicios de *cloud computing*.

A continuación se desarrollará un marco teórico del derecho a la protección de datos personales que permita, en primer lugar, comprender este derecho; para pasar a analizar si en el Ecuador dicho derecho está siendo tutelado o no, y de no ser así, exponer criterios estándar que brinden un marco teórico de protección de datos personales óptimo para la legislación ecuatoriana.

2 DERECHO DE PROTECCIÓN DE DATOS PERSONALES

2.1 Panorama internacional del derecho a la protección de datos personales

En el siglo XIX, el Juez Cooley reflexiona formalmente acerca de "*the right to be let alone"*, en 1880; brindando el patrón para que, unos años más tarde, Warren y Brandeis desarrollen el concepto de *"privacy"* con su famoso artículo titulado "*The right to privacy"* publicado en el año 1890. (Martínez, 2004, pp. 66-71). Este artículo es el inicio de un movimiento doctrinario mundial alrededor de los conceptos que trae consigo.

El estudio de Warren y Brandeis plantea un amplio derecho personal *erga omnes* que va de la mano con la tecnología, descartando de su naturaleza a la propiedad privada. De esta forma nació el término *"privacy",* equivalente a "intimidad" o su traducción literal "privacidad" en el idioma español. Este derecho, en sus inicios, se concibió de forma excluyente, es decir, estaba encaminado defender la esfera personal y privada del ser humano frente al mundo. (García, 2007, p. 750). Sin embargo, esto cambiaría con el paso del tiempo.

Para Clímaco (2012, pp. 18-20) la *"privacy"* conlleva una dimensión psicológica destinada a proteger la integridad del ser humano, que de ser afectada, causaría detrimento a su autoestima. *"The right to privacy"* (derecho a la privacidad) nace ligado a otros como el de personalidad, dignidad o libertad. En definitiva el autor concluye refiriéndose de la siguiente forma de la *privacy*:

> "Como veremos a continuación en este recorrido histórico, sin perjuicio de las influencias de los otros pensamientos teóricos, esta concepción de la privacidad en el contexto anglosajón, vinculada primero a la idea dignidad humana para luego relacionarse con la idea de libertad, es la que mayor secuela ha tenido en el lenguaje universal de la protección de los datos personales, en tanto que pasa de ser un derecho de exclusión de los demás del ámbito privado a ser el espacio de soberanía de un individuo considerado en su dimensión integral, de acceder y controlar sus propios datos." (2012, pp. 25-26)

Acorde a la reflexión de Climaco surge la consideración de que la evolución tecnológica ha traído consigo una ampliación del derecho a la privacidad, lo que en el siglo XIX era un derecho garantista de defensa de la esfera privada de las personas frente a terceros, se ha extendido al derecho activo de los individuos para controlar la información que les pertenece. La concepción inicial de *"privacy"*, junto con la tecnología, se ha vuelto dinámica y abierta, (García, 2007, p. 751), en contraposición a su noción inicial, lo que ha representado avances innumerables en la materia.

Por otro lado, la intimidad se consideraba un privilegio de la burguesía en la revolución industrial, (Naranjo, 2007, p. 70), y por ello, su nacimiento supuso el reconocimiento formal de un derecho que previamente ya lo tenían ciertas clases sociales privilegiadas.

En el devenir del tiempo, se promueve a nivel internacional el reconocimiento del derecho a la intimidad, a través de varios instrumentos de amparo. El primer documento de armonización del derecho a la intimidad es la Declaración Universal de Derechos Humanos, acogido por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III) con fecha 10 de diciembre de 1948, misma que en su artículo 12 reconoce el derecho a la intimidad, ligándolo a la vida privada personal y familiar, el domicilio, la correspondencia, la honra y la reputación.

Posteriormente, bajo los mismos criterios del artículo 12 de la Declaración Universal de Derechos Humanos; el 16 de diciembre de 1966, la Asamblea General de las Naciones Unidas mediante la Resolución 2200 A (XXI) adopta el Pacto Internacional de Derechos Civiles y Políticos, instrumento que reconoce en su artículo 17 el derecho a la intimidad, vida privada personal y en familia; y, el derecho a la honra y reputación.

Consecutivamente, el 22 de noviembre del año 1969, se suscribe la Convención Americana sobre Derechos Humanos, también conocida como Pacto de San

José. Este tratado, en su artículo 11 reconoce el derecho a la intimidad, la protección a la honra y dignidad; y, el derecho a la vida privada personal y familiar.

En 1974 el Congreso de Estados Unidos aprueba la "*Privacy act*", cuerpo normativo destinado a brindar protección únicamente para aquellos datos tratados por entidades del sector público.

A nivel europeo, debido a los instrumentos internacionales, y en atención a la realidad social, política y económica de dicho continente. En 1968 la Asamblea del Consejo de Europa emite la Resolución 509 sobre "los derechos humanos y los nuevos logros científicos y técnicos". Cuerpo normativo que brinda, por vez primera, una pauta prematura para salto sustancial existente entre el derecho a la intimidad, y lo que hoy conocemos como derecho a la protección de datos personales.

Aunque con la resolución 509 se vislumbra un posible derecho a la protección de datos personales, frente al desarrollo de las tecnologías, surge en el año 1983 en Alemania, "la sentencia del censo", sentencia en que los legisladores germanos dan vida al derecho denominado "autodeterminación informativa". El derecho de "autodeterminación informativa" nace como evolución del derecho a la intimidad frente al desarrollo de las nuevas tecnologías, supliendo todos los aspectos que el derecho a intimidad, por sí mismo no podía abarcar. Solamente a partir de esta sentencia se puede considerar que existe, lo hoy en día conocemos como el derecho a la protección de datos personales.

Para consagrar los criterios emitidos por el Tribunal Federal Alemán, el 24 de octubre de 1995 el Parlamento Europeo y Consejo de Europa expiden la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta directiva constituye el modelo ejemplificativo a nivel mundial del derecho a la protección de datos personales, y el primer instrumento de

armonización normativa que ampara ampliamente el derecho a la protección de datos personales, (Puente, 2010, pp. 911-913); los conceptos que trae consigo este cuerpo normativo tienen implicancias a nivel mundial, y por lo mismo, serán desarrollados posteriormente.

La historia tiene un papel preponderante en la evolución del derecho a la protección de datos personales, los sucesos y conceptos antecedentes a este derecho lo consolidan e independizan frente a otros. Este proceso histórico muy pronto tendrá efectos directos Ecuador, país que ha consagrado constitucionalmente el derecho a la protección de datos personales, que para alcanzar su tutela efectiva, deberá implementar normativa específica referida a este derecho.

2.1.1 Derechos ligados al derecho a la protección de datos personales: una reseña al *"privacy"*, derecho a la intimidad y autodeterminación informativa

Como se evidencia en párrafos anteriores, el nacimiento del derecho a la protección de datos personales responde a un progresivo reconocimiento mundial de derechos estrechamente ligados al mismo como "*the right to privacy*", intimidad o autodeterminación informativa. Es importante hacer una breve diferenciación conceptual entre estos derechos, para con posteridad, inferir la independencia del derecho a la protección de datos.

Con respecto a los derechos a la *privacidad* e *intimidad,* no existe una posición consolidada a nivel doctrinario para definirlos; ciertos autores como Sánchez Bravo los tratan indistintamente, y otros autores como Davara Rodríguez, aunque no diferencian sus conceptualizaciones, si distinguen las esferas de protección que resguardan. Es importante manifestar que, posiblemente las posiciones de todos estos autores sean acertadas, pero la forma de delimitar la esfera de protección del derecho sea la errónea.

Algunos autores al referirse a la *"privacy"* estadounidense, la equiparan con el derecho a la intimidad español. Efectivamente, a nuestro criterio, *"the right to privacy"* protege las mismas esferas que el derecho a la intimidad, y por lo tanto, son equivalentes. Este criterio lo sostienen varios autores, y otros, realizan diferenciaciones entre el derecho a la privacidad y el derecho a la intimidad, que a la larga, termina siendo una distorsión de sus orígenes y naturaleza jurídica.

El derecho a la intimidad, en sus inicios se limitaba a resguardar la esfera de vida privada de las personas, es decir, era excluyente y negativo (se protege con la inacción de las personas, al no entrometerse en la vida privada del resto). Sin embargo, con el pasar de los años, este derecho expande su connotación; y se desarrolla a la par de la sociedad. Así pues, la intimidad también pasa a proteger las decisiones que las personas toman respecto a la información que identifica su vida personal.

Lo antes expuesto se clarifica con la reflexión de Conde Ortiz, quien considera que, aunque prevalezcan ideas de aislamiento para definir a la intimidad, esta trasciende; es un derecho inherente a toda persona, que no solo lo libera de injerencias a su vida privada, sino que también, lo capacita para realizar acciones encaminadas a controlar la información que le concierne, derecho ligado a la libertad. La intimidad concebida de forma abierta, para este autor, se extiende a la amplitud del *"privacy",* y por lo tanto, es insostenible afirmar que el derecho a la privacidad difiere del derecho a la intimidad en idioma castellano.

Como se manifiesta en líneas anteriores, nos inclinamos por considerar tanto a al derecho a la intimidad, como al "right to privacy" o su tradución literal al español "derecho a la privacidad" como equivalentes, esta línea nos permitimos citar una breve reflexión que realiza Sánchez al respecto:

> "Antes de adelantarnos en otras consideraciones sí quisiéramos expresar nuestro desagrado por la reiterada utilización en la legislación y doctrina españolas del neologismo *privacidad*; término sin arraigo en nuestro lenguaje, y que no es más una traducción literal y simplista de la noción inglesa *privacy.* Y aquí radica la gravedad de la confusión, por cuanto no se trata de una simple asunción lingüística

> de un término extraño a nuestro diccionario; sino de la equiparación de conceptualizaciones de intimidad que aparecen claramente diferenciadas en los sistemas de Derecho continental y del Common Law. […] El término privacy puede considerarse que comprende lo que para nosotros es intimidad y vida privada, círculos concéntricos de distinta amplitud; si vida privada comprende, obviamente, lo que es íntimo no todo lo que es íntimo puede extenderse a vida privada." (1998, pp. 45-46)

De lo antes manifestado, el autor es muy claro al señalar que a su criterio no existe diferencia ente la intimidad y privacidad en el idioma español, y que dicha diferenciación realizada por otros autores resulta errónea y a la vez acarrea confusiones conceptuales.

Sin embargo, la interminable discusión doctrinaria generada alrededor del derecho a la intimidad y privacidad deja de tener relevancia en materia de protección de datos cuando nace el derecho a la "autodeterminación informativa", derecho que viene a suplir toda discrepancia doctrinaria generada previamente. Con su aparición, la concepción de protección de datos personales dio un giro de ciento ochenta grados, cimentando así, los valores que este derecho tutela en la actualidad.

La autodeterminación informativa nace formalmente a partir de jurisprudencia constitucional alemana, específicamente con la sentencia dictada en el año de 1983 referida al recurso plateado contra la Ley del Censo aprobada en 1982. En la sentencia, el Tribunal Constitucional Federal de Alemania argumentó sobre la importancia del derecho a la personalidad; y, las amenazas a este derecho que trae consigo el creciente desarrollo tecnológico. Respecto al razonamiento de dicha sentencia se puede destacar lo siguiente:

> "Dentro de las condiciones para el moderno procesamiento de datos se encuentra el derecho general de la personalidad […] y que protege a los individuos frente a la recolección, archivo, empleo y difusión ilimitada de sus datos personales. El derecho fundamental garantiza en esta medida la capacidad de los individuos, para determinar, en principio, la divulgación y empleo de sus datos personales.
>
> Los límites a ese derecho a la "autodeterminación informativa" se admiten sólo con base en la prevalencia del interés general, requieren de un fundamento legal y constitucional […]" (Schwabe, 2009, p. 94)

El Tribunal bosqueja un derecho a la "autodeterminación informativa" que efectiviza un derecho a la personalidad coartado por el avance tecnológico y procesamiento de datos; este derecho se podría limitar frente al interés general de las personas. Haciendo referencia al derecho general de la personalidad y el reconocimiento de la autodeterminación informativa, Martínez señala:

> "El derecho general de la personalidad comporta una atribución al individuo de la capacidad de decidir, en el ejercicio de su autodeterminación, qué extremos desea revelar de su propia vida […].
>
> Esta libertad de decisión, de control, supone además que el individuo tenga la posibilidad de acceder a sus datos personales, que pueda, no sólo tener conocimiento de que los otros procesan informaciones relativas a su persona, sino también someter el uso de éstas a un control, ya que, de lo contrario, se limitará su libertad de decidir por autodeterminación […]" (Martínez, 2004, p. 240)

El Tribunal elabora el concepto de autodeterminación informativa basado en tres preceptos: En primer lugar, abandona la antigua teoría de las esferas, por la que se distinguían los niveles de protección de intimidad o privacidad conforme a la esfera de reserva de la persona. En segundo lugar, se realiza un análisis profundo de la personalidad; y, finalmente, extrae del tronco común del derecho a la personalidad, un derecho derivado, destinado a preservar la identidad del individuo frente al tratamiento de sus datos personales. (Serrano, 2003, p. 64)

El derecho a la autodeterminación informativa surge del derecho a la personalidad, es una rama del tronco de esta. Dicho derecho nace en respuesta al desarrollo tecnológico y la consecuente insuficiencia del derecho a la intimidad. Con la autodeterminación informativa se cumple el "Pacto Social Informático" al que se refiere Pérez Luño por el que el ser humano consiente dar sus datos personales, y el Estado se compromete a brindarle las debidas garantías en su utilización, lo que genera el equilibrio que debe existir entre el flujo de información y la garantía de privacidad de los hombres. (1996, p. 67). Las problemáticas que trajo consigo la tecnología inspiraron nuevos retos jurídicos, que desencadenaron en la introducción de un derecho derivado y específico, como lo es la autodeterminación informativa.

Lo que busca controlar la autodeterminación informativa es:

> "[…] la utilización de informaciones personales, es decir, la atención se centra en la elaboración de los datos, no en su calificativo de íntimo, reservado, secreto o privado, por lo que no es significativa su mayor o menos proximidad al núcleo íntimo de la persona […]" (Serrano, 2003, pp. 67-68)

Por las razones citadas, y porque el derecho de la autodeterminación informativa tiene su fundamento en la personalidad del individuo; es decir, es intrínseco a este, y garantiza la protección del dato, considerándolo parte esencial de la persona en sí misma. Consecuentemente, es irrelevante la esfera de confidencialidad que a la que pertenece el dato, puesto que, lo que se debe salvaguardar es el contexto de su uso. (Serrano, 2003, p. 68). Por lo tanto, la teoría de las esferas de privacidad resulta insustancial para el presente análisis.

Es claro que la autodeterminación informativa se configura como una ampliación del derecho a la intimidad, y busca proteger un ámbito específico de la personalidad del individuo -sus datos expuestos frente al desarrollo de las nuevas tecnologías- para asegurar a este su plena libertad, decisión y capacidad de actuación frente a posibles abusos generados durante el manejo de su información. (Serrano, 2003, p. 68). Este derecho siempre estará ligado a la protección del individuo y por ende de su información, pero no será lo suficientemente desarrollado para contemplar todos los aspectos que trae consigo el derecho a la protección de datos personales.

Con la creación de cuerpos normativos como la Ley Orgánica de Protección de Datos de Carácter Personal española de 1999, o la misma Directiva 95/46/CE del Parlamento Europeo y del Consejo, trae consigo ya no solo el reconocimiento de la autodeterminación informativa del individuo, sino que configura un nuevo derecho denominado "derecho a la protección de datos personales". (Serrano, 2003, p. 195). El derecho a la protección de datos personales es vasto y se estructura de forma particular, no solo reconoce la autodeterminación informativa, sino que también despliega una serie de principios y derechos que

amparan al individuo durante el tratamiento de sus datos personales. El derecho al que nos referimos ya no solo trae consigo garantías para el titular de los datos, sino que impone obligaciones al responsable del fichero, salvaguardando así el buen manejo de datos del individuo, incluso sin que este se haya percatado de tal protección.

Con lo expuesto en líneas anteriores, inicialmente aparecen a nivel mundial, derechos como el de intimidad o *"the right to privacy"*, alrededor de estos conceptos se generó una discusión doctrinaria muy reñida, que terminó por equipararlos. Por lo tanto, debido a que su tutela resultaba insuficiente para proteger a las personas frente al desarrollo de las tecnologías, estos derechos evolucionan, dando nacimiento a uno nuevo denominado "autodeterminación informativa", que da pautas para el posterior reconocimiento de un derecho mucho más desarrollado y complejo, denominado "protección de datos personales".

2.1.2 La protección de datos personales como un derecho independiente y complejo

Como se concluyó previamente, las discusiones generadas alrededor de derechos como el de intimidad o el de autodeterminación informativa anteceden e inspiran el desarrollo y reconocimiento de un nuevo derecho independiente y complejo denominado "protección de datos personales"; a continuación, se desarrollan los razonamientos que nos llevan a deducir su naturaleza compleja, que lo distingue frente a otros derechos, haciéndolo un derecho independiente de otros.

2.1.2.1 Configuración compleja del derecho a la protección de datos personales

Para entender la configuración compleja del derecho a la protección de datos personales habrá que asemejar su naturaleza jurídica a la del derecho a la tutela

judicial efectiva. Como bien expresa Aguirre, a un derecho complejo como la tutela judicial efectiva, se lo debe definir a partir de sus notas configuradoras, solo así se puede comprender sus alcances. (Véase Aguirre, 2010).

El derecho a la protección de datos personales es un derecho con una configuración compleja, y al hacer esta aseveración nos referimos a que el mismo no tiene una manifestación autónoma como la generalidad de derechos. (Aguirre, 2010, p. 7). Como explica Naranjo este derecho no tiene un núcleo unívoco, sino que lo conforman varios principios, derechos e incluso garantías (*hábeas data*). Su desarrollo es constante en la medida en que la sociedad evoluciona. (Naranjo, L., entrevista personal, 31 de julio de 2015)

El derecho a la protección de datos personales al materializarse en varios derechos y principios, para entender el contenido esencial de este derecho hay que comprender que el mismo no es inmutable, sino que se lo determina de forma casuística (teoría relativa del contenido esencial de los derechos). Al explicar el contenido del derecho a la protección de datos personales a partir de la teoría relativa del contenido esencial de los derechos, se descarta la teoría absoluta del contenido esencial de los derechos, y por lo tanto ya no tiene relevancia la idea de que este derecho tenga un solo núcleo concéntrico que constituya su única esfera esencial. (Aguirre, 2010, p. 9)

El derecho a la protección de datos personales por ser un derecho de contenido complejo no se agota con el amparo de uno de sus elementos esenciales. Los distintos contenidos del derecho a la protección de datos personales son: a) principios (consentimiento informado, finalidad, lealtad y licitud, calidad o exactitud, seguridad, entre otros); b) derechos (derecho a autodeterminación informativa, derechos de acceso, rectificación, cancelación, entre otros); c) deberes (deber de información); y d) garantías (*hábeas data*, garantías institucionales con la creación de entes administrativos que garantizan su amparo). Los contenidos de este derecho serán desarrollados en líneas posteriores, pero se los enuncia con el fin de comprender que es preciso

reconocer a estos de forma conjunta para que se ampare el derecho a la protección de datos personales en toda su composición y complejidad.

A la par de lo explicado, autores como Herrán o Isaza, consideran al derecho de protección de datos personales como un derecho complejo; evidenciando esta postura, uno de los autores manifiesta lo siguiente:

> "El derecho a la protección de datos personales involucra que todas las personas tenemos el derecho fundamental a la protección de nuestros datos personales, que implica la posibilidad de controlar qué se hace con ellos; es decir, de saber quién tiene información sobre nosotros, cuál es esta información, de dónde procede, para qué finalidad se tienen los datos y a quién se facilitan, en tanto que se trata de información que no pertenece a quien la gestiona, sino al titular de los datos." (Isaza, 2014, p. 49)

Siguiendo esta línea, y para ampliar dicho criterio, Herrán concluye luego de una amplia explicación del tema lo siguiente:

> "Ciertamente la protección de datos personales ha sido entendida inicialmente como una manifestación del derecho a la intimidad del individuo, pero este entendimiento, poco a poco ha ido ampliándose, de forma que en la actualidad superando esa inicial consideración se ha ido progresando en su delimitación jurídica hasta alcanzar un concepto jurídico más extenso que comprendería un haz de facultades y actuaciones de la persona que llegaría a significar la posibilidad para la persona de delimitar y determinar hasta qué punto desea comunicar y compartir sus datos, pero no solo eso, sino que no se opone sino que facilita el tratamiento automatizado de la información. Recuérdese que la especialidad en estos casos se encuentra en el hecho de que la agresión no es tanto la publicidad que se concede a la información cuanto que dicha información se introduce en un tratamiento automatizado, con lo que el problema consistirá en que información aparentemente intrascendente pueda llegar a ser importante y desvelar aspectos de la personalidad del interesado que de otro modo hubieran quedado en su esfera personal." (2002, p. 114)

Se evidencia entonces que la configuración del derecho a la protección de datos personales es compleja, su concepto jurídico se ha extendido a tal punto que se compone de varios contenidos esenciales. Bajo estos criterios será preciso entonces explicar los razonamientos por los que este derecho se ha desarrollado de tal forma que se vuelve independiente frente a un derecho que forma parte de sus contenidos esenciales (autodeterminación informativa), pero que no constituye su único núcleo esencial.

2.1.2.2 Independencia del derecho a la protección de datos personales frente a la autodeterminación informativa

Varios tratadistas equiparan a la autodeterminación informativa y al derecho a la protección de datos personales, posición con la que discrepamos. Para nosotros, aunque la autodeterminación informativa es un elemento esencial del derecho a la protección de datos personales, el uno se distingue del otro. El derecho de protección de datos personales no solo se configura por reconocer a las personas el poder de decisión que tienen respecto al tratamiento de su información, también les otorga facultades activas como la rectificación, control o borrado de sus datos durante el manejo y tratamiento que de estos se realice. (Isaza, 2014, p. 49)

Para conocer la corriente que equipara a la autodeterminación informativa con la protección de datos personales, parafraseamos a Davara, este autor manifiesta que la doctrina utiliza la expresión "protección de datos personales" para referirse a la protección jurídica que tienen las personas en lo que concierne al tratamiento automatizado de sus datos personales, y define a esta expresión como:

> "[…] el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad." (Davara, 2008, p. 49)

El autor también se refiere al derecho a la protección de datos personales como una mera "expresión". Consideramos restringida la visión del autor Davara respecto a la concepción del derecho a la protección de datos personales, la misma no divisa ni desarrolla a cabalidad elementos como los derechos ARCO (acceso, rectificación, cancelación y oposición) (AGPD, 2013, p. 22); que, junto con varios principios para el tratamiento de datos personales, construyen el derecho a la protección de datos personales.

Por otro lado, hay posturas de autores como la de Lucas Murillo, quien coincide con la existencia de aspectos distintivos del derecho a la protección de datos personales. Pero equipara a este derecho con el de la autodeterminación informativa, por considerar que el primero es solo una extensión del segundo, criterio que para mayor comprensión se cita a continuación:

> "Personalmente, he preferido hablar de autodeterminación informativa por que, si bien se trata de una fórmula poco estética, es, sin embargo, más precisa pues apunta al núcleo del derecho, a su aspecto sustantivo, mientras que la protección de los datos personales es su manifestación instrumental y, por eso, tiene un carácter técnico que le priva de capacidad significativa [...]" (Lucas, 2008, p. 44)

Murillo en líneas posteriores de su texto se refiere al derecho a la protección de datos personales como sinónimo de autodeterminación informativa. A nuestro criterio, equiparar a la autodeterminación informativa con el derecho a la protección de datos personales desconoce la configuración compleja que caracteriza este derecho.

Como José Luis Barzallo comenta, el derecho a la autodeterminación informativa es amplio, está vinculado con la libertad de expresión por un lado, y por otro también a la protección de datos personales. Es este un derecho extenso, efectivamente en una parte es esencial para que se configure el derecho a la protección de datos personales, pero no solo aplica en ese ámbito, lo que lo convierte en un derecho independiente. (Barzallo, J., entrevista personal, 15 de mayo de 2015)

De igual forma, al explicar la naturaleza compleja del derecho a la protección de datos personales, Naranjo especifica que la autodeterminación informativa podría considerarse el núcleo primigenio, aunque no único, del derecho a la protección de datos personales, pues es uno de sus elementos constitutivos. (Naranjo, L., entrevista personal, 31 de julio de 2015)

Así pues coincidimos con la postura que considera al derecho a la protección de datos personales específico e independiente, por ser un derecho complejo que

no se agota con la autodeterminación informativa del titular de los datos. Este criterio también se ha corroborado con el reconocimiento del derecho de protección de datos personales en el artículo II-68 de la Constitución Europea, o las sentencias 290 y 292 de 30 de noviembre de 2000 (véase fundamento 7) del Tribunal Constitucional Español. (Almuzara, Marzo, Coudert y Navalpotro, 2005, pp. 49-54)

Una vez que se han desarrollado las razones por las consideramos que el derecho a protección de datos personales es un derecho de configuración compleja, es claro que en la actualidad resulte inadecuado equiparar a la autodeterminación informativa con el derecho a la protección de datos personales, ambos efectivamente se interrelacionan (la autodeterminación informativa es una de sus varias manifestaciones), pero son independientes el uno del otro. Esto se evidencia debido a que el derecho a la autodeterminación informativa se materializa por sí mismo, y como tal, únicamente constituye una esfera del derecho a la protección de datos personales, mientras que el segundo no se configura sin el debido amparo de todos sus contenidos esenciales.

2.1.3 Principales corrientes de reconocimiento del derecho a la protección de datos personales

Como se ha venido enunciando, el derecho a la protección de datos personales es un derecho instrumental e independiente, que para ser tutelado efectivamente, precisa del reconocimiento de otros derechos que, en su conjunto, lo consolidan. Debido a que existen divergencias ideológicas respecto al alcance del derecho a la protección de datos personales, no se ha logrado alcanzar mecanismos de tutela homogéneos a nivel mundial, razón por la cual, se han desarrollado tres claras corrientes de reconocimiento de este derecho mundialmente:

2.1.3.1 La corriente estadounidense

Resulta contraproducente pensar que el país que dio vida al *"the right to privacy"*, en la actualidad tenga un incipiente desarrollo de protección de datos a nivel mundial. Para comprender este modelo hay que poner observancia a la realidad política, social, cultural y económica de este país, existe predilección por el desarrollo del mercado y crecimiento de capitales.

Para la corriente los datos son considerados bienes inmateriales, y por lo tanto, se comercializan libremente. (Naranjo, L., entrevista personal, 31 de julio de 2015). Estos datos en Norteamérica representan ganancias inmensas para grandes compañías que venden información. Entonces, es evidente, que no se reconozca como tal el derecho a la protección de datos personales existente en diversas partes del mundo.

Las mínimas regulaciones que aporta este modelo en materia de protección de datos personales promueven el flujo de información, precaviendo los intereses empresariales. Este modelo favorece la autorregulación y considera inapropiada la intervención regulatoria de entes públicos. Debido a los carentes mecanismos de regulación, se han formulado variadas propuestas legislativas, algunas considerando al dato como bien inmaterial sujeto de comercialización; y, otras adaptándose al modelo europeo. (De Miguel, 2011, p. 291). Sin embargo, ninguna de estas propuestas ha tenido la suficiente acogida por parte del sector empresarial y por lo mismo no han prosperado.

Las normas de autorregulación del modelo estadounidense (políticas de privacidad en contratos) se desarrollan en base a principios similares a los del modelo europeo, sin embargo, resultan insuficientes por una razón trascendental: la ausencia de mecanismos que garanticen el cumplimiento de las políticas de privacidad.

Poseen también escasas leyes especiales destinadas a regular ciertos ámbitos delicados como la *"Children's Online Privacy Act"* de 1999, encaminada a

proteger los datos personales de niños menores de 13 años de edad. (De Miguel, 2011, pp. 292-293). Existen varios artículos que corroboran la inconformidad de las personas con la incipiente protección que brindan estas leyes a sus datos personales.

2.1.3.2 La corriente europea

Conforme a lo señalado en líneas anteriores, el derecho a la protección de datos personales en Europa desarrolla la corriente que considera a los datos personales como parte esencial de la personalidad del individuo. Debido a que sus datos definen al humano frente al resto de la sociedad, le son intrínsecos, por lo tanto, no los puede ceder, ni dejará de tener derechos sobre ellos. Se protege a la persona titular del dato y no al dato como tal. (Davara, 2008, p. 50); (Guerrero, 2006, p. 206); (Conde, 2005, p. 29) y (Quintana, p. 27)

Debido a la importancia que se reconoce a los datos en el modelo europeo, este faculta a los poderes públicos a velar por un sistema preventivo que resguarda el derecho a la protección de datos personales. En este modelo la autorregulación es complementaria, pues los entes públicos cumplen un papel protagonista. (De Miguel, 2011, p. 291). Por lo tanto, existe un organismo independiente encargado de precautelar, tanto de forma preventiva como reactiva, el derecho a la protección de datos personales. Dicha entidad tiene autoridad frente a grandes empresas, y goza de amplias facultades, incluso para imponer multas.

El 24 de octubre del año 1995 el Parlamento y Consejo Europeo expiden la Directiva 95/46/CE, con la que unifican en todo el continente el derecho a la protección de datos personales, esta normativa se acoge a los criterios de autodeterminación informativa definidos con anterioridad.

La corriente europea de protección de datos personales desarrolla un sistema preventivo (Naranjo, L., entrevista personal, 31 de julio de 2015), a través del cual se protege a la información de los usuarios *a priori*, esta protección se logra

imponiendo obligaciones a los responsables de tratamiento de datos, a partir de primer momento de la recogida de datos. El sistema preventivo de protección de datos personales se configura con principios, derechos e incluso la participación activa del Estado por medio de un ente estatal que resguarda el derecho de los ciudadanos.

Sin lugar a dudas, la corriente europea de protección de datos personales es la más completa y desarrollada a nivel mundial, a tal punto que incluso en Estados Unidos existen propuestas para implementar normativa que se acoja a ésta corriente.

Es importante mencionar que en Europa, el reconocimiento a la protección de datos personales se recoge pormenorizadamente en leyes generales, aunque a nivel constitucional su amparo sea muy breve y en algunos casos ambiguo (Puccinelli, 2004, p. 21), lo que difiere del caso latinoamericano, como veremos a continuación.

2.1.3.3 La corriente latinoamericana

Países como Argentina, Colombia, México o Perú han integrado a sus legislaciones leyes especiales de protección de datos personales, sin embargo, estas leyes a pesar de recoger amplios conceptos europeos, se adaptan de cierto modo a la corriente estadounidense; realizando también sus propios aportes, como lo es el *hábeas data.* A esta corriente, según Téllez, se la puede considerar un híbrido de las dos explicadas en párrafos anteriores. (2013, p. 117)

Como José Luis Barzallo explica, la protección de datos personales en Latinoamérica nace a partir del *hábeas data*. En Latinoamérica por falta de legislación de protección de datos personales, se adaptaron las normas que se tenían del *hábeas data* a la protección de datos personales. Aunque algunos países si desarrollan normativa específica de protección de datos personales.

José Luis Barzallo también considera a la corriente latinoamericana como un híbrido de las corrientes estadounidense y europea. Por un lado, derecho a la protección de datos personales no es tan estricto como en Europa, y esto responde a la cercanía con los Estado Unidos de América, y por otro lado, es inevitable que se recojan criterios europeos respecto a la concepción del derecho a la protección de datos personales. (Barzallo, J., entrevista personal, 15 de mayo de 2015)

Legislaciones como la colombiana, argentina o mexicana son representantes del modelo latinoamericano de protección de datos personales, las que además de incorporar la figura del *hábeas data* como mecanismo de garantía jurisdiccional del derecho a la protección de datos personales, han implementado leyes específicas de protección de datos personales para reconocer de óptimamente los derechos de sus ciudadanos de forma preventiva y proactiva.

No es posible definir a nivel latinoamericano un modelo específico de protección de datos personales, cada país ha desarrollado legislación con criterios distintivos, sin embargo, el *hábeas data* es un punto de conexión en experiencia de protección de datos personales de los países de Latinoamérica, incluso Ecuador.

De la figura del *hábeas data* se hablará más a fondo en líneas posteriores, pero queremos desatacar que es una propuesta latinoamericana que desarrolla un sistema reactivo de protección de datos personales. (Naranjo L., entrevista personal, 31 de julio de 2015)

Este modelo es conocido por ser reconocido ampliamente a nivel constitucional, sin embargo, solo algunos países poseen leyes específicas de protección de datos personales, (Puccinelli, 2004, p. 21) que desarrollan, a más de un sistema reactivo, un sistema preventivo, implementando autoridades destinadas a velar por el buen cumplimiento de su normativa.

De las tres experiencias de protección de datos personales expuestas podemos deducir que no existe mundialmente un criterio consolidado respeto al reconocimiento del derecho a la protección de datos personales. A pesar de esto, para el caso específico ecuatoriano, será preciso atender a las distintas experiencias internacionales, para poder garantizar holísticamente, tanto preventiva como reactivamente, el derecho a la protección de datos de carácter personal reconocido constitucionalmente.

2.1.4 Reflexiones finales relativas al derecho a la protección de datos personales en el panorama internacional

Como se ha evidenciado en líneas anteriores, no son equivalentes los conceptos de protección de datos personales y de autodeterminación informativa, el primero, al ser un mecanismo de tutela, es un derecho de naturaleza compleja que se configura a través de varios contenidos esenciales (principios, derechos y deberes), es por esto que el óptimo reconocimiento del segundo es imprescindible para que el primero tenga legitimidad.

Sin autodeterminación informativa, el derecho a la protección de datos personales está incompleto, y por lo tanto no se configura. Pero la autodeterminación informativa comprende solo una parte del amplio y complejo derecho que es la protección de datos de carácter personal.

Para que se ampare de forma preventiva un derecho a la protección de datos reconocido formalmente, es necesario desarrollar un sistema preventivo que lo reconozca desde el inicio del tratamiento de datos. Únicamente la conjunción de los sistemas reactivo y preventivo de protección de datos personales configurará, en su complejidad, el derecho que se busca tutelar.

Para que se brinde una adecuada tutela por parte del Estado al derecho a la protección de datos personales no solo se deberán brindar garantías individuales (derechos del individuo), sino también garantías institucionales, (Herrán, 2002, p

93), solo así podrá existir un control previo que genere un sistema preventivo de protección de datos personales.

Las garantías institucionales se configuran con la creación de un ente estatal dedicado exclusivamente a velar por el derecho en cuestión. Esta autoridad podrá configurarse observando parámetros brindados por experiencias como la europea, (véase Herrán, 2002), es decir, teniendo autonomía frente a las funciones estatales y facultades sancionadoras, para un efectivo cumplimiento de sus fines.

Finalmente, es importante considerar que el derecho a la protección de datos personales no se limita a proteger una delimitada esfera de privacidad o intimidad de las personas. Este derecho tampoco puede limitarse a dar a los datos el carácter de bienes inmateriales y protegerlos como tal, aunque la denominación "protección de datos" da lugar a tal confusión. En realidad este derecho protege a la integridad de la persona al considerar a los datos como parte esencial del individuo.

Existen varios modelos de reconocimiento al derecho a la protección de datos personales porque, al ser este un derecho complejo, conlleva el amparo de varios derechos, principios y garantías inmersas en el mismo; y, por lo tanto, su concepción puede variar conforme la corriente ideológica que lo adapte en un ordenamiento jurídico. Pero siempre será necesario velar por que el sistema de protección de datos personales se configure dando amparo de forma preventiva y reactiva.

La presente investigación se demarca al caso ecuatoriano, donde se reconoce constitucionalmente el "derecho a la protección de datos personales" en el artículo 66 numeral 19 de la Constitución de la República. Consideramos que esta declaración constitucional, busca un desarrollo amplio del derecho, en que se implementen criterios que brinden una protección preventiva y reactiva. Por lo tanto, se tomaron como punto de partida distintas experiencias internacionales

que aportan a una ampliación del actual reconocimiento que da la legislación ecuatoriana al derecho a la protección de datos personales.

2.2 Panorama del derecho a la protección de datos de carácter personal en Ecuador

La protección de datos personales en el Ecuador se reconoce formalmente como derecho, en la Constitución de la República en el año 2008; sin embargo, desde 1996 ha existido el desarrollo previo del mecanismo de garantía jurisdiccional denominado *Hábeas Data*, a través del que se ha introducido las primeras nociones de amparo a un derecho a la protección de datos personales en el país.

En lo referente al derecho a la protección de datos personales, no hay en la normativa ecuatoriana un cuerpo legal específico que lo ampare y garantice a plenitud. Existen leyes especiales que se encuentran ligadas a este derecho, como las siguientes: Ley Orgánica de Transparencia y Acceso a la Información Pública, destinada a dar pautas en el tratamiento de información del sector público; Ley del Sistema Nacional de Registro de Datos Públicos, que crea y regula el sistema de registro de datos públicos; y, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que ha incluido un pequeño apartado referido a la protección de datos personales, sin embargo, éste artículo resulta ambiguo y precario, considerando la profundidad del tema.

Por otro lado, han existido en el país propuestas de leyes destinadas a la protección de datos de carácter personal, dichas propuesta no han sido adoptadas, aunque reflejan el interés de ciertos funcionarios por dar vida a la protección de datos en la normativa ecuatoriana.

En el año 2010, se presenta ante la Asamblea Nacional un proyecto de Ley denominado “Ley de Protección a la Intimidad y Datos Personales”, propuesta por Vethoven Chica, proyecto que se desestimó en el 2013 tras recomendación de la Comisión Especializada Permanente de Justicia y Estructura del Estado.

(López Carballo, 2014). Este proyecto de ley desarrollaba criterios arcaicos en materia de protección de datos personales, por lo que se considera positivo que no haya prosperado.

Conforme a lo expresado por el Ing. Fabián Jaramillo Palacios, ex presidente de la Función de Transparencia y Control Social durante el año 2013, la Superintendencia de Telecomunicaciones en su momento desarrolló un proyecto de "Ley de Protección de Datos y Privacidad" (López Carballo, 2014), mismo que no se volvió público y tampoco prosperó, esto debido a que con la promulgación de la Ley Orgánica de Telecomunicaciones en Registro Oficial de 18 de febrero de 2015 este órgano de control dejó de existir.

De lo expuesto en párrafos anteriores, es evidente la necesidad de implementar en el Ecuador una Ley que reconozca a cabalidad el derecho a la protección de datos personales, otorgado a los ecuatorianos con la actual Constitución, y lo tutele con mecanismos de garantías individuales e institucionales, conforme al modelo europeo. La importancia de crear esta Ley, se ve reflejada no solo en los proyectos legislativos creados, sino también, debido al reconocimiento formal de este derecho a nivel constitucional; y, por la implementación del *Hábeas Data* dentro de la normativa ecuatoriana.

2.2.1 Reconocimiento al derecho a la protección de datos personales en la Constitución de la República del 2008

En el año 2008 con la expedición de la actual Constitución de la República del Ecuador, se reconocen nuevos derechos a los ecuatorianos, uno de estos es el derecho a la protección de datos personales, mencionado en el numeral 19 del artículo 66 de este cuerpo legal.

> "19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley." (Constitución, art. 66)

El derecho a la protección de datos de carácter personal en este artículo se define, por un lado, con la autodeterminación informativa al mencionar que *"la recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley*"; sin embargo, también se incluye dentro de tal definición "*el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección*", texto que hace alusión a los derechos ARCO (acceso, rectificación, corrección y oposición) de los que se hablará en párrafos posteriores.
A demás, los numerales 18 y 20 del artículo 66 contemplan otros derechos ligados con la protección de datos personales, como el de la intimidad, el buen nombre, o la honra:

"18. El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona. […]
20. El derecho a la intimidad personal y familiar". (Constitución, art. 66)

Así podemos vislumbrar que nuestra Constitución, además de introducir un nuevo derecho denominado "derecho a la protección de datos de carácter personal", lo distingue de otros derechos como el de la intimidad; o, el de honor y buen nombre, consagrando así en su texto, un nuevo derecho independiente del resto que deberá ser amparado por el Estado, rigiéndose para el ejercicio de derechos enunciados en el texto de la Constitución de la República del Ecuador.

La Corte Constitucional ecuatoriana, en uso de sus facultades, ha desarrollado el contenido complejo y abstracto del derecho a la protección de datos de carácter personal en su sentencia No. 001-14-PJO-CC concerniente al estudio del caso No. 0067-11-JD, con lo cual ha sentado un precedente vinculante en el país. En dicha sentencia la Corte se refiere al derecho a la protección de datos como un derecho con contenido complejo que conlleva varias dimensiones relativas a la información personal, igualmente el análisis de la Corte da apertura a futuros pronunciamientos favorables a un sistema preventivo del derecho a la protección de datos personales.

La sentencia en su parte analítica reconoce al derecho a la protección de datos personales como un derecho específico, independiente y complejo, que no se agota con el reconocimiento de la autodeterminación informativa (derecho que considera un elemento del primero), al respecto nos permitimos citar la parte pertinente de dicha sentencia que esclarece este criterio:

"[…] el derecho a la protección de datos –y específicamente, su elemento denominado "autodeterminación informativa"-, tiene carácter instrumental, supeditado a la protección de otros derechos constitucionales que se pueden ver afectados cuando se utilizan datos personales […]" (Corte Constitucional, sentencia 001-14-PJO-CC, 2014, p. 12)

El razonamiento citado lo emite la Corte Constitucional en base al criterio del doctrinario Óscar Puccinelli, de quien citan el siguiente párrafo dentro del texto de su sentencia:

"[…] Por 'derecho a la protección de datos' se propone entender a la suma de principios, derechos y garantías establecidos en favor de las personas que pudieren verse perjudicadas por el tratamiento de los datos nominativos a ella referidos […]" (Puccinelli, como se citó en Corte Constitucional, sentencia 001-14-PJO-CC, 2014, p. 12)

La sentencia al distinguir a la autodeterminación informativa como elemento constitutivo del derecho a la protección de datos personales, no considera a estos derechos como sinónimos, es más brinda al segundo autonomía compleja. Al derecho a la protección de datos personales se le reconoce el carácter de complejo e instrumental, esto debido a que se conforma de derechos, principios y garantías, y también se ha desarrollado más que la autodeterminación informativa.

Lastimosamente, la *ratio decidendi* de esta sentencia se desliga por completo análisis general citado, concluyendo en definitiva que las personas jurídicas

podrán tener legitimación activa para presentar acciones de *hábeas data* bajo ciertos supuestos. (Véase Corte Constitucional, sentencia 001-14-PJO-CC, 2014, pp. 20-22)

Así podemos observar claramente la sentencia de la Corte Constitucional fundamenta su parte analítica en criterios que conciben al derecho a la protección de datos personales como un derecho de configuración compleja, como ya se ha descrito en líneas previas. Esto brinda una luz al futuro desarrollo del derecho a la protección de datos personales como derecho subjetivo. Sin embargo, la *ratio decidendi* de esta sentencia no aporta en nada al desarrollo del derecho a la protección de datos personales como un derecho complejo, lo que desvaloriza por completo a la parte analítica de la sentencia. Tendrá que pasar mucho tiempo para que la Corte Constitucional, por medio de jurisprudencia vinculante, desarrolle ampliamente todos los elementos que componen el derecho a la protección de datos personales, y configure así un sistema preventivo de protección de datos personales en Ecuador.

2.2.2 La acción del *hábeas data* como mecanismo de garantía jurisdiccional

En el año de 1988 aparece en Brasil la acción de *hábeas data*, con este antecedente, los países de América del Sur comienzan a incorporar figuras similares en sus constituciones. En el caso de Ecuador, por medio de una reforma constitucional de enero de 1996, aparece el *hábeas data*, acción que se regula con la promulgación de la Ley de Control Constitucional, publicada en el Registro Oficial No. 99 del 2 de julio de 1997. Posteriormente, se lo regulariza en la Constitución de 1998. (Salmon, s.f., p. 131)

El término *"hábeas data"* proviene del latín "*habere"* que significa "téngase en posesión" y de "*datum*" que significa dato, por lo tanto, esta frase significa literalmente "traer los datos". (Salmon, s.f., p. 130). Igualmente, esta acción tiene su antecedente en la acción de "*habeas corpus*", la misma que inspiró su creación.

En el artículo 92 de la Constitución de la República del Ecuador ampara la acción de "*habeas data"* bajo los siguientes términos:

> "Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.
>
> Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.
>
> La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados." (Salmon, s.f., p. 135)

Conforme desprende del artículo previamente citado, la acción de *hábeas data* que se reconoce constitucionalmente en Ecuador, es amplia, y faculta por si misma, al titular de los datos para conocer del destino y uso que se haga de estos, así como, para ejercer acciones para que su información sea utilizada de forma óptima, sin violentar sus derechos.

Para Pérez Luño "El *hábeas data* constituye un cauce procesal para salvaguardar la libertad de la persona en la esfera informática", para este autor esta acción es con naturaleza jurídica paralela a la del *hábeas corpus,* ambas constituyen mecanismos de garantía procesales de defensa de derechos de libertad personal en el caso del *hábeas corpus* y de libertad informática en el caso del *hábeas data.* (1996, pp. 44-45)

Como se ha evidenciado, el *hábeas data* comprende un mecanismo de garantía jurisdiccional que contempla un amplia gama de facultades para el titular de los datos. Estas facultades sin lugar a duda configuran en Ecuador un sistema reactivo de protección de datos personales. Con sistema reactivo queremos

decir que la interposición de una acción de *hábeas data,* se condiciona necesariamente a la existencia previa del tratamiento de datos personales. Es decir, existiría ya una relación en la cual el titular de la información haya facultado a una persona (responsable de tratamiento) a realizar tratamiento de sus datos personales. Es evidente entonces que el *hábeas data* no brinda a los ecuatorianos un sistema preventivo de protección de datos personales.

Por lo dicho, no se puede considerar como equivalentes a una garantía como el *hábeas data* y el derecho a la protección de datos de carácter personal. Si bien, esta acción ampara, a nivel constitucional, derechos como el de autodeterminación informativa, o el de acceso a los datos; no es un mecanismo suficiente para el amparo completo de un derecho complejo como el de protección de datos de carácter personal. Esta garantía no configura en el Ecuador un sistema preventivo de protección de datos personales, sistema que a criterio de la autora debe implementarse para un real amparo del derecho que se reconoce a los ecuatorianos en el numeral 19 del artículo 66 de la Constitución de la República.

2.2.3 El derecho a la protección de datos personales en la normativa ecuatoriana

Como se ha evidenciado en líneas previas, la normativa ecuatoriana reconoce el derecho a la protección de datos de carácter personal de forma clara y expresa a nivel constitucional. La Constitución ecuatoriana también desarrolla el mecanismo de amparo del *hábeas data*, acción que es efectiva para proteger el derecho a la protección de datos personales cuando ya ha ocurrido la violación o ya existe tratamiento de datos. Por lo tanto, el *hábeas data* resulta insuficiente para prevenir la violación del derecho a la protección de datos personales, debido a que su contenido es amplio y complejo, y no se agota únicamente con el amparo de garantías jurisdiccionales, sino con el desarrollo de principios y deberes específicos.

Como explica Ramiro Ávila acogiéndose a la idea garantista de Luigi Ferrajoli, con la Constitución del 2008 se implementa en el Ecuador una concepción integral de las garantías no restringida a lo judicial, estas garantías se clasifican en dos grupos: la primera, en función de los poderes del Estado; y, la segunda, en relación a los derechos y al rol de la justicia constitucional. Nos interesa hacer referencia para el caso particular a las garantías que existen en función de los poderes del Estado, las que se dividen en tres: normativas, políticas públicas y jurisdiccionales. Ávila sintetiza el criterio de Ferrajoli expresando que no existe poder del Estado que no sea garante de los derechos constitucionales. (Ávila et al., 2008, p. 93)

Para Naranjo en Ecuador, el *hábeas data* se utiliza como único mecanismo de protección de datos personales. Esta garantía jurisdiccional si bien evita transgresiones directas a través de los derechos de acceso, rectificación, cancelación y oposición; no permite proteger otros derechos que pueden verse conculcados por la elaboración de perfiles con datos erróneos de las personas. Por lo que es indispensable nutrir de contenidos esenciales al derecho a la protección de datos personales a través de normativa, jurisprudencia, definición y aplicación de políticas públicas, y de la creación de una institución dedicada exhaustivamente a proteger el de los titulares de estos datos. (Naranjo L., entrevista personal, 31 de julio de 2015)

Convencidos de que en Ecuador es necesario implementar normativa de protección de datos personales, pues solo así será posible configurar un derecho a la protección de datos personales complejo que ampare a los ecuatorianos no solo de forma reactiva, sino también preventiva, reafirmamos nuestro criterio con lo previsto en el artículo 84 de la Constitución de la República.

> "Art. 84.- La Asamblea Nacional y todo órgano con potestad normativa tendrá la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales, y los que sean necesarios para garantizar la dignidad del ser humano o de las comunidades, pueblos y nacionalidades. En ningún caso, la reforma de la Constitución, las leyes, otras normas jurídicas ni los actos del poder público atentarán contra los derechos que reconoce la Constitución."

Es así que, la existencia del derecho constitucional a la protección de datos de carácter personal exige el desarrollo de criterios específicos que, además de operativizar judicialmente el derecho, desarrollen su contenido preventivo ampliamente en normativa especial. El Estado ecuatoriano entonces está obligado a implementar normativa que garantice el derecho a la protección de datos personales de forma preventiva, independientemente de si ya se contempla la garantía jurisdiccional denominada *hábeas data.*

Se ha evidenciado entonces la necesidad de crear una ley de protección de datos de carácter personal dentro de la legislación ecuatoriana. Esta ley, deberá moldearse adoptando los criterios que recoge en su texto la Constitución de la República, al reconocer el derecho a la protección de datos de carácter personal. Como hemos manifestado en líneas previas, los criterios que deben inspirar al legislador ecuatoriano en la redacción de esta ley, deberán estar sustentados en un derecho mucho más desarrollado y completo, que haga énfasis en el desarrollo de un sistema de protección de datos preventivo, lo que solo se podrá lograr observando experiencias internacionales y acogiendo principios estándares aceptados por diversos países.

Debido a que el presente trabajo precisa delimitar algunas pautas conceptuales del derecho a la protección de datos personales se han observado ciertos criterios internacionales concordantes con los Estándares Internacionales sobre Protección de Datos Personales y Privacidad difundidos por la Red Internacional de Protección de Datos, foro del que Ecuador es país miembro. Esto con el fin de describir a continuación algunos parámetros, que consideramos deberían ser adecuados en la normativa ecuatoriana, para generar y reforzar un sistema preventivo que posibilite el amparo del derecho a la protección de datos personales en Ecuador.

2.2.3.1 Estándares generales del derecho a la protección de datos personales

Como ya se ha mencionado en párrafos previos, aunque en Ecuador no existe una ley de protección de datos personales, este trabajo precisa definir estándares generales que sirvan de base para comprender la importancia y complejidad de un sistema preventivo que resguarde el derecho a la protección de datos personales.

Conforme a lo estudiado en líneas anteriores, los criterios recogidos en el modelo europeo se han construido a través de un desarrollo empírico y por ende jurisprudencial, que ha desencadenado en la expedición de normativa general con conceptos estándar que desarrollan un sistema preventivo de protección de datos personales y pueden ser acogidos por varias legislaciones. El sistema preventivo de protección de datos personales, a nuestro criterio, se conjuga con las nociones generales que contempla la normativa ecuatoriana y con el contenido de los Estándares Internacionales sobre Protección de Datos Personales y Privacidad difundidos por la Red Internacional de Protección de Datos, foro del que Ecuador es país miembro.

Para continuar en el capítulo tercero con el análisis materia de la presente investigación referido al derecho a la protección de datos personales de usuarios ecuatorianos en relaciones B2C con proveedores de servicios de *cloud computing,* ha sido preciso recoger una variedad de conceptos contemplados en los Estándares Internacionales sobre Protección de Datos Personales y Privacidad difundidos por la Red Internacional de Protección de Datos. Estos conceptos se amplían con el contenido de normativa europea como la Directiva 95/46/CE del Parlamento y del Consejo Europeo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la Ley Orgánica de Protección de Datos de Carácter personal de España, y con doctrina internacional.

2.2.3.1.1 Sujetos activos del derecho a la protección de datos personales

Como se ha planteado repetidas veces, el derecho a la protección de datos personales tiene su antecedente en el derecho a la intimidad, por ser un derecho ligado a la personalidad está direccionado a la protección de personas naturales. (Guerrero, 2006, pp. 22-24). La legislación española reconoce este derecho únicamente a personas naturales, sin embargo, otras legislaciones también se lo reconocen a las personas jurídicas.

Considerando que existen contradicciones y no hay unanimidad respecto a la protección de personas jurídicas, y mucho menos en aquellos casos en que personas naturales componen personas jurídicas (Santos, 2005, pp. 38-40), a nuestro criterio, este derecho debería expandirse para aquellos casos en que el buen nombre y por ende fama de personas jurídicas se pueda ver afectado por el tratamiento erróneo de sus datos, es decir, cuando dichos entes jurídicos puedan demostrar su legítimo interés.

Cabe señalar que el texto de la sentencia No. 001-14-PJO-CC de la Corte Constitucional dictada el 23 de abril de 2014 reconoce la legitimación activa de personas jurídicas para presentar la acción de *hábeas data* en Ecuador, criterio deberá expandirse para la implementación de una Ley de Protección de Datos Personales en este país.

Al respecto, el artículo 51 de la Ley de Garantías Jurisdiccionales y Control Constitucional describe como legitimados activos de la acción a hábeas data a "toda persona, natural o jurídica, por sus propios derechos o como representante legitimado para el efecto." (LOGJCC, art. 51)

2.2.3.1.2 Definiciones generales del derecho a la protección de datos personales

2.2.3.1.2.1 Datos personales

En el texto de los Estándares internacionales sobre Protección de Datos Personales y Privacidad, se define al dato de carácter personal como aquella información concerniente a una persona identificada o identificable a través de medios que puedan utilizarse razonablemente. (Conferencia Internacional de Autoridades de Protección de Datos y Privacidad 31 [CIAPDP], 2009, pp. 7). Este estándar puede ser ampliado con el texto de la Directiva 95/46/CE del Parlamento y del Consejo Europeo que define a los datos personales de la siguiente forma:

> "Art 2.- Toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, cultural o social." (Dir.95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995)

En la legislación ecuatoriana, la disposición general novena de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos define a datos personales como "aquellos datos o información de carácter personal o íntimo que son materia de protección en virtud de esta ley" y como datos personales autorizados a:

> "[…] aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el que fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular." (LCEFEMD).

Así, los datos personales siempre estarán relacionados con aquella persona que puede identificarse a través de la información que pueda obtenerse de estos o su asociación. (Véase Santos, 2005, pp. 42-43). Para complementar esta

definición parafraseamos a Davara, al decir que los datos personales son aquellos pertenecientes a la persona, y por ser parte del individuo, afectan a su vida privada e intimidad, por lo que son personalísimos, siendo únicamente su titular quien puede decidir sobre los mismos. (2008, p. 53)

La legislación ecuatoriana en la Ley del Sistema Nacional de Registro de Datos Públicos realiza la siguiente distinción respecto a la accesibilidad de los datos:

> "Art. 6.- Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales.
>
> El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial.
>
> También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado […]." (LSNRDP, art. 6)

El artículo 92 de la Constitución de la República en su inciso tercero da la pauta para la existencia de un régimen distinto para el tratamiento de datos sensibles, un régimen similar al europeo, al especificar lo siguiente:

> "[…] En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se entendiera su solicitud, esta podrá atender a la jueza o juez […]" (Constitución, art. 92)

El texto de la Ley del Sistema Nacional de Registro de Datos Públicos, relativo a los datos confidenciales, en la actualidad es la única definición legal aplicable a los datos sensibles a los que se refiere el artículo 92 de la Constitución de la República. Sin embargo, dicha definición resulta insuficiente para describir a cabalidad lo que en realidad es un dato sensible y el régimen especial de protección de datos sensibles a los que se refiere la doctrina y al desarrollo legislativo internacional del derecho a la protección de datos personales. Así

vislumbramos la necesidad de incorporar en nuestra legislación un régimen especial para la protección de datos sensibles, en el cual se amplíe la definición de este tipo de datos; y, aunque la misma no se homogénea a nivel mundial, consideramos importante citar la que aporta Serrano:

> "[…] los datos sensibles pueden definirse desde un punto de vista formal y desde un punto de vista material. Formalmente son aquellas categorías de datos que requieren unas especiales y reforzadas garantías de tratamiento. Desde el punto de vista material hacen referencia a las cualidades de la persona que definen su dignidad, que configuran su personalidad, que dibujan su forma de ser y de comportarse." (2003, p. 380)

La definición citada por su amplitud, debería adaptarse a nuestra legislación, puesto que esto representaría reconocer a los ecuatorianos un derecho a la protección de datos personales mucho más avanzado, basado en criterios doctrinarios plasmados en otras legislaciones internacionales del derecho a la protección de datos personales sensibles.

2.2.3.1.2.2 Tratamiento de datos

El derecho a la protección de datos personales se reconoce para aquellos casos en que exista tratamiento de datos de carácter personal. Es por esto, que resulta imperativo entender lo que es el tratamiento de datos personales.

Los Estándares Internacionales sobre Protección de Datos Personales y Privacidad difundidos por la Red Internacional de Protección de Datos, definen al tratamiento como cualquier operación o conjunto de operaciones, automatizadas o no, aplicadas a datos de carácter personal. (CIAPDP, 2009, p. 7). Ampliando la definición desarrollada, La Directiva 95/46/CE del Parlamento y del Consejo Europeo puntualiza lo siguiente:

> "Art. 2. […] b) Cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite al acceso de los mismos, cotejo o interconexión,

> así como su bloqueo, supresión o destrucción." (Dir. 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995)

En concordancia a esta definición encontramos a la establecida en el artículo 3 de la Ley Orgánica de Protección de Datos de Carácter Personal española 15/1999 de 13 de diciembre:

"[…] c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias […]" (LOPD, art. 3)

Al respecto Conde Ortiz comenta que el eje a considerarse para determinar si nos encontramos frente a un tratamiento de datos es característica de "técnicos", además concluye que la expresión "de carácter automatizado o no" amplia el ámbito de protección a todas las fases del manejo del dato, sea o no automatizada. (Conde, 2005, p. 79). Así Santos al referirse al ámbito de aplicación de la Ley Orgánica de Protección de Datos española hace alusión a los datos automatizados o no automatizados. (2005, p. 43)

La normativa ecuatoriana no brinda una definición clara del tratamiento de datos como tal, sin embargo, contempla referencias en el texto de varios cuerpos legales que dan la pauta para aplicar la definición estándar contemplada en la normativa europea.

Del texto observado en el numeral 19 del artículo 66 de la Constitución de la República se despliega una posible enunciación del tratamiento de datos como "la recolección, archivo, procesamiento, distribución o difusión de estos datos o información". Además el artículo 92 del mismo cuerpo legal al establecer "en soporte material o electrónico" hace alusión al tratamiento de datos tanto por medios electrónicos como materiales. Finalmente, hay que tomar en cuenta la mención realizada en el inciso primero del artículo 9 de la Ley de Comercio

Electrónico, Firmas Electrónicas y Mensajes de Datos haciendo alusión a este concepto al indicar que “para la elaboración, trasferencia, o utilización de bases de datos obtenidas directa o indirectamente del uso o transmisión de mensajes de datos […]” (LCEFEMD, art. 9). Como se puede observar la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos únicamente se refiere al tratamiento de datos que ser realice por medios electrónicos, sin embargo nuestra Carta Magna es muy específica al considerar tanto medios electrónicos como materiales. Por lo tanto, consideramos indispensable aplicar los criterios constitucionales en normativa de protección de datos personales, la misma que contemple el tratamiento de datos personales por medios materiales o electrónicos.

2.2.3.1.2.3 Ficheros de datos

La Directiva 95/46/CE del Parlamento y del Consejo Europeo define al fichero de datos personales de la siguiente forma:

“Art 2. […] c) Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.” (Dir. 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995)

Para Conde Ortíz, un fichero es aquel soporte que permite la acumulación de datos personales de forma organizada y su consecuente tratamiento. (Conde, 2005, pp. 75-77). Así este autor concluye que no es indispensable la existencia de un fichero para que aplique el derecho a la protección de datos personales, bastará con que los datos se encuentren organizados de alguna forma. También será importante considerar que los ficheros informatizados o manuales deberán ser regulados.

La normativa ecuatoriana no contempla una definición de ficheros de datos, sin embargo, la utilización de términos como “archivos” o “bancos de datos” (referidos soportes materiales y digitales), contemplados en la redacción del

artículo 92 de la Constitución de la República, y del artículo 49 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional; pueden dar la pauta para desarrollar el término a cabalidad adoptando, como modelo los criterios que trae consigo la normativa europea.

2.2.3.1.2.4 Procedimiento de disociación

La Ley Orgánica de Protección de Datos de Carácter Personal española 15/1999 de 13 de diciembre, define al procedimiento de disociación de la siguiente forma:

"Art 3. […] f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable." (LOPD, art. 3)

Para Santos, dejan de ser datos personales aquellos obtenidos por medio de un procedimiento que no permita identificar a la persona a quien se refiere la información recopilada. (2005, p. 43). Al respecto es importante mencionar que, para que el criterio de este autor aplique, deberá ser imposible identificar los datos compilados con su titular.

Aunque la normativa ecuatoriana no hace mención en su contenido a algún estipulado que se encuentre vinculado al procedimiento de disociación, este concepto está ligado al tratamiento de los datos personales, y se encuentra ligado a derechos como el de oposición o cancelación. Por lo que es indispensable que para la creación de normativa de protección de datos en Ecuador se lo integre en su texto supliendo el vacío existente en la actualidad.

2.2.3.1.2.5 Cesión de datos

La Ley Orgánica de Protección de Datos de Carácter Personal española 15/1999 de 13 de diciembre, define a la cesión de datos de la siguiente forma:

“Art 3. […] i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.” (LOPD, art. 3)

Artículo 11. Comunicación de datos.

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado […]” (LOPD, art. 11)

La normativa ecuatoriana se refiere a la cesión de datos en el artículo 66 numeral 19 de la Constitución de la República de la siguiente forma:

“19. […] La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.” (Constitución, art. 66)

El mismo cuerpo legal hace alusión al mismo término cuando en el primer inciso de su artículo 92 declara que el titular de los datos “tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.” (Constitución, art. 92)

En último lugar, citamos el inciso primero del artículo 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos que hace referencia a la cesión de datos bajo los siguientes términos:

> “Art 9.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros […]” (LCEFEMD, art. 9)

Concordamos con la visión de Vizcaíno, quien considera al concepto como cualquier forma de revelación o manifestación de los datos a un tercero por parte del responsable del tratamiento. (2001, pp. 157-158). Para que las reglas

relativas a la cesión sean adaptables a un sistema de protección de datos personales, es preciso observar la realidad de cada caso particular.

Con lo señalado, es claro que la normativa ecuatoriana vigente da la pauta para que, con la implementación de una ley de protección de datos de carácter personal, se defina el concepto de cesión de datos, estándar imprescindible para el óptimo reconocimiento del derecho a la protección de datos personales ecuatoriano. Pero al momento de definir este estándar deberemos estar atentos a la realidad de casos prácticos, para que la normativa no sea anticuada.

2.2.3.1.3 Los responsables de tratamiento

En los Estándares Internacionales sobre Protección de Datos Personales y Privacidad difundidos por la Red Internacional de Protección de Datos, se define a la persona responsable como "aquella persona física o jurídica, de naturaleza pública o privada que, sola o en conjunto de otros, decida sobre el tratamiento." (CIAPDP, 2009, p. 7). En la misma línea, la Directiva 95/46/CE del Parlamento y del Consejo Europeo define al responsable de tratamiento de la siguiente forma:

> "Art 2. […] d) La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario." (Dir. 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995)

Al respecto, la normativa ecuatoriana hace referencia a este sujeto en el artículo 92 de la Constitución de la República y el artículo 49 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, bajo los siguientes términos:

> [CR] Art. 92.- "[…] Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

> La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo […]" (Constitución, art. 92)

[LOGJCC] Art. 49.- "El titular de los datos podrá solicitar al responsable del archivo o banco de datos […].

Las personas responsables de los bancos o archivos de datos personales […]" (LOGJCC, art. 49)

Bajo estos criterios, resulta factible la implementación de una definición estándar basada en el modelo europeo respecto a los responsables de tratamiento de datos personales.

2.2.3.1.4 Los encargados de tratamiento

Los prestadores de servicios de tratamiento son definidos en los Estándares Internacionales sobre Protección de Datos Personales y Privacidad, difundidos por la Red Internacional de Protección de Datos, como "persona física o jurídica, distinta de la persona responsable, que lleva a cabo un tratamiento de datos de carácter personal por cuenta de dicha persona responsable." (CIAPDP, 2009, p. 7). En la misma línea, la Directiva 95/46/CE del Parlamento y del Consejo Europeo define a los encargados de tratamiento de la siguiente forma:

"Art 2. […] e) la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento." (Dir. 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995)

La normativa ecuatoriana no es clara en mencionar un criterio ligado a los encargados de tratamiento, sin embargo, el inciso tercero del artículo 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Dato, a nuestro juicio al hacer alusión a las "personas vinculadas por una relación de negocios, laboral, administrativa o contractual" hace factible considerar una definición

patrón basada en el modelo europeo para los encargados de tratamiento. Lo mencionado también se sustenta en el hecho de que estos sujetos derivan de la existencia de responsables de tratamiento de datos personales, los que si se contemplan claramente en la normativa ecuatoriana.

2.2.3.1.5 Principios del derecho a la protección de datos personales

Los principios que se desarrollan a continuación son aceptados a nivel mundial como elemento esencial para la configuración del derecho a la protección de datos personales. Estos principios se recogen en los Estándares Internacionales sobre Protección de Datos Personales y Privacidad difundidos por la Red Internacional de Protección de Datos, foro del que Ecuador es país miembro. Es importante señalar que estos principios, en conjunto, constituyen el pilar del sistema preventivo de protección de datos personales que precisa desarrollarse en Ecuador y se consideran un componente esencial y fundamental del derecho a la protección de datos personales.

2.2.3.1.5.1 Principio de consentimiento informado

Respecto al consentimiento, será necesario que el titular de los datos manifieste previamente su voluntad libre, inequívoca, específica e informada para que opere la recogida y tratamiento de datos. (Armagnague, 2002, pp. 381-382). El consentimiento variará conforme a los tipos de datos que sean tratados, en ciertos casos de interés público, incluso no será necesario que el mismo se expresado.

El consentimiento, como regla general, deberá ser libre e informado, expreso y específico, y, revocable, aunque estas características puedan variar en ciertos casos concretos. (Sánchez, 1998, pp. 92-93)

La normativa ecuatoriana se refiere al consentimiento en el artículo 66 numeral 19 de la Constitución de la República de la siguiente forma:

“19. […] La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.” (Constitución, art. 66)

El mismo cuerpo legal hace alusión al término cuando en el primer inciso de su artículo 92 declara que “las personas responsables de los bancos o archivos de datos personales podrán difundir la información la información archivada con autorización de su titular o de la ley.” (Constitución, art. 92)

También el inciso primero del artículo 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos hace referencia al consentimiento informado del titular de datos y a las excepciones existentes, bajo los siguientes términos:

> “Art 9.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros […]
>
> “No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.
>
> El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.” (LCEFEMD, art. 9)

Así vislumbramos que la normativa ecuatoriana contempla en su texto al consentimiento expreso del titular de los datos, e incluso señala casos determinados para los cuales no sería necesario dicho consentimiento. Hay que distinguir al consentimiento expreso del informado, el primero solamente constituye una manifestación de la voluntad del titular de los datos (voluntad que podría estar viciada); mientras que el consentimiento informado implica la manifestación de voluntad realizada en base a la información previa que haya brindado el responsable de tratamiento.

En base a la diferencia sustancial que existen entre el consentimiento expreso e informado, es importante que para que exista un óptimo reconocimiento del derecho a la protección de datos personales en el Ecuador, se desarrolle normativa que exija un consentimiento no solo expreso, sino también informado del titular de los datos, en contexto con el desarrollo de la doctrina y legislación comparada. Solo de esta forma se configurará efectivamente el derecho a la autodeterminación informativa, que a su vez, constituye un elemento esencial para el derecho a la protección de datos personales.

2.2.3.1.5.2 Principio de finalidad

El principio de finalidad es definido en los Estándares Internacionales sobre Protección de Datos Personales y Privacidad difundidos por la Red Internacional de Protección de Datos en base a los siguientes estipulados:

> "1. El tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas de la persona responsable. 2. La persona responsable se abstendrá de llevar a cabo tratamientos no compatibles con las finalidades para las que hubiese recabado los datos de carácter personal, a menos que cuente con el consentimiento inequívoco del interesado." (CIAPDP, 2009, p. 10)

Previa la creación de un fichero de datos personales será preciso conocer la finalidad del mismo, para Del Peso Navarro este principio es tan amplio que incluso engloba otros principios como el de utilización no abusiva y el de pertinencia. (2000, p. 18). La aplicación de este principio estará condicionada a que el responsable del fichero indique desde un inicio la finalidad de los ficheros de datos, para así verificar que los datos recolectados empaten con dicha finalidad. Los datos brindados para determinadas razones no podrán utilizarse para otros fines que los inicialmente establecidos. Dichos fines deberán ser determinados y específicos, en caso de modificación posterior de la finalidad esta deberá ser compatible con la establecida inicialmente.

Este principio puede verse violentado en el caso de transmisión de datos entre ficheros, frente a lo cual será preciso realizar un control de los procedimientos y protocolos técnicos de transmisión de datos. También será preciso poner observancia a los datos que hubiesen dejado de estar sujetos a un fin, caso en el cual se procederá a destruirlos o conservarlos de forma anónima. (Sánchez, 1998, pp. 83-85)

El principio de finalidad debe ser analizado detenidamente, pues existirán casos claros en que la finalidad del tratamiento faculte únicamente a una empresa para un fin específico en el tratamiento de datos; pero por la existencia de ciertas cláusulas contractuales dichas facultades se expanden a varias empresas asociadas directa o indirectamente con el proveedor, ampliando también la finalidad de uso de los datos. En aquellos casos la finalidad será difusa para el usuario, pues no sabrá a ciencia cierta qué persona tendrá acceso a su información y para qué la utiliza.

2.2.3.1.5.3 Principio de lealtad y licitud

En los Estándares Internacionales sobre Protección de Datos Personales y Privacidad difundidos por la Red Internacional de Protección de Datos se define a este principio de la siguiente forma:

> "1. Los tratamientos de datos de carácter personal se deberán realizar de manera leal, respetando la legislación nacional aplicable y los derechos y libertades de las personas, de conformidad con lo previsto en el presente Documento y con los fines y principios de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos. 2. En particular, se considerarán desleales aquellos tratamientos de datos de carácter personal que den lugar a una discriminación injusta o arbitraria contra los interesados." (CIAPDP, 2009, p. 10)

En lo que a este principio respecta, la lealtad se refiere a las circunstancias en que se han recogido los datos, que las finalidades de su recogida y tratamiento sean legítimas, y la pertinencia de la información frente a la finalidad por la que se recolectó. El autor Del Peso Navarro (2000, p. 19) considera que por medio de este principio "el procedimiento para recabar los datos a los afectados no ha

de ser de forma ilícita o desleal". Para que este principio opere, será necesario la aplicación de procedimientos transparentes utilizados en el recogida de los datos; igualmente, será preciso obtener consentimiento informado del titular de los datos, previa su recogida y tratamiento, salvaguardando la licitud y lealtad de forma preventiva (Sánchez, 1998, pp. 82-83)

Para que este principio se active es indispensable que también se aplique el principio de finalidad, así el titular de los datos, por un lado, conocerá *a priori* la finalidad del tratamiento de sus datos; y, posteriormente, podrá constatar que el tratamiento se realiza de forma leal y lícita.

2.2.3.1.5.4 Principio de calidad o exactitud

Como se ha mencionado, las denominaciones que se utilizan para delimitar estos principios son variadas, es así que los Estándares Internacionales sobre Protección de Personales y Privacidad difundidos por la Red Internacional de Protección de Datos definen al principio de calidad y exactitud se define disyuntivamente separándolo en principio de proporcionalidad y principio de calidad, (CIAPDP, 2009, p. 11), sin embargo, el contenido de este principio es el mismo.

Conforme a este principio, los datos deberán ser pertinentes, no excesivos, exactos y actualizados respecto a los fines para los que se recogieron. Este principio va de la mano con el de "finalidad de los datos", a partir de la que se determinará su calidad y exactitud. (Sánchez, 1998, pp. 85-86)

La exactitud de los datos implica que los datos objeto de tratamiento, no serán deformados. Los datos deberán ser completos, para lo cual será necesaria su periódica actualización y verificación. (Molina, 2012, p. 488). Además este principio implica que el responsable del fichero deberá también proporcionar los medios necesarios para comprobar la exactitud y actualización de los datos recogidos, (Del Peso, 2000, p. 19), es decir, también contempla obligaciones para dicho actor.

Es elemental la aplicación de este principio pues garantiza al titular de los datos que su información no será tergiversada y se utilizará sin alteraciones que pudiesen llegar a perjudicarlo.

2.2.3.1.5.5 Principio de conservación limitada de los datos

Por medio de este principio se establece un tiempo máximo de conservación de datos personales, con el objeto de asegurar a los individuos que su cierta información relativa a estos no supondrá un elemento universal que lo defina eternamente. La excepción a este principio es aquella información que posteriormente adquirirá relevancia histórica, casos en que será necesario, transcurrido un periodo de tiempo, disociar a los datos de su titular. El periodo de conservación de los datos deberá estar conectado a la finalidad de su registro, de no ser así, podrían conservarse datos descontextualizados que acarrean perjuicios para sus titulares. (Sánchez, 1998, pp. 86-87)

Es elemental que el titular de los datos sepa que su tratamiento tiene un tiempo de vigencia y no lo perfilarán para siempre, además este principio también impone al responsable de tratamiento la obligación de no mantener eternamente información antigua, que muchas veces, por el tiempo deja de ser fidedigna.

2.2.3.1.5.6 Principio de no utilización abusiva

Se establece por medio de este principio que los datos recogidos no podrán ser utilizados para finalidades incompatibles con aquellas establecidas para su recogida. (Del Peso, 200, p. 18). Debido a este principio, tanto la finalidad que se establezca en la recogida para el uso de los datos, y los procedimientos empleados durante el tratamiento de éstos, deberán ser informados previamente a los titulares de dichos datos. De este modo, los responsables de los ficheros aseguran una coherencia lógica entre los presupuestos y resultados del procedimiento de tratamiento de los datos personales. (Sánchez, 1998, p. 88)

En los Estándares Internacionales sobre Protección de Datos Personales y Privacidad difundidos por la Red Internacional de Protección de Datos recoge el contenido de este principio en el que denominan “principio de responsabilidad”, y como se observa a continuación tiene una estrecha relación con el principio e utilización no abusiva:

> “La persona responsable deberá: a) adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en el presente Documento y en la legislación nacional aplicable, y b) dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervisión en el ejercicio de sus competencias, conforme a lo establecido en el apartado 23.” (CIAPDP, 2009, p. 13)

El principio de utilización no abusiva es el resultado de la aplicación de principios como el de finalidad o el de licitud, sin los cuales no existiría un tratamiento de datos óptimo realizado mediante procedimientos transparentes.

2.2.3.1.5.7 Principio de seguridad

El principio de seguridad en la normativa comunitaria europea se incorpora por medio del artículo 17 de la Directiva 95/46/CE del Parlamento y del Consejo Europeo, mismo que se cita a continuación:

> “Art. 17.- Seguridad.- 1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la perdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.
>
> Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.
>
> 2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

> 3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:
>
> — que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;
>
> — que las obligaciones del apartado I, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.
>
> 4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente." (Dir. 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995)

Este principio atiende a la necesidad del titular de que sus datos sean tratados de forma segura por el responsable del tratamiento, lo que constituye un factor clave para el éxito de todo sistema de protección de datos. (Puccinelli, 2004, p. 231). Para la Agencia Española de Protección de Datos, la seguridad supone que quien trate los datos garantice a través de sistemas técnicos y organizativos se encargará de precautelar por su integridad, disponibilidad y confidencialidad de la siguiente forma:

- La integridad supone que la información no será objeto de modificaciones no autorizadas, lo que se obtiene por medio de la asignación de contraseñas o cierre de sesión automático.

- La disponibilidad se garantiza cuando los datos siempre son accesibles a las personas autorizadas, esto se consigue por medio de *back ups*, también conocidos como copias de seguridad.

- Finalmente, la confidencialidad se precautela cuando la información únicamente es conocida y accesible para los usuarios autorizados. (2013, pp. 17-18)

Para Vízcaíno será preciso adoptar medidas de índole técnica y organizativa para garantizar la seguridad de los datos y evitar su alteración, perdida, tratamiento o acceso no autorizado. (2001, p. 142)

En la normativa ecuatoriana el artículo 26 de la Ley del Sistema Nacional de Registro de Datos Públicos tiene relación con las medidas de seguridad, mismo que se cita a continuación:

> "Art. 26.- Seguridad.- Toda base informática de datos debe contar con su respectivo archivo de respaldo, cumplir con los estándares técnicos y plan de contingencia que impidan la caída del sistema, robo de datos, modificación o cualquier otra circunstancia que pueda afectar la información pública." (LSNRDP, art. 26)

Así pues, el principio de seguridad impone al responsable de tratamiento obligaciones de medios, lo que exige la adopción de medidas de seguridad distintas de acuerdo al tipo de datos que trate. Pero para la adopción de dichas medidas es preciso, en el caso ecuatoriano, crear una autoridad de protección de datos personales con capacidades regulatorias que pueda emitir normativa vinculante en aspectos de protección de datos personales.

2.2.3.1.6 Derechos y deberes que configuran el derecho a la protección de datos personales

Como se expuso en líneas anteriores, al ser el derecho a la protección de datos personales un derecho complejo, este se configura a través de la mixtura de distintos derechos de los titulares de la información, así como de deberes que se les imponen a los responsables del tratamiento de dichos datos.

2.2.3.1.6.1 El derecho a la autodeterminación informativa

Para complementar la definición amplia desarrollada en párrafos previos relativa al derecho de autodeterminación informativa, parafraseamos el criterio de Davara (2008, p. 72), quien considera que este derecho reconoce a la persona su facultad de decidir solo sobre la difusión de la información que a ella respecta. El derecho a la autodeterminación informativa puede ejercitarse de varias formas: una es la facultad de oposición que tiene el titular, fundado en motivos legítimos, a que sus datos sean objeto de tratamiento, siendo esta una

manifestación muy clara de autodeterminación de sus datos frente al manejo abusivo de estos. (Sánchez, 1998, p. 97). Dicha potestad de oposición del titular deberá ser previa la recogida y el tratamiento de los datos de carácter personal. (López-Vidriero y Santos, 2005, pp. 92-93), puesto que las facultades de oposición posteriores al tratamiento constituirán otros derechos que serán tratados en líneas posteriores.

Por otro lado, el consentimiento del titular, a nuestro criterio, por constituir un elemento indispensable que justifica el tratamiento de sus datos, es otra clara expresión del derecho a la autodeterminación informativa, es decir, aunque muchos lo traten como un principio de tratamiento de datos de carácter personal, en la práctica, este efectiviza el derecho a la autodeterminación informativa.

2.2.3.1.6.2 El deber de información

Este deber a cargo de los responsables de tratamiento constituye la condición previa para la aplicación de los demás derechos que configuran el derecho a la protección de datos personales. Para que el resto de derechos sean aplicados, será preciso que el titular de los datos tenga información previa a cerca del proceso de recogida y posterior tratamiento de sus datos; lo que va de la mano con la existencia de un consentimiento informado, conforme a lo tratado en líneas previas.

La información que el responsable de tratamiento está obligado brindar al titular de los datos, se refiere, por un lado, a la existencia del fichero y ubicación de su responsable; y, por otro, a los derechos que amparan al titular de los datos. (AGDP, 2013, pp. 7-9). Con esta información previa se pretende que el afectado de forma reflexiva consienta o no el tratamiento de sus datos personales, y en caso de que dicho consentimiento se haya dado sobre la base de información inexacta o engañosa, este viciaría de nulidad. (Véase Vizcaíno, 2001)

Se considera que el deber de información transparenta el procedimiento de tratamiento de datos personales, imponiendo a los dueños de los ficheros la

obligación de dar publicidad de sus procesos y de inscribirse en un registro público de ficheros para uniformar sus procedimientos y asegurar la publicidad y transparencia de éstos.

En el inciso primero del artículo 92 de la Constitución de la República del Ecuador se reconoce a toda persona el derecho de "conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos", manifestación que concuerda con la establecida en el artículo 49 de la Ley de Garantías Jurisdiccionales y Control Constitucional. Declaración que, a nuestro criterio, brinda la pauta para crear formalmente el deber de la información a los responsables de tratamiento que configura, junto a otros derechos y principios, el derecho a la protección de datos personales.

2.2.3.1.6.3 El derecho de indemnización

Este derecho implica la indemnización del daño o lesión en los bienes o derechos que sea inferida al titular de los datos debido a un tratamiento abusivo de estos, es decir, por haberse violentado su derecho a la protección de datos de carácter personal por parte del responsable o encargado del tratamiento. Además Freixas señala que incluso en aquellos casos en que el incumplimiento sea generado por una tercera persona, el afectado podrá ejercer su derecho a la indemnización. (2001, pp. 198.199). Para el ejercicio de este derecho será preciso distinguir entre fichero público y privado:

- Ficheros públicos.- En este caso será preciso probar que existió incumplimiento debido al funcionamiento normal o anormal de los servicios públicos, salvo cuestiones de fuerza mayor. (Guerrero, 2006, pp. 308-310). Estos casos deberán ser observados con detenimiento de acuerdo a las circunstancias específicas que se presenten.

- Ficheros privados.- Regirá en estos casos la responsabilidad civil, a nuestro criterio aplicando inversión de carga de la prueba, debido a la dificultad que

implicaría para el afectado probar negligencia del responsable o encargado del tratamiento.

El derecho a la indemnización está comprendido en la “reparación integral” a la que se refiere el inciso final del artículo 49 de la Ley de Garantías Jurisdiccionales y Control Constitucional. Es por esta razón que consideramos a éste como uno de los derechos que necesariamente deberán integrarse y ser reconocidos ampliamente en una normativa de protección de datos personales.

2.2.3.1.6.4 Los derechos ARCO

Con el ejercicio de estos derechos los titulares de los datos son facultados para ejercer varias garantías que han construido al derecho a la protección de datos personales. (Santos, 2005, p. 91). Para Freixas estos derechos constituyen la piedra angular de las garantías que se ofrecen a los ciudadanos, (2001, p. 186), el autor también resalta en su texto la importancia del derecho de acceso, ya que, por medio de este, se podrán ejercitar otros como el de rectificación o cancelación.

Para que los titulares de los datos puedan ejercer estos derechos deberán poner observancia a los siguientes aspectos:

- Por ser personalísimos, su ejercicio es exclusivo de su titular, o de un representante debidamente acreditado.

- Estos derechos son independientes entre sí, no es preciso ejercitar uno como requisito para el ejercicio de otro.

- Estos derechos deben ser dirigidos inicialmente frente a los responsables de los ficheros, quienes deberán atender a dicha solicitud de forma gratuita.

Para el debido ejercicio de estos derechos será preciso que la normativa de protección de datos personales implemente un ente público autónomo e

independiente, que vele por la protección de los derechos de sus ciudadanos, difundiéndola y ofreciendo mecanismos administrativos de garantía para aquellos casos en que los responsables de ficheros se nieguen a cumplir con sus obligaciones. (AGDP, 2013, pp. 22-23)

Es importante mencionar que la normativa ecuatoriana en los artículos 66 numeral 19 y 92 de la Constitución de la República, y en el artículo 49 y 50 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional hace alusión a estos derechos. Es por esto que consideramos imprescindible adoptar en la legislación ecuatoriana una Ley de protección de datos personales que reconozca formalmente todos los derechos ARCO, basándose los Estándares Internacionales sobre Protección de Datos Personales y Privacidad difundidos por la Red Internacional de Protección de Datos, foro del que Ecuador es país miembro. Cabe señalar que dichos estándares están basados en los criterios adoptados por el modelo europeo de protección de datos personales, por lo mismo, también se observarán estos segundos.

a) El derecho de acceso.-

Este derecho se deberá ejercitar en aquellos casos en que el afectado desee saber con exactitud los datos personales que un responsable de fichero posee del mismo, de dónde fueron recabados y si han sido comunicados a más personas. (López-Vidriero y Santos, 2005, p. 89). A través del ejercicio de este derecho, el titular de los datos podrá tener conocimiento de aquellos que están siendo tratados, su origen, las finalidades de su tratamiento y almacenamiento, sus cesionarios, y los datos resultantes de dicho tratamiento.

Para el amparo de este derecho se debe poner observancia a los siguientes aspectos (AGDP, 2013, p. 24):

- El tiempo para ejercitarlo debe contemplar intervalos específicos de tiempo, con lo cual se garantizará que no existan peticiones excesivas; para estos

casos existirán excepciones en para casos en que se acredite un interés legítimo para el efecto.

- Igualmente, debe establecerse un tiempo máximo para que los responsables del fichero den respuesta a la petición del titular de los datos.

El artículo 66 numeral 19 de la Constitución de la República y el inciso tercero del artículo 92 se refiere a este derecho al manifestar lo siguiente:

> "Art. 66.- 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección […].
>
> Art. 92.- […] La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación […]" (Constitución, arts. 66 y 92)

También el numeral 1 del artículo 50 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional detalla uno de los casos en los que será factible la interposición de la acción de hábeas data, señalando lo que sigue:

"Art. 50.- 1. Cuando se niega el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que consten en entidades públicas o estén en poder de personas naturales o jurídicas privadas […]" (LOGJCC, art. 50)

El reconocimiento del derecho de acceso es ampliamente acogido en la legislación internacional, incluso la normativa ecuatoriana hace alusión a este expresamente en varios apartados. De igual forma, los Estándares Internacionales sobre Protección de Personales y Privacidad difundidos por la Red Internacional de Protección de Datos. (Véase CIAPDP, 2009, p. 19), hacen referencia al derecho de acceso de forma general y deberá observarse los mismos.

Será entonces preciso que en el desarrollo de normativa especial de protección de datos personales en Ecuador, se consideren criterios recogidos en otras legislaciones como los intervalos de tiempo para su ejercicio, o el tiempo máximo que tiene los responsables de tratamiento para tramitar solicitudes de los titulares de los datos personales. Con la finalidad de que el derecho de acceso al que hace mención la normativa ecuatoriana sea desarrollado más a fondo para un óptimo amparo al derecho a la protección de datos personales.

b) El derecho de rectificación.-

El afectado ejercerá su derecho a rectificación cuando desee que sus datos sean modificados por el responsable del fichero. (López-Vidriero y Santos, 2005, p. 91). Éste derecho tiene el objeto de garantizar la veracidad de la información objeto de tratamiento, permitiendo corregir errores o modificar los datos inexactos o incompletos.

- Para resolver sobre la solicitud de rectificación o cancelación, el responsable de tratamiento deberá tener un tiempo máximo establecido, a partir de la recepción de la solicitud, para atenderla.

- De darse el caso de que los datos rectificados fueron cedidos a terceros previamente, el responsable del fichero deberá comunicar la rectificación efectuada al cesionario, para que este, en un tiempo determinado realice la modificación pertinente. (AGDP, 2013, p. 25)

El artículo 66 numeral 19 de la Constitución de la República y el inciso tercero del artículo 92 se refieren al derecho de rectificación de la siguiente forma:

> "Art. 66.- 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección […]

> Art 92.- […] La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación […]" (Constitución, arts. 66 y 92)

También el numeral 1 del artículo 50 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional detalla uno de los casos en los que será factible la interposición de la acción de hábeas data, señalando lo que sigue:

"Art. 50.- […] 2. Cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos […]" (LOGJCC, art. 50)

En el texto de los Estándares Internacionales sobre Protección de Personales y Privacidad difundidos por la Red Internacional de Protección de Datos, (véase CIAPDP, 2009, p. 19), se hace referencia al derecho de rectificación de forma general. Así, resulta factible desarrollar más a fondo, y por lo tanto, brindar un amplio reconocimiento al derecho de rectificación en la legislación ecuatoriana. Éste derecho deberá reconocerse poniendo observancia a patrones brindados en la legislación comparada como la europea, para sí establecer tiempos máximos para su atención y obligaciones para el responsable del tratamiento que efectivicen su óptima tutela.

c) <u>El derecho de cancelación</u>.-

Por medio de éste derecho el titular de los datos se encontrará facultado a que se bloqueen y posteriormente sean suprimidos los datos que resulten ser inadecuados o excesivos relativos a su persona. La cancelación no debe ser definida como sinónimo de destrucción, sino como retirada de los datos del conocimiento del público general, para que accedan únicamente a estos los órganos administrativos con el fin de determinar responsabilidades en el tratamiento. Estos datos serán eliminados únicamente luego de cumplido el plazo de prescripción. (Freixas, 2001, p. 196). Al ejercer este derecho se

realizará un bloqueo de los datos, con la finalidad de impedir su tratamiento, con sus respectivas excepciones legales.

- Para salvaguardar este derecho, la normativa deberá obligar al responsable del fichero a atender las solicitudes de los titulares de datos respecto al ejercicio de este derecho, en un tiempo determinado contado a partir de la fecha de presentación de la respectiva solicitud.

- En aquellos casos que los datos cancelados hubieran sido cedidos previamente, será importante que la normativa contemple la obligación del responsable del fichero de comunicar al cancelación efectuada al cesionario, de esta forma los datos erróneos no seguirán siendo tratados en perjuicio de su titular por terceros a quienes les fueron cedidos. (AGDP, 2013, p. 26)

Ciñéndonos a los mismos preceptos contemplados en la legislación ecuatoriana, previamente desarrollados para el caso derecho de rectificación, consideramos que aunque nuestra normativa no mencione al derecho de cancelación como tal, será preciso que este sea desarrollado y reconocido cabalmente; imponiendo obligaciones para el responsable del fichero, que activen un derecho a la protección de datos personales complejo e instrumental del que se ha venido hablando en párrafos previos.

d) El derecho de oposición.-

A este derecho es complejo definirlo debido a que se lo podría confundir con el derecho a la cancelación, o con la manifestación de oposición del derecho a la autodeterminación informativa. Por un lado, el derecho a la oposición se distingue del de cancelación debido a que no da a su titular la facultad de pedir el bloqueo y posterior borrado de sus datos; éste únicamente tendrá la potestad de oponerse al tratamiento que se realiza de sus datos, y esta oposición deberá estar fundamentada en motivos suficientes y apegados a los que contemple la Ley.

Tampoco se puede confundir este derecho con la oposición que efectiviza el derecho a la autodeterminación informativa, para lo que citamos a la autora Serrano “No se trata de garantizar el derecho a la oposición a todo interesado, como una manifestación de la autodeterminación personal […]” (2003, pp. 370-371). El derecho a la oposición se traduce en la acción del interesado frente al tratamiento de sus datos que ya se está realizando, y solo se ejercitará en motivos legítimos que justifiquen la razón por la cual el titular de los datos no quiere que su información sea tratada, o que esta no sea utilizada para ciertos tipos de tratamiento. Este derecho procederá cuando concurran tres supuestos:

- Las decisiones tomadas por los responsables de los ficheros respecto al tratamiento de sus datos personales deben ser perjudiciales para el titular de dichos datos, trayendo consecuencias que le permitan oponerse a tal decisión.

- Las decisiones tomadas por los responsables de los ficheros deberán estar referidas exclusivamente al tratamiento automatizado de datos.

- El tratamiento automatizado de los datos debe atribuir variables que permitan configurar un perfil de personalidad del titular de los datos o afectado.

El derecho a la oposición también se contempla en el texto de los Estándares Internacionales sobre Protección de Personales y Privacidad difundidos por la Red Internacional de Protección de Datos, (véase CIAPDP, 2009, pp. 20-22), lo que da una pauta más para su futuro reconocimiento formal en el país.

Como se evidencia, el derecho a la oposición es novedoso y por ende la normativa ecuatoriana por el momento no lo menciona específicamente. Sin embargo las particularidades de éste derecho deberían ser consideradas por el legislador ecuatoriano durante el desarrollo de normativa que permita un

reconocimiento y tutela óptima de un derecho a la protección de datos personales complejo e instrumental.

2.3 Conclusiones previas

El tema de análisis en el presente trabajo es la protección de datos personales en el *cloud computing* analizada desde la relación B2C que se genera entre los usuarios ecuatorianos y los proveedores de servicios de cómputo en la nube. Una vez que en el capítulo primero se definió al modelo de prestación de servicios que constituye el *cloud computing*, el capítulo segundo plantea un marco teórico preventivo del derecho a la protección de datos personales y su aplicabilidad en la legislación ecuatoriana. Posteriormente, en el capítulo tercero, se contrastará el contenido de los capítulos primero y segundo para proponer la implementación de normativa de protección de datos personales en la legislación ecuatoriana, que acoja los principios del derecho a la protección de datos personales que generen un sistema preventivo que ampare a los ecuatorianos frente a los riesgos que pueden generar las relaciones B2C por el uso de servicios de cómputo en la nube.

El capítulo segundo tuvo la finalidad de brindar estándares adaptables a la normativa ecuatoriana, que haciendo énfasis en la implementación de sus principios, configuren un sistema preventivo amparando así un derecho a la protección de datos personales compuesto, específico e instrumental, amparado actualmente por vía constitucional.

Con dichos criterios y conceptos, se ha obtenido un marco teórico que pone en manifiesto los principios del derecho a la protección de datos personales que, a criterio de la autora, deberán implementarse en la legislación ecuatoriana para resguardar del derecho a la protección de datos personales de los ecuatorianos en relaciones B2C generadas por el uso de servicios de cómputo en la nube.

A continuación será estudiado el caso de la relación B2C generada por la prestación de servicios de *cloud computing* a partir de las políticas de privacidad

de Dropbox, y sus particularidades respecto al tratamiento de datos de *e-consumers* ecuatorianos. Para que, los retos y riesgos que éste servicio despliega sean considerados para el desarrollo de normativa específica de protección de datos de carácter personal para Ecuador que acoja los principios estándares del derecho a la protección de datos personales ya expuestos.

3 EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL ECUATORIANO ANALIZADO A PARTIR DE LA RELACIÓN B2C EN LA PRESTACIÓN DE SERVICIOS DE *CLOUD COMPUTING*

3.1 Análisis introductorio

Como se ha manifestado en el capítulo primero, la nube de cómputo es un modelo de prestación de servicios TIC que se encuentra en desarrollo a nivel mundial, y su uso cada día es más amplio. Los servicios de *cloud computing* también son utilizados por ecuatorianos, es más hoy en día muchos somos usuarios de "la nube" sin siquiera haberlo notado.

La nube trae consigo un sin número de cuestionamientos y retos en distintas áreas del derecho, sin embargo, el propósito de este trabajo es centrarse en la problemática detectada en lo que se refiere al derecho a la protección de datos personales de los ecuatorianos, específicamente para aquellos casos en que se forjan relaciones B2C por el uso de servicios de cómputo en la nube.

A continuación, el presente capítulo empatará los capítulos anteriormente desarrollados, teniendo en cuenta las siguientes pautas generales:

Inicialmente se analizarán las particularidades que se generan en la relación B2C, por la prestación de servicios de *cloud computing,* donde se realizará una breve referencia a los roles de los actores de esta relación en el caso del *cloud computing* y de las políticas de privacidad estipuladas por los proveedores de servicios de cómputo en la nube que son contratos de adhesión para la normativa del consumidor ecuatoriana.

Posteriormente, haciendo referencia a lo estudiado en el capítulo segundo, se describirán los principios estándar de protección de datos personales a partir de la relación B2C por la prestación de servicios de *cloud computing*. Donde se hará referencia a las distintas funciones que desempeñe el proveedor de

servicios de acuerdo a las fases del ciclo de vida de los datos en el *cloud computing,* con lo que se podrá identificar los riesgos que genera el no desarrollo de un sistema preventivo de protección de datos personales.

Para una adecuada comprensión del derecho a la protección de datos personales en este paradigma tecnológico, se realizará un análisis de la relación B2C generada por la prestación servicios de Dropbox, a partir de sus políticas de privacidad. Para este análisis se estudiará el contenido de las políticas de privacidad que estipula Dropbox a sus usuarios, dicho análisis se basará en los principios estándar que generan un sistema preventivo del derecho a la protección de datos personales, y conectará el contenido de sus cláusulas con las fases del ciclo de vida del *cloud computing,* para así vislumbrar las distintas funciones que pueden realizar los proveedores de servicios de cómputo en la nube y los posibles riegos que genera el no reconocimiento expreso de los principios del derecho a la protección de datos personales.

A partir de la identificación de estos riesgos, se divisarán las políticas de privacidad de Dropbox que deberían revisarse por este prestador de servicio de *cloud computing,* para que así demostrar al lector la importancia de implementar en Ecuador principios estándar que generen un sistema preventivo de protección de datos personales.

Finalmente, el desarrollo de este trabajo de investigación permitirá esbozar una propuesta normativa que permita regular el derecho a la protección de datos personales aplicable a las particularidades generadas por el uso de servicios de *cloud computing* en relaciones B2C.

3.2 La relación B2C en la prestación de servicios de *cloud computing* en Ecuador

La relación B2C en contratación electrónica se refiere a un tipo de *e-business* por el que el empresario, a través de internet, brinda sus productos y/o servicios a consumidores de a pie (no empresariales), es decir existe una relación de

contratación directa. (Confederación de Empresarios de Andalucía, 2014, p. 2). En la prestación de servicios de *cloud computing* nos referimos a relación B2C cuando el usuario es el consumidor promedio que accede a servicios de cómputo en la nube, para su uso personal y sin interés empresarial alguno.

El *cloud computing* es inmenso, y debido a esto pueden presentarse variadas relaciones que den roles distintos a cada actor. Esta investigación se centra en analizar específicamente la relación B2C que se genera por la contratación directa de servicios de cómputo en la nube, tipo de contratación en la que también toma relevancia la normativa de defensa al consumidor.

También es importante considerar que, en las relaciones B2C por contratación electrónica de servicios *cloud computing,* las políticas de privacidad a las que los ecuatorianos se adhieren son contratos electrónicos de adhesión, y en el Ecuador existe normativa que establece ciertos parámetros para que sus cláusulas no violenten los derechos de los consumidores. Con la finalidad de contextualizar jurídicamente al lector respecto al foco del análisis de este trabajo, relativo a la relación B2C generada por la prestación de servicios de *cloud computing,* en el presente trabajo también se ha considerado necesario hacer alusión a cierta normativa de *e-consummers* ecuatorianos como la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos y la Ley Orgánica de Defensa al Consumidor.

Aunque el tema nuclear de análisis del presente trabajo es la relación B2C en la prestación de servicios de *cloud computing,* hay que recordar que también hay muchos contratos B2B (*bussiness to bussiness*) en la nube y en aquellos casos también debe ampararse el derecho a la protección de datos personales de los usuarios. Es imperioso mencionar que la normativa de *e-consummers,* citada en este trabajo, solo aplica para casos de relaciones B2C generadas por contratación de servicios de cómputo en la nube, pero no aplicará para las relaciones B2B, que son incluso más comunes en la contratación de servicios de *cloud computing*.

Por lo mencionado, aunque se utilicen como referencia ciertas disposiciones de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos y la Ley Orgánica de Defensa al Consumidor, el contenido de estas resulta insuficiente para amparar un derecho amplio y complejo, como lo es el de protección de datos personales en la inmensidad de casos (como el de Dropbox, estudiado en la presente investigación), que pueden generarse por el uso de datos personales que se gestiona en los servicios de *cloud computing.*

3.2.1 Actores de la relación B2C en la prestación de servicios de *cloud computing* en Ecuador

Como se definió en el capítulo primero, el proveedor de servicios de cómputo en la nube, en la órbita del derecho a la protección de datos personales podrá ser, de acuerdo al caso, responsable de tratamiento o encargado de tratamiento. (Grupo del artículo 29 sobre protección de datos, 2010; CSA, 2011)

a) Responsable de tratamiento: De acuerdo a la relación directa B2C que se analiza en el presente estudio, en la que el proveedor contrata directamente con el usuario ecuatoriano, brindándole así servicios en la nube. Para la aplicación de normativa de protección de datos personales el proveedor de servicios de *cloud computing* será considerado responsable de tratamiento.

   En el caso de las políticas de privacidad de Dropbox, el responsable de tratamiento es Dropbox, y por ende, es este quien debe cumplir con las obligaciones que impone el derecho a la protección de datos personales.

b) Encargado de tratamiento: En casos de relaciones B2C, los encargados serán subcontratistas del proveedor de servicios. Los encargados actuarán bajo las directrices del responsable de tratamientos, las mismas que estarán definidas en un acuerdo de prestación de servicios firmado entre estos.

   Para el caso de Dropbox, los encargados serán sus subcontratistas a los que se refiere en su política de privacidad como “otros que trabajan para Dropbox”.

Por otro lado, el usuario de servicios de *cloud computing* de acuerdo a lo expresado en el capítulo primero, para la aplicación de normativa de protección de datos personales, podrá ser el suscriptor o el interesado. (CRID, 2010, p. 11). Para el caso de relaciones B2C, conforme al presente análisis el usuario o consumidor ecuatoriano, por ser quien suscribe el contrato para la prestación de servicios de cómputo en la nube y también el titular de los datos personales, será tanto el suscriptor como el interesado, es decir no existirá diferencia entre ambos.

Para identificar al consumidor será preciso entender a éste como aquella persona que adquiere bienes y servicios, sin intención de obtener una ganancia, para su posterior comercialización; el consumidor no extiende el proceso de producción (Sarango, 2013), como si sucede con el proveedor.

Asimismo, en Ecuador se consideran consumidores a las personas que estén inmersas en la definición del artículo 2 de la Ley Orgánica de Defensa al Consumidor:

"Consumidor.- Toda persona natural o jurídica que como destinatario final, adquiera, utilice o disfrute bienes o servicios, o bien reciba oferta para ello. Cuando la presente Ley mencione al consumidor, dicha denominación incluirá al usuario." (LODC, Art. 2)

Entonces, para la relación B2C que se analiza en el presente trabajo el consumidor podrá ser tanto una persona natural como jurídica, según la normativa de defensa al consumidor ecuatoriana.

Podemos evidenciar que los roles que cumple cada actor en la relación B2C, materia de análisis de esta investigación, son distintos a los que podrían generarse en otro tipo de contrataciones de servicios de cómputo en la nube como B2B (*Business to Business),* en las que la normativa de defensa al consumidor no sería aplicable por tratarse de contrataciones entre empresas.

Debido a que tema de este trabajo de titulación se centra únicamente en aquellas relaciones B2C generadas por la contratación de servicios de *cloud computing,* en este análisis se observa y aplica normativa de defensa al consumidor en el ámbito ecuatoriano. Sin embargo, también resaltamos la necesidad de que se desarrollen a futuro investigaciones centradas en la relación B2B por la prestación de servicios de *cloud computing* y las implicancias que esta puede tener en el derecho a la protección de datos personales de los ecuatorianos.

3.2.2 Contratos electrónicos de adhesión (*click wrap)* generados por la relación B2C en la prestación de servicios de *cloud computing* en Ecuador

La contratación electrónica por medio de contratos de adhesión (también conocidos como *click wrap* en el sistema anglosajón), es un tema bastante amplio que amerita un trabajo de investigación específico para desarrollarlo. Sin embargo, debido a que la relación B2C en la prestación de servicios de *cloud computing* que se analiza en esta investigación se genera por la contratación por medio de contratos electrónicos de adhesión, hemos considerado necesario hacer una breve referencia al tema para mayor entendimiento del lector.

Para Acuña y Cordero (2014, p. 102) “en los contratos de adhesión, las condiciones se encuentran establecidas con anterioridad por el empresario y al consumidor no le queda más que aceptar o no los términos del contrato”. Estos autores explican que dentro de la contratación electrónica es muy común que se utilicen contratos de adhesión como los *click wraps*, pues para el proveedor es más fácil que sus términos y condiciones sean generalizados y de fácil acceso para sus usuarios. Además estas figuras permiten al proveedor de los servicios a preestablecer una propuesta, para que el usuario se limite a aceptarla o rechazarla sin más.

Siguiendo la línea de Acuña y Cordero, Rojas reflexiona sobre la necesidad de que estos contratos existan, pues para el empresario sería imposible negociar individualmente con cada uno de sus usuarios. (2013, pp. 277-278)

Los contratos *click wrap* son contratos de adhesión ya que sus cláusulas contienen términos y condiciones no negociables por el consumidor, con la particularidad de que se perfeccionan a través del consentimiento realizado medios electrónicos. (Véase Rojas, 2013)

El consentimiento en los contratos *click wrap* se manifiesta de forma expresa cuando el consumidor acepta los términos y condiciones de un contrato, dándole click al botón de "Acepto", "*Agree"* o "Estoy de acuerdo". (Rojas, 2013, p. 278) y (Acuña & Cordero, 2014, pp. 121-122). El consumidor manifiesta su consentimiento simplemente al pulsar un botón.

Con base a la teoría de los contratos de adhesión por medios electrónicos o *click wrap,* es importante tener en cuenta las disposiciones del ordenamiento jurídico ecuatoriano. En la presente investigación es importante tener en cuenta que a los proveedores de servicios de cómputo en la nube les rige la normativa vigente relativa a contratación electrónica y derechos de defensa del consumidor, misma que se encuentra recogida en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; y, en la Ley Orgánica de Defensa del Consumidor.

La normativa ecuatoriana, en el artículo 2 de la Ley Orgánica de Defensa al Consumidor, define al contrato de adhesión como aquel en el que las cláusulas se establecen unilateralmente por el proveedor. (LODC, Art. 2)

Igualmente, del texto de la Ley Orgánica de Defensa del Consumidor es importante que los proveedores de servicios de *cloud computing* en la elaboración de sus políticas de privacidad, tengan en cuenta lo establecido en los artículos 41 relativo a los contratos de adhesión, y el 43 referente a las cláusulas prohibidas en los contratos de adhesión.

Por otro lado, La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en su artículo 3 contempla la incorporación por remisión, método a

través del cual se instrumentaliza el consentimiento en la contratación electrónica, (LCEFEMD, art. 3), este es el método que introduce indirectamente los contratos electrónicos de adhesión o *click wrap* en el ordenamiento jurídico ecuatoriano. En los casos que usuarios ecuatorianos contraten servicios de *cloud computing* con proveedores de servicios de *cloud computing*, éstos expresarán su aceptación a través de un *click,* el que remitirá a términos y condiciones incorporados de forma directa al mensaje de datos.

Así mismo, el consentimiento que perfeccione los contratos electrónicos de adhesión o *click wrap* se sustenta en los requisitos y solemnidades previstas en la ley que rija en lo que fuere aplicable conforme a lo establecido en la normativa ecuatoriana en los artículos 44 y 46 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; y que en este tipo de contratos se remitiría al artículo 1459 del Código Civil.

Finalmente, en lo concerniente a la presente investigación, para que un proveedor de servicios de cómputo en la nube esté facultado a dar tratamiento de la información de sus usuarios será preciso que el usuario acepte a través de un *click* sus "políticas de privacidad". En estas políticas de privacidad los proveedores de servicios de cómputo en la nube estipulan cláusulas que los capacitan a recoger, almacenar, procesar, perfilar y archivar la información de sus usuarios instrumentalizándose en contratos electrónicos de adhesión o *click wrap*.

En las relaciones B2C por contratación de servicios de *cloud computing,* los contratos en que se estipulan políticas de privacidad son de adhesión o *click wrap*. Por lo que los proveedores de servicios de cómputo en la nube estipularán arbitrariamente las cláusulas de sus contratos. Si el usuario no está conforme con el contenido de las políticas de privacidad no las podrá negociar, y la única forma de que no se adhiera a las mismas sería no contratando los servicios de *cloud computing,* es decir, no dando *click* en el botón de "aceptar".

3.3 Descripción de los principios estándar del derecho a la protección de datos personales a partir de la relación B2C por la prestación de servicios de *cloud computing*

El presente apartado tomará de referencia a los principios estándar del derecho a la protección de datos personales presentados previamente en el capítulo segundo, los que serán descritos a partir de la relación B2C por la prestación de servicios de *cloud computing.*

Es importante recordar que los principios estándar que se describen a continuación generan un sistema preventivo de protección de datos personales, y por ende la falta de desarrollo expresa de estos en la legislación ecuatoriana está generando riesgos que deben observarse por el legislador para su debida prevención.

Con la finalidad de detectar los riesgos que genera para los ecuatorianos la contratación de servicios de *cloud computing* en relaciones B2C, a continuación se describen los principios estándar que configuran un sistema preventivo del derecho a la protección de datos personales, definidos en el capítulo segundo de este trabajo.

3.3.1 Principio de consentimiento informado

El consentimiento informado se refiere a una manifestación de voluntad del titular de los datos, realizada en base a la información previa que haya brindado el responsable de tratamiento. Este tipo de consentimiento ampara a los ecuatorianos en la relación B2C, y obliga a los proveedores de servicios de *cloud computing* a dar información previa al tratamiento de datos a sus usuarios.

El consentimiento informado constituye uno de los pilares que configuran un sistema preventivo de protección de datos personales, por lo que es elemental que el Estado intervenga para que los proveedores de servicios de *cloud computing* se cercioren de garantizarlo. Pero para que un proveedor de servicios

de *cloud computing* obtenga un consentimiento válido de sus usuarios ecuatorianos también deberá ceñirse a las disposiciones de legislación ecuatoriana relativas al consentimiento de *e-consumers,* la que enunciamos a continuación por ser relevante en el presente análisis, por su conexión con el consentimiento informado en materia de protección de datos personales.

La Ley Orgánica de Defensa del Consumidor en su artículo 4 numeral 4 reconoce a los usuarios el derecho especial de información, el que está estrechamente vinculado con el consentimiento informado. Este derecho para el caso de contratación electrónica se desarrolla en el artículo 50 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, el que se cita a continuación:

> Art. 50.- Información al consumidor.- En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento.
>
> Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados.
>
> La publicidad, promoción e información de servicios electrónicos, por redes electrónicas de información, incluida la Internet, se realizará de conformidad con la ley, y su incumplimiento será sancionado de acuerdo al ordenamiento jurídico vigente en el Ecuador.
>
> En la publicidad y promoción por redes electrónicas de información, incluida la Internet, se asegurará que el consumidor pueda acceder a toda la información disponible sobre un bien o servicio sin restricciones, en las mismas condiciones y con las facilidades disponibles para la promoción del bien o Servicio de que se trate.
>
> En el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o a través de listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos.
>
> La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se sancionará de acuerdo a lo dispuesto en la presente ley.

> El usuario de redes electrónicas, podrá optar o no por la recepción de mensajes de datos que, en forma periódica, sean enviados con la finalidad de informar sobre productos o servicios de cualquier tipo." (LCEFEMD, art. 50)

Los proveedores de servicios en la nube de cómputo, según el artículo 17 de la Ley Orgánica de Defensa del Consumidor, están obligados a dar cumplimiento al derecho de información de los usuarios ecuatorianos, de no ser así, se podría acarrear nulidad contractual por haberse viciado su consentimiento. El derecho especial a la información de los consumidores en materia de contratación electrónica, a nuestro criterio, debe ser observado por los proveedores de servicios de *cloud computing* al momento de estipular políticas de privacidad a usuarios ecuatorianos.

En el ámbito del derecho al consumidor en Ecuador se hace referencia al consentimiento informado, no existe normativa que esclarezca sus alcances para casos ligados a la órbita de la protección de datos personales. A la par de lo expuesto en el capítulo segundo, consideramos que hay la necesidad de implementar normativa de protección de datos personales que exija un consentimiento no solo expreso, sino también informado del interesado para que se realice específicamente el tratamiento de sus datos, en contexto con el desarrollo de la doctrina y legislación comparada.

Finalmente, a la par de lo expuesto, la necesidad de implementar normativa de protección de datos personales que ampare a los usuarios ecuatorianos de servicios de *cloud computing* con un consentimiento informado, se evidenciará en líneas posteriores en el análisis ejemplificativo del caso Dropbox. Únicamente con un óptimo reconocimiento del derecho a la protección de datos personales preventivo, las políticas de privacidad informarán previamente al usuario respecto de las razones por las cuales realizará el tratamiento de datos personales, explicando claramente todas las funciones que efectuará como responsable de tratamiento, es decir tanto de acceso, procesamiento y almacenamiento.

Este principio se activa en el ciclo de vida de los datos en el *cloud computing* cuando el proveedor vaya a realizar funciones de acceso, procesamiento y almacenamiento de datos, pues desde la estipulación de sus políticas de privacidad, deberá informar a cerca de todas las funciones que desempeñará mientras dure el tratamiento de datos personales.

Por lo enunciado, es evidente que en la normativa ecuatoriana es preciso definir a fondo y específicamente el consentimiento informado que debe brindar el titular de la información para que se genere un sistema preventivo de protección de datos personales. En la actualidad, tomando como ejemplo el caso de Dropbox, alrededor del mundo, ya hay más de cuatrocientos millones de usuarios, (Contreras, 2015), signatarios de las políticas de privacidad que este proveedor de servicios en la nube estipula; atendiendo al principio de consentimiento informado del derecho a la protección de datos personales, estos usuarios deberían haber brindado su consentimiento basados en información previa y suficiente del tratamiento que se realizará de su información.

3.3.2 Principio de finalidad

Conforme a lo establecido en el capítulo segundo, este principio obliga al responsable de tratamiento a indicar desde un inicio la finalidad de los ficheros, para verificar que los datos recolectados empaten con dicha finalidad. Así la información brindada por sus titulares para que sea tratada para determinados fines, no podrá utilizarse con otra finalidad que la específicamente establecida desde un inicio.

Como se puede observar, el principio de finalidad tiene relevancia en todas las actuaciones que realice a lo largo del tratamiento el responsable. Es por esto que en el presente análisis, el proveedor de servicios de *cloud computing* deberá cumplir con este principio siempre que efectúe funciones de acceso, procesamiento y almacenamiento de información.

Es elemental señalar que el principio de finalidad es el pilar fundamental para generar un sistema preventivo de protección de datos personales y además es la base de todos los principios estándar expuestos en el capítulo segundo de este trabajo. Es a partir de la información inicial que brinda el proveedor de servicios de *cloud computing* acerca de la finalidad del tratamiento, que éste podrá ceñir posteriormente la realización de sus operaciones conforme a los principios de lealtad y licitud, calidad o exactitud, no utilización abusiva y conservación limitada de los datos.

Debido a que cada tres de cuatro personas encargadas de tomar decisiones utilizan servicios de *cloud computing* para sus negocios, (QuoteColo, 2015), es evidente que una inmensa cantidad de información recogida de la nube se provee a compañías para su toma de decisiones. Si en Ecuador se implementa una Ley de Protección de Datos Personales en la que se detalle el contenido y los alcances del principio de finalidad, los proveedores de servicios de cómputo en la nube deberían actuar conforme a este principio en la misma redacción de sus políticas de privacidad. Lo que llevaría a activar en Ecuador un sistema preventivo de protección de datos personales y a evitar que los usuarios de estos servicios desconozcan de las finalidades del tratamiento de sus datos.

3.3.3 Principio de lealtad y licitud

Para que el responsable de tratamiento cumpla con este principio, debe necesariamente haber cumplido con el principio de finalidad, así el titular de los datos, por un lado, conocerá *a priori* la finalidad del tratamiento de sus datos; y, posteriormente, podrá constatar que el tratamiento es realizado de forma leal y lícita.

En lo que a este principio respecta, la lealtad se refiere a las circunstancias en que se han recogido los datos, que las finalidades de su recogida y tratamiento sean legítimas, y la pertinencia de la información frente a la finalidad de su recolección.

El responsable de tratamiento deberá cumplir con las obligaciones que le impone este principio mientras se encuentre se desarrollando operaciones como actualización o utilización de datos, las que se enmarcan en la función de procesamiento de la información. Únicamente en esa función se podrá constatar que el mismo ha cumplido con la finalidad establecida al inicio del tratamiento de datos personales.

La mayor cantidad de datos que se almacenan en la nube son contactos, música, fotografías, emails, calendarios, búsquedas, entre otros, (Eclipse, 2015); esto combinado con el considerable crecimiento del *cloud computing* en los últimos años evidencia la necesidad de que se active un sistema preventivo de protección de datos personales en Ecuador. Este sistema se generaría con una Ley de Protección de Datos Personales, que exija al proveedor de servicios de *cloud computing* a cumplir con el principio de lealtad y licitud a partir de la misma la redacción de sus políticas de privacidad y en el desarrollo de sus actividades de tratamiento de información.

3.3.4 Principio de calidad o exactitud

De lo expuesto en el capítulo segundo del presente trabajo, este principio entabla la obligación del responsable de tratamiento de que los datos recogidos sean pertinentes, no excesivos, exactos y actualizados respecto a los fines para los que se recogieron.

El principio de calidad o exactitud está destinado a ser observado por el proveedor de servicios de cómputo en la nube, cuando este realice operaciones de acceso, transferencia, intercambio, actualización, orden o utilización de los datos de sus usuarios. Debido a que estas operaciones entrañan a las funciones de procesamiento y almacenamiento de información, definidas en el capítulo primero de este trabajo, este principio garantiza al titular de los datos que su información no será tergiversada y se utilizará sin alteraciones en el ejercicio de dichas funciones.

Considerando que los expertos en informática creen que el mayor riesgo de la nube se debe a que la información puede estar expuesta al acceso de terceros, (V3, 2015); con una Ley de Protección de Datos Personales en la legislación ecuatoriana, se obligaría al proveedor de servicios de *cloud computing* a observar el principio de calidad y exactitud a partir de la redacción de sus políticas de privacidad y en el desarrollo de todas sus actividades de tratamiento de datos. Con lo que se activaría un sistema preventivo de protección de datos personales que prevenga la exposición de la información a terceros no facultados por su titular para el tratamiento de datos personales.

3.3.5 Principio de conservación limitada de los datos

En el capítulo segundo ya se hizo referencia a la importancia que tiene este principio y su conexión con el principio de finalidad. Para que el titular de los datos sepa que su información será tratada por un lapso de tiempo y no lo perfilarán para siempre, a través de este principio se impone al responsable de tratamiento la obligación de no mantener eternamente la información de sus usuarios.

Este principio deberá cumplirse por el responsable de tratamiento de datos cuando el mismo implemente medidas de disociación o destrucción de los datos, estas operaciones se efectúan en la función de acceso a los datos, según lo establecido en el ciclo de vida de los datos en el capítulo primero de este trabajo.

Los proveedores de servicios de hosting en la nube año 2015 aproximadamente almacenan ocho zettabytes de contenido digital, (Bluzebra Technologies, s.f.), si suponemos que ese contenido al año 2020 posiblemente se duplicará, es evidente que los datos solo deberán conservarse archivados por un tiempo prudencial. El proveedor de servicios de *cloud computing,* con una Ley de Protección de Datos Personales, estaría obligado a observar el principio de conservación limitada de los datos en la redacción de sus políticas de privacidad, con lo que la información no estaría almacenada eternamente en la nube y

también esto contribuiría para que en Ecuador se desarrolle un sistema preventivo de protección de datos personales.

3.3.6 Principio de no utilización abusiva

En el capítulo segundo de este trabajo se define al principio de utilización no abusiva, el que obliga a que los responsables de los ficheros aseguren una coherencia lógica entre los presupuestos y resultados del procedimiento de tratamiento de los datos personales. Esto se logra cuando la finalidad establecida para la recogida, el uso de los datos, y los procedimientos empleados durante el tratamiento de éstos, son compatibles con los informados inicialmente en las políticas de privacidad a los usuarios.

El principio de utilización no abusiva es el resultado de la observancia preventiva de principios como el de finalidad o el de licitud en el procedimiento de tratamiento de datos. Este principio entonces deberá observarse mientras el responsable de tratamiento actualiza, ordena o utiliza en su negocio la información de sus usuarios, es decir, mientras cumple la función de procesamiento de datos según lo descrito en el capítulo primero de este trabajo.

Según encuestas, el 95% de personas diariamente utiliza algún servicio de *cloud computing,* (Bluzebra Technologies, s.f.), habrá que imaginar entonces lo que representaría para estos usuarios que toda su información no sea tratada conforme al principio de utilización no abusiva. Con una Ley de Protección de Datos Personales en la legislación ecuatoriana, se obligaría al proveedor de servicios de *cloud computing* a cumplir con este principio que, junto a otros elementos, generaría un sistema preventivo de protección de datos personales en el país.

3.3.7 Principio de seguridad

Conforme a lo expuesto en el capítulo segundo, el principio de seguridad impone al responsable de tratamiento obligaciones de medios, lo que exige que adopte

distintas medidas de seguridad durante todas las operaciones que realice en el tratamiento de los datos de sus usuarios. Estas medidas serán implementadas con el fin de que, a lo largo de procedimiento de tratamiento de datos personales, se garantice la integridad, disponibilidad y confidencialidad de la información de sus usuarios.

El principio de seguridad tiene relación directa con todas las operaciones que realice el proveedor de servicios de cómputo en la nube, durante el ciclo de vida de los datos definido en el capítulo primero de este trabajo. Por lo dicho, este principio tendrá relevancia en las funciones de acceso, procesamiento y almacenamiento de la información.

En la actualidad documentos, datos, carpetas, información de consumidores, cada día circula directamente a aplicaciones en la nube (SaaS) sin pasar por los protocolos de seguridad empresariales. (Ciphercloud, 2013). Además los proveedores de servicios de *cloud computing* al año 2013 invirtieron 150 billones de dólares en el desarrollo de este paradigma. (Bluzebra Technologies, s.f.). Es importante que con una Ley de Protección de Datos Personales, se obligue a que, en observancia al principio de seguridad, estos proveedores inviertan en la implementación de medidas de seguridad de distintos niveles. Estas medidas de seguridad deberán ser estipuladas en sus políticas de privacidad de acuerdo a los distintos niveles de seguridad que manejen.

Será la autoridad de protección de datos personales que, en su momento se instituya con la implementación de una Ley de Protección de Datos Personales, quien establezca dichos niveles de seguridad de acuerdo al tipo de datos que recojan (inocuos, sensibles, etc.) y procesen los proveedores de servicios de *cloud computing*.

3.4 Análisis de la relación B2C por la prestación de servicios de *cloud computing* en Ecuador*:* caso de las políticas de privacidad de Dropbox

Enfatizamos que este trabajo intenta dar a conocer al lector la importancia de que se resguarde de forma preventiva el derecho a la protección de datos de los ecuatorianos. La única forma de prevenir posibles violaciones al derecho a la protección de datos personales en relaciones B2C, se da cuando un proveedor de servicios de *cloud computing* estipula las cláusulas en sus políticas de privacidad, que se acogen a los distintos principios estándar que forman parte constitutiva del derecho a la protección de datos personales.

Este análisis servirá de sustento para poder detectar y ejemplificar los riesgos que se generan por el no cumplimiento de responsabilidades que tiene el proveedor de servicios de *cloud computing,* desde la estipulación de sus políticas de privacidad. Dichas responsabilidades serán consideradas a partir a los principios estándar del derecho a la protección de datos personales expuestos en el capítulo segundo de este trabajo, y serán asignadas acorde al ciclo de vida de los datos en el *cloud computing* expuesto en el capítulo primero de esta investigación.

Para hacer ver al lector que en Ecuador actualmente no se está previniendo posibles violaciones a su derecho a la protección de datos personales, y con la finalidad exclusiva de ilustrar pragmáticamente las pautas que rigen en la actualidad para el tratamiento de datos personales de los usuarios ecuatorianos en relaciones B2C generadas en la prestación de servicios de cómputo en la nube, el presente análisis tomará como punto de referencia las políticas de privacidad que se estipulan para casos B2C con Dropbox.

En el Ecuador los servicios de Dropbox son muy famosos entre el público en general, por su difusión, son muy utilizados por gente joven, que no es consciente de las afectaciones que podrían generar a sus derechos a través de este tipo de contrataciones.

En la presente investigación se toma como ejemplo al caso de las políticas de privacidad de Dropbox, pero hay muchos otros proveedores de servicios de *cloud computing* muy popularizados en Ecuador como *iCloud, Google, Facebook, SkyDrive,* etc. en todos esos casos también puede existir una relación B2C con usuarios ecuatorianos. Aunque resulta excesivo realizar un análisis de todos esos casos en un solo trabajo de grado, será importante que a futuro, y para precautelar los derechos de los ecuatorianos, también sean analizadas las políticas de privacidad que se estipulan en cada caso.

Es importante tener presente que debido a que esta investigación se centra en la prestación de servicios de *cloud computing* para usuarios ecuatorianos únicamente para aquellos casos en que se generen relaciones B2C, también será preciso dar algunas referencias de la normativa que en la actualidad aplica para las relaciones con *e-consumers* ecuatorianos (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos y la Ley Orgánica de Defensa al Consumidor), aclarando que las mismas simplemente complementan la presente investigación, pues no constituyen el objeto de la misma.

3.4.1 Análisis del contenido de las políticas de privacidad que establece Dropbox conforme al ciclo de vida de los datos

Es primordial recordar que las fases del ciclo de vida de seguridad de los datos definidas en el capítulo primero son el sustento de esta parte del análisis. Es importante también mencionar que estas fases están centradas en las distintas acciones y funciones que el proveedor de servicios de cómputo en la nube puede realizar, lo que es de mucha ayuda para este estudio, pues se busca definir sus responsabilidades generadas en virtud de los principios del derecho a la protección de datos personales por estipular sus políticas de privacidad y el manejo de información de sus usuarios.

Dropbox es un servicio de alojamiento en la nube fundado en el año 2007, y en la actualidad constituye una de las opciones más populares de nube personal. Entre los principales servicios que oferta incluye el de almacenamiento en la

nube y la sincronización de archivos en la nube (Dropbox, s.f.), su amplia difusión entre los usuarios posiblemente se deba a las facilidades que proporciona y lo sencillo que resulta manejarlo.

En definitiva, el nivel de servicios que oferta Dropbox, dentro de la clasificación de *cloud computing* brindada en el primer capítulo es el de SaaS (*Software as a Service*), esto debido a que su utilización se realiza a través de un *software* que almacena y sincroniza archivos en la nube.

Dropbox ofrece a sus usuarios tres planes: el primero gratuito, se denomina "Dropbox Basic" y brinda 2GB espacio en la nube; el segundo, denominado "Dropbox Pro" incluye 1TB de espacio en la nube por un costo mensual de 9,99 USD; y finalmente, el tercero denominado "Dropbox for Business" que tiene un costo de 15 USD al mes por suscriptor. Los términos y condiciones de las políticas de privacidad que se pacten se establecerán acorde al tipo de plan que el usuario contrate. Los contratos de los planes "Dropbox Basic" y de "Dropbox Pro" serán de adhesión, mientras que en el caso del plan "Dropbox for Business" de acuerdo al caso será posible negociar las cláusulas contractuales con el proveedor.

En base a lo señalado, las cláusulas que serán utilizadas para el presente estudio se las denomina como "políticas de privacidad" en la página web Dropbox.com, las mismas que no aplicarán para el plan de "Dropbox for Business" (caso de contratación B2B). Se analizan únicamente las "políticas de privacidad", pues son estas las que definirán la actuación del responsable de tratamiento en las fases del ciclo de vida de datos en la nube definidas en el capítulo primero del presente trabajo.

A continuación se realizará un análisis de los aspectos más relevantes de las políticas de privacidad, mismas que se publicaron el 13 de febrero de 2015. Dropbox en sus políticas de privacidad divide de la siguiente forma a sus cláusulas:

a) Qué recopilamos y por qué lo hacemos.
b) Con quiénes se comparte la información.
c) Cómo protegemos tu información.
d) Dónde se almacenan los datos.
e) Cambios.

Como se puede evidenciar los títulos que distinguen a cada cláusula son amplios y en cada una de estas se hace referencia a temas variados, es por esto que será preciso analizar a fondo el contenido de cada apartado de sus cláusulas dividiéndolas conforme a sus apartados.

a) Cláusula primera: Qué recopilamos y por qué lo hacemos

"Qué recopilamos y por qué lo hacemos

Recopilamos y usamos la siguiente información para prestar, mejorar y proteger nuestros Servicios:" (Dropbox, 2015)

Esta cláusula enumera toda la información que será recogida y tratada en virtud del contrato de las partes. Esta información podrá ser relativa a la cuenta del usuario, los documentos que este suba en la nube (fotografías, pdf, diapositivas, etc.), e información que identifique los dispositivos de los usuarios y su navegación en red.

En esta cláusula entonces Dropbox debería brindar toda la información respecto de los datos que recogerá, con qué finalidad se recogen y los usos que dará a los datos de sus usuarios, incluso si estos son inocuos.

> "Cuenta. Recopilamos cierta información y la vinculamos a tu cuenta, como tu nombre, dirección de correo electrónico, número de teléfono, información de pago y dirección física. Algunos de nuestros servicios te permiten acceder a tus cuentas y a tu información relacionada con otros proveedores de servicios." (Dropbox, 2015)

En el apartado de “cuenta”, Dropbox especifica cierta información que será recogida por el hecho de crear una cuenta con ellos. El contenido de este párrafo, en relación con el ciclo de vida de los datos en el *cloud computing* hace alusión a la fase 1 de creación, debido a que se refiere a la creación o modificación de un contenido digital que será almacenado en la nube.

Conforme a lo expuesto en el capítulo segundo de este trabajo, ciertos datos detallados en este apartado como el nombre, la dirección de correo electrónico, el número de teléfono y la dirección física son datos personales y a estos les aplica el régimen normal de tratamiento de datos personales, para lo cual debería aplicar, conforme al principio de seguridad, las medidas de seguridad respectivas.

Al Dropbox estipular que recopilará “información de pago” no detalla qué tipo de datos exactamente serán recogidos, podría ser el tipo de tarjeta de crédito, los números de tarjeta de crédito, información crediticia, entre otros. Entre la variedad de datos que podría recopilar Dropbox basándose en “la información de pago” que estipulan en el contrato podría incluir datos sensibles, lo que implicaría que, basados en el principio de seguridad, adopten medidas más altas de seguridad y adopten un régimen de tratamiento de datos sensibles, distinto al que manejan con el resto de datos.

Se puede observar también que en este apartado se enumera cierta información que Dropbox recopilará de sus usuarios, pero en ninguna parte se informa en detalle al usuario de la finalidad para la cual estos datos serán recogidos, lo que violenta el principio de finalidad del derecho a la protección de datos personales expuesto en líneas previas. Al informar debidamente la finalidad para la cual se recolectan los datos, se estaría contraviniendo de forma automática principios del derecho a la protección de datos personales como el de lealtad y licitud, calidad o exactitud, y el de no utilización abusiva.

Si Dropbox no informa sobre la finalidad para la que recolecta los datos de los usuarios en sus políticas de privacidad también contraviene el derecho a la

información de los consumidores ecuatorianos, lo que devengaría en que no exista consentimiento informado del usuario conforme a lo descrito en líneas previas en lo relativo al derecho a la protección de datos personales.

> Servicios. Cuando usas nuestros Servicios, almacenamos, procesamos y transmitimos tus archivos (incluidos tus fotos, datos estructurados y correos electrónicos) e información relacionada con ellos (como etiquetas de ubicación en fotos). Si nos concedes acceso a tus contactos, almacenaremos esos contactos en nuestros servidores para que puedas usarlos. De este modo, te será más fácil llevar a cabo ciertas acciones, como compartir tus archivos, enviar mensajes de correo electrónico e invitar a otras personas a usar los Servicios. (Dropbox, 2015)

El apartado de “servicios” hace referencia a ciertos datos que serán almacenados y procesados por Dropbox por la utilización de sus servicios de cómputo en la nube. En relación con el ciclo de vida de los datos, lo estipulado en esta parte tiene relación directa con la fase 2 de almacenamiento, debido a que se especifica que los datos serán almacenados por Dropbox; y con la fase 3 de uso, ya que se hace referencia al procesamiento de los datos que realizará Dropbox.

En este apartado Dropbox enuncia las distintas acciones que realizará durante el tratamiento de datos personales de sus usuarios, como las de almacenamiento y procesamiento (que podría incluir la realización de perfiles). Pero aunque se enumeran dichas acciones, no se detallan las razones por las que Dropbox las efectuará, lo que contraviene el principio de finalidad del derecho a la protección de datos personales.

Cuando Dropbox estipula que recogerá fotos, datos estructurados y correos electrónicos, la interpretación que se puede dar de ese tipo de datos es muy general y ambigua, no se sabe a ciencia cierta qué datos exactamente serán recogidos. Los correos o fotos podrían contener datos sensibles del titular, lo que implicaría que, Dropbox en observancia al principio de seguridad, adopte medidas más altas de seguridad y un régimen de tratamiento de datos sensible distinto.

Por otro lado, de acuerdo a lo expuesto en el capítulo segundo de este trabajo, bajo el supuesto de que el usuario conceda acceso a sus contactos, Dropbox estaría obligado a informar detallando y justificando las acciones que serán realizadas por la recogida de este tipo de información. Esto acorde a los principios de finalidad y de no utilización abusiva, los que evidenciamos que no han sido observados para la redacción de este párrafo.

En este apartado se enumera cierta información que Dropbox recopilará de sus usuarios, pero en ninguna parte se informa en detalle al usuario de la finalidad para la cual estos datos serán recogidos, lo que violenta el principio de finalidad del derecho a la protección de datos personales expuesto en líneas previas. Al informar debidamente la finalidad para la cual se recolectan los datos, se estaría contraviniendo de forma automática principios del derecho a la protección de datos personales como el de lealtad y licitud, calidad o exactitud, el de conservación limitada y el de no utilización abusiva.

Si Dropbox no brinda la debida información, respecto a la finalidad para la que recolecta los datos de los usuarios en sus políticas de privacidad, contraviene el derecho a la información de los consumidores ecuatorianos, lo que devengaría en que no observe el principio de consentimiento informado del usuario, conforme a lo descrito en líneas previas en lo relativo al derecho a la protección de datos personales.

> Uso. Recopilamos información de los dispositivos que usas para acceder a los Servicios y acerca de ellos. Aquí se incluyen las direcciones IP, el tipo de explorador y dispositivo, la página web que visitaste antes de acceder a nuestros sitios y los identificadores asociados con tus dispositivos. Es posible que tus dispositivos (según la configuración) también transmitan información a los Servicios acerca de tu ubicación. (Dropbox, 2015)

Lo estipulado en el apartado de “uso”, hace referencia a los datos que Dropbox recoge de sus usuarios por el hecho de que estos utilicen sus servicios. Esta información se relacionará con los dispositivos con los que se utilizan sus servicios y ciertos datos de su navegación, y en algunos casos, también

recogerán información relativa a la ubicación del usuario. Como se puede observar, al igual que en el apartado de “cuenta”, este párrafo por referirse a la información de los usuarios, que el proveedor de servicios recogerá en su sistema para ser tratada, tiene relación con la fase 1 de creación respecto al ciclo de vida de los datos definido previamente.

Atendiendo a lo expuesto en el capítulo segundo, datos detallados en este apartado como: direcciones IP, el tipo de explorador y dispositivo por medio del que se accede a la red son datos inocuos que exigen medidas de seguridad bajas, conforme al principio de seguridad. Sin embargo, si los datos inocuos son asociados con su titular, estos pasan a ser datos personales y les aplica el régimen normal de tratamiento de datos personales, para lo cual Dropbox, observando el principio de seguridad, debería implementar las medidas de seguridad respectivas.

Al Dropbox estipular que recopilará información de “la página web que se visita antes de acceder a Dropbox o sus sitios asociados” y “otros identificadores asociados con los dispositivos del usuario”, no especifica concretamente los datos que serán recogidos. Por un lado no se conoce a ciencia cierta qué sitios son asociados a Dropbox, así que hay obscuridad respecto a los sitios que podrá conocer Dropbox de la navegación de sus usuarios.

Por otro lado, al Dropbox recolectar información relativa a “otros identificadores asociados” tendría facultades inmensas para recoger datos de sus usuarios, no se puede determinar a ciencia los identificadores a los que se refieren y el tipo de datos a los que podrían acceder. Esto evidencia abuso por parte de Dropbox en la redacción de este apartado, pues este proveedor saca provecho del desconocimiento que tienen sus consumidores (usuarios) de la innovación tecnológica, para distintos datos que no es posible determinar.

También Dropbox podría recolectar datos que le permitan determinar la ubicación exacta de sus usuarios, lo que podría generar la necesidad de que

tome acciones preventivas en el manejo de esos datos sometiéndolos a un régimen de tratamiento de datos sensibles.

De lo descrito en líneas previas se evidencia que en este apartado Dropbox tiene facultades muy amplias para recoger mucha información de sus usuarios, información que en muchos casos podrá incluir datos sensibles, lo que implicaría que, basados en el principio de seguridad, sean adoptadas medidas más altas de seguridad en régimen de tratamiento de datos sensibles, distinto al que se da con el resto de datos.

En este apartado tampoco se informa en detalle al usuario sobre las razones de la recogida de datos y la finalidad de tratamiento, lo que violenta el principio de finalidad del derecho a la protección de datos personales previamente. Al informar debidamente la finalidad para la cual se recolectan los datos, se estaría contraviniendo de forma automática principios del derecho a la protección de datos personales como el de lealtad y licitud, calidad o exactitud, o el de no utilización abusiva.

Si Dropbox no informa al usuario, desde un inicio en sus políticas de privacidad, sobre la finalidad para la que recolecta sus datos, contravendría el derecho a la información de los consumidores ecuatorianos, lo que acarrearía en que no exista consentimiento informado del usuario conforme a lo descrito en líneas previas en lo relativo al derecho a la protección de datos personales.

> "Cookies y otras tecnologías. Aplicamos ciertas tecnologías, como cookies y etiquetas de píxeles, para prestar, mejorar, proteger y promocionar nuestros Servicios. Por ejemplo, las cookies nos ayudan a recordar tu nombre de usuario para tu próxima visita, a comprender la forma en que interactúas con nuestros Servicios y a mejorar nuestros Servicios en función de esa información. Puedes configurar tu explorador para que no admita las cookies, pero ello puede limitar la capacidad de usar los Servicios [...]" (Dropbox, 2015)

Finalmente, el párrafo que se refiere a "cookies y otras tecnologías" advierte que cierta información será recogida por Dropbox en caso de utilizar estas tecnologías. Este párrafo entonces se refiere a la fase 1 de creación,

conforme al ciclo de vida de los datos expuesto. El tema de cookies y otras tecnologías es bastante complejo, y podría generar un nuevo trabajo de investigación, es por esto que para fines del presente trabajo solo se deberá entender, que debido a su uso, los proveedores de servicios de *cloud computing* podrán recopilar más información de sus usuarios, datos que deberían ser almacenados, procesados y archivados de conformidad con los principios estándares que generan un sistema preventivo de protección de datos personales.

b) Cláusula segunda: Con quiénes se comparte la información

> "**Con quiénes se comparte la información**
>
> Podremos compartir información según se describe a continuación, pero no la venderemos a anunciantes ni a otros terceros.
>
> Otras personas que trabajan para Dropbox. Dropbox usa determinados terceros de confianza para prestar, mejorar, proteger y promocionar los Servicios. Estos terceros solamente tendrán acceso a tu información para llevar a cabo tareas en representación de nosotros y de conformidad con esta Política de privacidad." (Dropbox, 2015)

El contenido íntegro de este este párrafo establece que toda la información recogida por Dropbox, en conexión con lo estipulado previamente en la cláusula "Qué recopilamos y por qué lo hacemos", podrá ser compartida con varios actores. En este apartado hay indeterminación de los terceros de confianza, lo que acarrea que no se sepa a ciencia cierta quienes podrían acedar a la información del usuario.

Al Dropbox hablar de "terceros de confianza" debería detallar claramente qué funciones cumplirán estos terceros, pues conforme a la actual redacción de este postulado, no se puede comprender a ciencia cierta si estos terceros tendrán solamente facultades de encargados de tratamiento, o si hasta cierto punto podrían llegar a ser responsables.

Independientemente del papel que desempeñen los "terceros de confianza" sus actividades deberán ser llevadas a cabo conforme a políticas de

privacidad que se acojan al contenido de los principios estándar descritos previamente, de no ser así, no se estaría previniendo posibles violaciones al derecho a la protección de datos personales de los ecuatorianos.

En este apartado se hace referencia a los actores con quienes Dropbox podrá compartir la información de sus usuarios, entonces su contenido cuadra con la fase 4 del ciclo de vida de los datos, relativa a la compartición de los datos. Pero debido a que también se hace alusión a las funciones que cumplirán los terceros de confianza, también se hace referencia a la fase 3 relativa a la utilización de los datos.

> "Otros usuarios. Nuestros Servicios revelan cierta información, como tu nombre y dirección de correo electrónico, a otros usuarios en tu perfil de usuario y las notificaciones de uso compartido. Determinadas características te permiten poner información adicional a disposición de otros usuarios." (Dropbox, 2015)

Respecto a este apartado es importante tener en cuenta que al Dropbox estipular que "determinadas características te permiten poner información adicional a disposición de otros usuarios", debería exponer en detalle las características del servicio que conllevarán exponer su información a otros usuarios, para que en su momento el usuario decida si desea hacerlo o no. Lo señalado se debería realizar en observancia al derecho a la información de los usuarios y a los principios de finalidad y no utilización abusiva.

En este apartado por un lado hay indeterminación de los "otros usuarios" a los que se refiere Dropbox y del tipo de información que será compartida. Esto causa el riego de que el usuario no sepa qué información suya incluso pueda difundirse en redes sociales a otras personas. Esto contraviene el derecho a la información de los consumidores ecuatorianos, lo que acarrearía que no exista consentimiento informado del usuario conforme a lo descrito en líneas previas, en lo relativo al derecho a la protección de datos personales.

Este apartado hace alusión a otras personas con quienes Dropbox podrá compartir la información de sus usuarios, lo que hace que su contenido cuadre con la fase 4 del ciclo de vida de los datos, relativa a la compartición de los datos.

> "Otras aplicaciones. También puedes conceder acceso a tu información y a tu cuenta a terceros, por ejemplo, a través de las API de Dropbox. Ten en cuenta que, en ese caso, el uso de tu información se regirá por las políticas de privacidad y las condiciones de uso correspondientes." (Dropbox, 2015)

Este postulado advierte que cierta información será recogida por terceros producto de la utilización de las API (Interface de Programación de Aplicaciones) que tiene Dropbox, en aquellos casos la información que se recoja por estos terceros será tratada conforme a otras políticas de privacidad.

El tema de las API es bastante complejo, y su análisis podría desencadenar por sí mismo un nuevo trabajo de investigación, es por esto que, para fines del presente trabajo, solo es preciso tener claro que la utilización de las API, podría brindar acceso a la información del usuario a otros los proveedores de servicios de *cloud computing,* quienes tratarán dichos datos conforme a sus propias políticas de privacidad. Es por esto que Dropbox debería informar de mejor manera a sus usuarios desde la redacción de sus políticas de privacidad sobre las implicancias de utilizar sus API, esto conforme al principio de finalidad, no utilización abusiva y al derecho de información de usuarios, con lo que se adoptaría un sistema preventivo de protección de datos personales.

> "Administradores de Dropbox para empresas. Si usas Dropbox para empresas, tu administrador podrá acceder a tu cuenta de Dropbox para empresas y controlarla. Consulta las políticas internas de tu empleador si tienes alguna consulta respecto de esta regla. Si no usas Dropbox para empresas, pero interactúas con un usuario de Dropbox para empresas (por ejemplo, al unirte a una carpeta compartida o al acceder a archivos que ese usuario comparte), los miembros de esa organización podrán ver el nombre, la dirección de correo electrónico y la dirección IP asociados con tu cuenta en el momento de la interacción." (Dropbox, 2015)

Este apartado se refiere únicamente al tratamiento de información, que se generaría por contrataciones de servicios de *cloud computing* entre empresas (B2B), tema que no es materia de la presente investigación, y por lo tanto esta parte de las políticas de privacidad de Dropbox no será analizada.

> "Fuerzas del orden público. Podremos divulgar tu información ante terceros si determinamos que ello es razonablemente necesario para (a) cumplir con la ley, (b) proteger a una persona de la muerte o de lesiones graves, (c) prevenir fraudes o el abuso hacia Dropbox o hacia nuestros usuarios o (d) proteger los derechos de propiedad de Dropbox." (Dropbox, 2015)

La redacción de este apartado es tan amplia que podría dar pauta a diversidad de interpretaciones. Dropbox titula al postulado como "Fuerzas del Orden Público", pero de su redacción desprende que divulgarán la información de sus usuarios a "terceros" en general.

Las razones que enuncia Dropbox, para divulgar la información, son ambiguas y facultan al proveedor a compartir los datos de sus usuarios desmesuradamente. Este postulado podría contravenir principios del derecho a la protección de datos personales como el de lealtad y licitud o el de no utilización abusiva.

La redacción leonina de este postulado podría confundir al usuario, quien pensará que la información solo será compartida con autoridades estatales, cuando en realidad no es así. Habrá que determinar si para divulgar esta información es preciso tener orden judicial, porque de no hacerlo se podrían violentar principios del debido proceso. Lo dicho podría encajar en los numerales 8 y 9 del artículo 43 de la Ley Orgánica de Defensa al Consumidor ecuatoriana, relativa a las cláusulas prohibidas y nulas de pleno derecho en los contratos de adhesión.

El contenido del postulado se refiere a los terceros con quienes Dropbox podrá compartir la información de sus usuarios, contenido que cuadra con la fase 4 del ciclo de vida de los datos, relativa a la compartición de los datos.

> "[…] La correcta administración de tus datos es fundamental para nosotros y es una responsabilidad que asumimos con compromiso. Consideramos que los datos de los usuarios deben recibir las mismas protecciones legales, independientemente de si están almacenados en nuestros servicios o en el disco duro de sus computadoras. Nos regiremos por los siguientes principios de solicitud del gobierno cada vez que recibamos, analicemos y respondamos a las solicitudes del gobierno relacionadas con los datos de nuestros usuarios:
>
> Ser transparentes
>
> Combatir las solicitudes masivas
>
> Proteger a todos los usuarios
>
> Prestar servicios de confianza […]" (Dropbox, 2015)

El contenido de esta declaración de Dropbox debería enumerar los principios estándar del derecho a la protección de datos personales. Al Dropbox referirse a "ser transparentes", está declarando que sus actuaciones deberán ser acordes al principio de lealtad y licitud descrito en líneas previas. Sin embargo, al realizar las demás declaraciones de "combatir solicitudes masivas", "proteger a todos los usuarios", y "prestar servicios de confianza" no se sabe a ciencia cierta a qué se refieren exactamente y por la amplitud de sus declaraciones deberían actuar conforme a todos los principios de protección de datos personales descritos en líneas previas, pues únicamente la observancia de estos en conjunto genera un derecho a la protección de datos personales de los usuarios y por ende confianza.

c) Cláusula tercera: Cómo protegemos tu información

> "**Cómo protegemos tu información**
>
> Seguridad. Disponemos un equipo dedicado a preservar la seguridad de tu información y a llevar a cabo pruebas de vulnerabilidad. Seguimos trabajando en nuevas características para preservar la seguridad de tu información, además de otros desarrollos, como la autenticación de dos factores, el cifrado de archivos inactivos y las alertas cuando se vinculan a tu cuenta nuevos dispositivos y aplicaciones." (Dropbox, 2015)

Conforme al principio de seguridad del derecho a la protección de datos personales descrito en líneas previas, Dropbox en este apartado debería

detallar los distintos niveles de seguridad que brindará a la información conforme al tipo de datos a los que realice tratamiento. Sin la implementación de distintas medidas de seguridad, desde la misma redacción de las políticas de privacidad de Dropbox, se estaría haciendo caso omiso al principio de seguridad, que forma parte esencial del sistema preventivo del derecho a la protección de datos personales.

Debido a que este apartado hace referencia a ciertos procedimientos, que Dropbox realiza de la información para precautelar su seguridad, conforme al ciclo de vida de los datos en el *cloud computing*, este apartado tiene relación con la fase 3 de uso, ya que se refiere al procesamiento de los datos que realizará Dropbox.

> "Retención. Retendremos la información que almacenes en nuestros Servicios durante todo el tiempo necesario para prestarte esos Servicios. Si eliminas tu cuenta, también eliminaremos esa información. Pero ten en cuenta que: (1) puede haber latencia en la eliminación de esta información de nuestros servidores y almacenamiento de copias de seguridad y (2) podremos retener esta información si es necesario para cumplir con nuestras obligaciones legales, resolver disputas o ejercer nuestros acuerdos." (Dropbox, 2015)

Este apartado estipula el tiempo que Dropbox almacenará la información de sus usuarios, pero también especifica casos en que la mantendrán archivada en sus ficheros luego del cierre de la cuenta y cuando esta será destruida por completo.

El contenido de este apartado debería ser concordante al principio de conservación limitada de datos, del derecho a la protección de datos personales descrito en previamente. Es así que Dropbox debería especificar en este apartado un tiempo máximo para la conservación de datos de sus usuarios, luego de que haya finalizado la prestación de sus servicios y en caso de que Dropbox decida retener la información de sus usuarios debería disociarlos de su titular. Como se observa, la redacción de este postulado se deslinda del contenido del principio de conservación limitada del derecho a la protección de datos personales.

Por otro lado, al Dropbox estipular que “podrá retener la información de sus usuarios para cumplir con sus obligaciones legales, resolver disputas o ejercer sus acuerdos” pone en indefensión a sus usuarios y hace caso omiso al derecho a la protección de datos de carácter personal que los ampara, lo que encaja con los numerales 6 y 9 del artículo 43 de la Ley Orgánica de Defensa al Consumidor ecuatoriana, relativa a las cláusulas prohibidas y nulas de pleno derecho en los contratos de adhesión.

Conforme al ciclo de vida de los datos, lo estipulado en este postulado tiene relación directa con la fase 2 de almacenamiento, debido a que se especifica que los datos serán almacenados por Dropbox; la fase 3 de uso, ya que se hace referencia al procesamiento de los datos que realizará Dropbox, la fase 5 relativa al archivo de los datos luego que dejen de ser usados, y la fase 6 para los casos de destrucción definitiva de la información.

d) Cláusula cuarta: Dónde se almacenan los datos

> “**Dónde se almacenan los datos**
>
> En todo el mundo. Para prestar los Servicios, podremos almacenar, procesar y transmitir información en ubicaciones de todo el mundo (también fuera de tu país). La información también podrá almacenarse de forma local en los dispositivos que usas para acceder a los Servicios […]” (Dropbox, 2015)

Como se observa, esta cláusula explica el lugar físico en que se almacenarán los datos que serán utilizados por Dropbox, durante la prestación de sus servicios de cómputo en la nube. Esta cláusula refleja la característica de “reservas de recursos en común” del *cloud compuing,* explicada en el capítulo primero de este trabajo.

En definitiva, por referirse a la ubicación de las bases de datos de Dropbox donde se almacena la información de sus usuarios, esta cláusula tiene relevancia en la fase 2 del ciclo de vida de los datos en el *cloud computing,* referida al almacenamiento de datos.

e) Cláusula quinta: Cambios

> "**Cambios**
>
> Si participamos de una reorganización, fusión, adquisición o venta de nuestros activos, tu información podrá transferirse como parte de esa transacción. Te informaremos (por ejemplo, mediante un mensaje a la dirección de correo electrónico asociada con tu cuenta) cualquier transacción de este tipo y te indicaremos las opciones disponibles.
>
> Podremos revisar esta Política de privacidad oportunamente y publicar la versión más actualizada en nuestro sitio web. Te informaremos en caso de que tus derechos se vean apreciablemente afectados como consecuencia de una revisión." (Dropbox, 2015)

Esta cláusula hace referencia a aquellos casos en que Dropbox estará facultado para cambiar los términos y condiciones, establecidos en las políticas de privacidad ya expuestas.

Acorde a los derechos del usuario, Dropbox no puede realizar cambios de sus políticas de privacidad sin antes tener nuevamente el consentimiento informado de sus usuarios, de no ser así se devengaría en falta de desarrollo del sistema preventivo de protección de datos personales.

Además al Dropbox realizar cambios a sus políticas de privacidad, se encajaría en los numerales 6 y 9 del artículo 43 de la Ley Orgánica de Defensa al Consumidor ecuatoriana, relativa a las cláusulas prohibidas y nulas de pleno derecho en los contratos de adhesión.

Debido a que este postulado hace referencia a cambios que podrían afectar a cualquiera de las cláusulas previamente analizadas, es importante tener en consideración que el texto de esta cláusula podría llegar a tener incidencia en cualquiera de las seis fases de ciclo de vida de los datos en el *cloud computing* desarrolladas en el capítulo primero de este trabajo.

Del análisis realizado podemos evidenciar que todos los principios estándar del derecho a la protección de datos personales tienen relevancia en el contenido de todas las cláusulas estipuladas por Dropbox. Esto nos sirve de

sustento frente al lector, para detectar a continuación los riesgos que se generan por el no reconocimiento expreso de los principios estándar del derecho a la protección de datos personales, expuestos en el capítulo segundo de este trabajo.

3.4.2 Riesgos que genera el no reconocimiento expreso de los principios de protección de datos personales en el Ecuador

El presente trabajo busca resaltar la importancia de desarrollar en Ecuador un sistema preventivo, que garantice el derecho a la protección de datos personales de usuarios de servicios de *cloud computing*. Para que dicho sistema se active es elemental reconocer de forma expresa e inequívoca el contenido de sus principios, que junto a otros elementos, constituyen los contenidos esenciales que configuran derecho a la protección de datos personales.

El estudio ejemplificativo realizado previamente a las políticas de privacidad de Dropbox, toma elementos de análisis a los principios estándar del derecho a la protección de datos personales, expuestos en el capítulo segundo de este trabajo, ubicando a cada cláusula en las distintas fases del ciclo de vida de los datos en el *cloud computing,* de acuerdo a las acciones y funciones que el proveedor de servicios de cómputo en la nube puede realizar.

Este apartado empatará el contenido del análisis de las políticas de privacidad de Dropbox realizado en el punto 3.4.1 de este trabajo contrastándolo con las acciones y funciones que Dropbox puede desempeñar, de acuerdo al ciclo de vida de los datos en la nube, para así, poder detectar y puntualizar los riesgos que existen para los ecuatorianos al no desarrollar de forma clara y expresa en su legislación, los principios estándar del derecho a la protección de datos personales.

El contenido de las políticas de privacidad de Dropbox fue analizado conforme a diversas cláusulas relacionadas directamente con las funciones que los actores están facultados a realizar, de acuerdo a cada fase del ciclo de vida de los datos

en el *cloud computing,* definido en el capítulo primero de este trabajo. Para ilustración del lector, la siguiente figura ubica al contenido de cada cláusula en una de las seis fases explicadas con anterioridad:

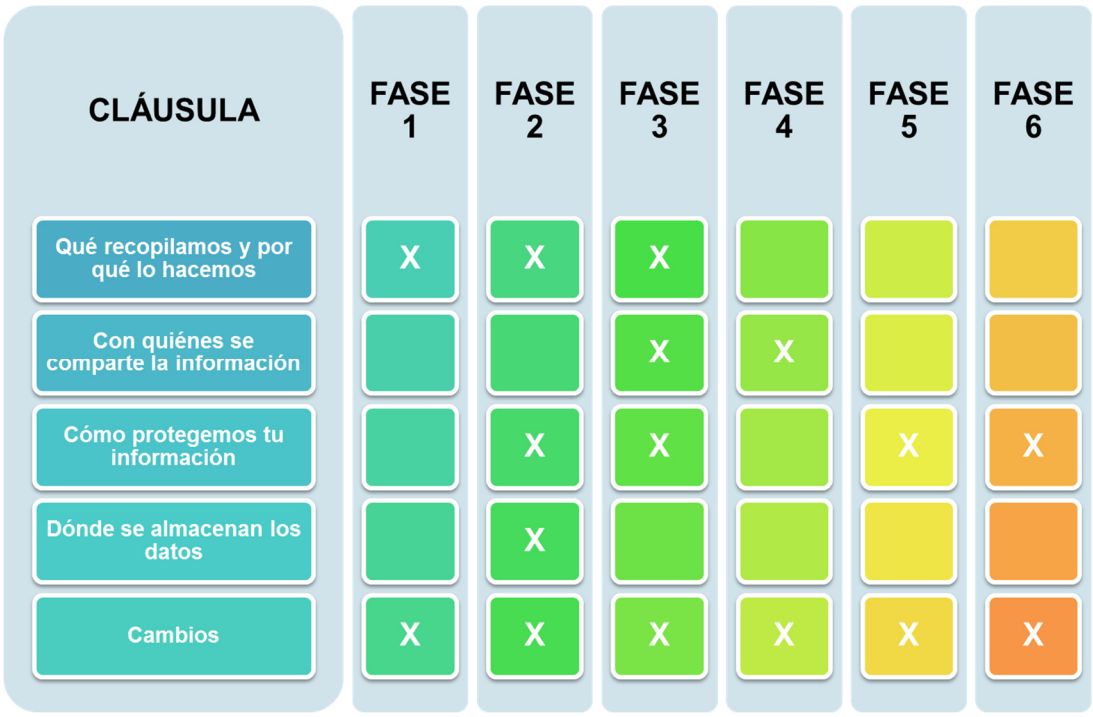

Figura 12. **Cláusulas de contrato de adhesión de Dropbox según las fases del ciclo de vida de los datos en el *cloud computing***

De acuerdo a lo establecido en las cláusulas de políticas de privacidad de Dropbox, combinadas con el contenido de la Figura 12 y la Figura 10, la Figura 13 define las distintas funciones que podrán practicar los actores de servicios de *cloud computing* en Dropbox.

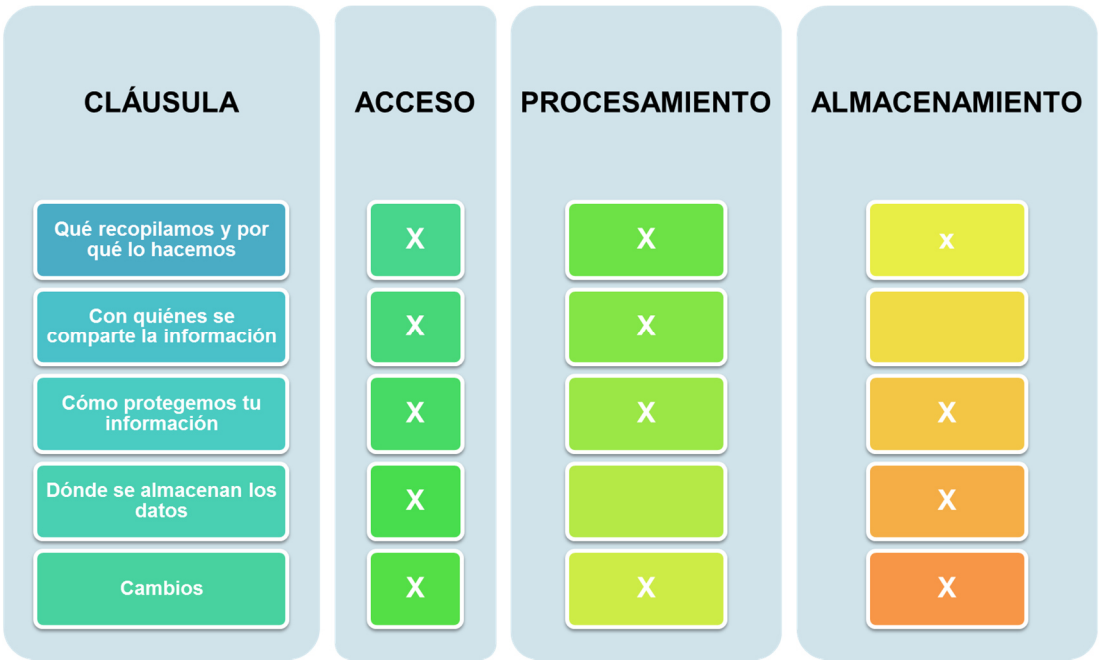

Figura 13. **Funciones que los proveedores pueden desempeñar de acuerdo a las políticas de privacidad estipuladas por Dropbox**

De las figuras expuestas podemos entonces inducir que, las cláusulas que establece el proveedor de servicios de Dropbox lo facultan desde el primer momento (adhesión a las políticas de privacidad), para realizar las funciones de acceso, procesamiento y almacenamiento de la información en las distintas fases del ciclo de vida de los datos en el *cloud computing.*

Así pues, de acuerdo a las funciones que realice el prestador de servicios de cómputo en la nube, este deberá cumplir, desde el momento en que redacte sus políticas de privacidad, con las obligaciones específicas que se le atribuyen por el derecho a la protección de datos personales de sus usuarios. Para lo cual, es necesario que exista un sistema preventivo de protección de datos personales en el Ecuador, en el que se especifique previamente y de forma clara las obligaciones que sus principios estándar generan para los responsables de tratamiento.

Igualmente, cada uno de los principios descritos en el punto 3.3 de este capítulo se relaciona con las distintas funciones, que el proveedor de servicio de *cloud computing* puede desempeñar, de acuerdo al ciclo de vida de los datos en la nube expuesto en el capítulo primero. Esta relación se detalla en la Figura 14 para mayor comprensión del lector.

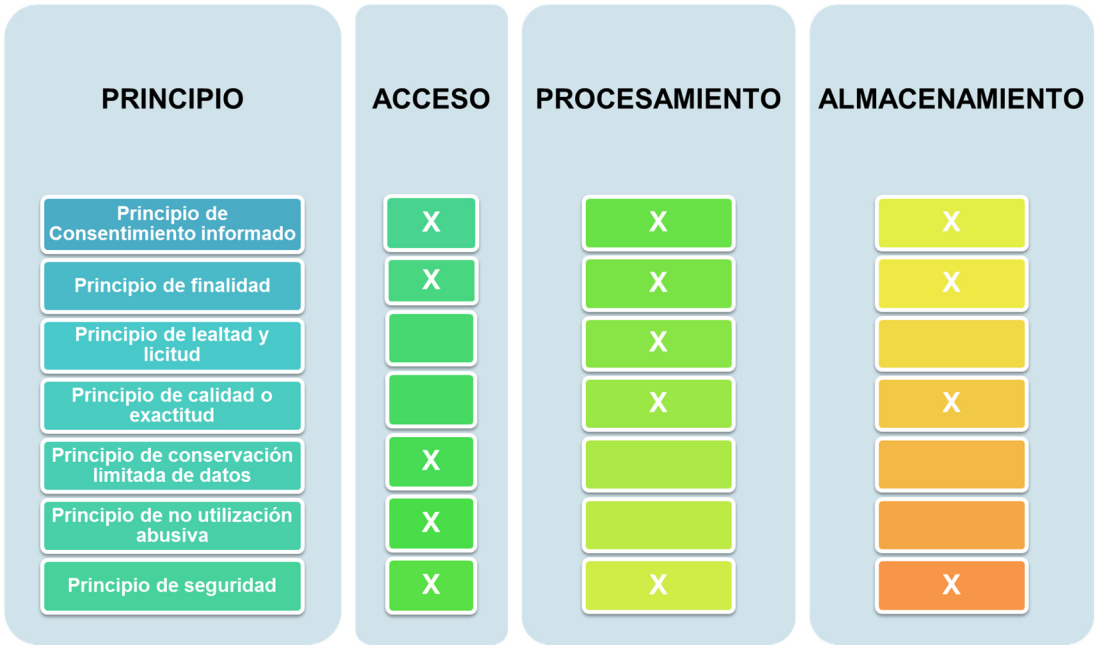

Figura 14. **Principios de protección de datos personales que los proveedores de servicios de *cloud computing* deben observar de acuerdo a las funciones que pueden desempeñar**

Cada uno de los principios que se distinguen en la Figura 14, debería ser observado y acogido por el proveedor de servicios de *cloud computing;* cuando este realice alguna de las funciones de acceso, procesamiento o almacenamiento que se detallan, conforme al caso. Por ejemplo, cuando el proveedor de servicios en la nube vaya a ejercer la función de almacenamiento de datos, esta debería ceñirse a los principios de finalidad, calidad o exactitud, y al de finalidad.

Por otro lado, del análisis particular de las políticas de privacidad que establece Dropbox en la relación B2C por la que presta servicios de *cloud computing* a usuarios ecuatorianos, hemos detallado en la Figura 13 las distintas funciones que Dropbox puede realizar respecto de los datos de sus usuarios. Estas funciones han sido definidas de acuerdo a cada fase del ciclo de vida de los datos en la nube, como se desarrolla en el capítulo primero de este trabajo.

El contenido de las Figuras 13 y 14 ha servido de sustento para poder relacionar de forma directa, el contenido de las cláusulas que estipula Dropbox, con los principios estándar del derecho a la protección de datos personales, definidos en el capítulo segundo.

Por un lado la Figura 13 nos da el punto de partida, ubicando el contenido de cada cláusula que Dropbox estipula en sus políticas de privacidad dentro las distintas funciones que puede realizar respecto de los datos de sus usuarios, esto conforme a lo definido en el ciclo de vida de los datos en la nube en el capítulo primero. Por otro lado, la Figura 14 enlaza a los principios estándar del derecho a la protección de datos personales con cada una de las funciones que un proveedor de servicios en la nube puede desempeñar.

La Figura 14 entonces sirve de sustento para la realización de la Figura 15, ya que la conecta con el contenido de la Figura 13 (funciones que los proveedores pueden desempeñar de acuerdo a las políticas de privacidad estipuladas por Dropbox). Cada función que Dropbox puede desempeñar de acuerdo a sus políticas de privacidad fue empatada con las funciones que obligarían al proveedor de servicios en la nube a observar y acoger ciertos principios del derecho a la protección de datos personales. Es decir se prestó atención las distintas funciones que se coincidían en ambas figuras para así realizar la Figura 15.

A continuación se expone la Figura 15, su contenido especifica los principios estándar de protección de datos personales que Dropbox debería observar para la redacción de cada una de sus cláusulas de privacidad.

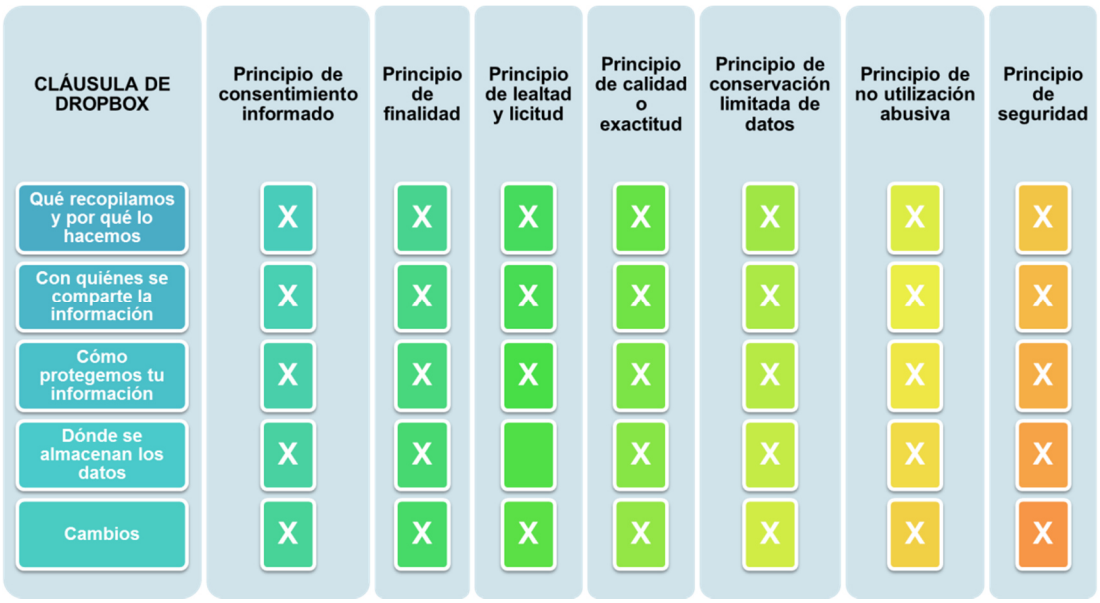

Figura 15. **Principios que los proveedores deben observar en la redacción de las cláusulas de políticas de privacidad de Dropbox**

En conexión con el análisis del punto 3.4.1 de este capítulo, en la Figura 15 se observa que los principios estándar de protección de datos personales deberían ser acogidos por Dropbox en la redacción de prácticamente todas sus cláusulas. Por ejemplo, para la redacción de la cláusula "Dónde se almacenan los datos", Dropbox debería tener en cuenta el principio de finalidad, de calidad o exactitud, de conservación limitada de datos de no utilización abusiva y de seguridad.

Cabe señalar que la cláusula "Dónde se almacenan los datos", es la única en la que Dropbox no estaría obligado a considerar el principio de lealtad y licitud, puesto que este principio únicamente tiene incidencia cuando el proveedor está facultado a cumplir funciones de procesamiento; y el contenido de la cláusula estipulada solo hace referencia a la realización de funciones de acceso y almacenamiento.

De acuerdo al análisis desarrollado se puede evidenciar que el proveedor de servicios de *cloud computig,* que en este caso ejemplificativo de análisis es Dropbox, debería sujetar la redacción de sus cláusulas contractuales relativas al

manejo de información de sus usuarios (políticas de privacidad) al contenido de todos los principios de protección de datos personales.

Del análisis realizado se evidencia la importancia cardinal de que en la normativa ecuatoriana se desarrolle expresamente el contenido de cada uno de los principios que configuran el derecho a la protección de datos personales. Si no se definen dichos principios no existe en la actualidad en Ecuador normativa específica que permita a los ecuatorianos entender el alcance de las cláusulas estipuladas por Dropbox, y por lo tanto este proveedor de servicios de *cómputo en la nube* ignorará el contenido del numeral 19 del artículo 66 de la Constitución de la República.

Esto desencadena en la posible violación del derecho a la protección de datos personales de los ecuatorianos pues, conforme desprende del análisis ejemplificativo del caso Dropbox, en la actualidad este derecho no es resguardado previamente en la redacción de políticas de privacidad por proveedores de servicios de *cloud computing*.

En Ecuador no se han desarrollado principios estándar, que prevengan posibles violaciones al derecho a la protección de datos personales de los ecuatorianos. Este particular, analizado a partir de la relación B2C en la prestación de servicios de *cloud computing*, ha permitido detectar que el usuario es vulnerable frente a las políticas de privacidad que estipulan proveedores de *cloud computing* como Dropbox.

En Ecuador debido a que no se ha desarrollado normativa que genere un sistema preventivo, definiendo principios estándar del derecho a la protección de datos personales, se han detectado los siguientes riesgos basados en el análisis ejemplificativo realizado a las políticas de privacidad de Dropbox:

1. No se brinda información suficiente a los usuarios respecto al tratamiento de sus datos, lo que va contra el principio de consentimiento informado;

2. La redacción de las cláusulas de Dropbox es muy ambigua y no especifica la finalidad para la cual recogerá y tratará los datos, lo que contraviene el principio de finalidad;

3. Es poco probable que, en el desarrollo del tratamiento de datos personales, Dropbox proceda conforme al principio de lealtad y licitud, pues sus políticas de privacidad no acogen el principio de finalidad;

4. Ya que Dropbox no especifica en sus políticas de privacidad los datos de sus usuarios y las razones para su recogida, mientras este realice funciones de tratamiento de esta información, no será probable que actúe conforme al principio de calidad o exactitud;

5. Dropbox no determina tiempos límite para conservar los datos de sus usuarios, lo que contraviene el principio de conservación limitada de los datos;

6. Debido a que las políticas de privacidad de Dropbox no establecen una finalidad para la recogida, el uso de los datos, y los procedimientos empleados durante el tratamiento de éstos, no es acogido el principio de no utilización abusiva; y

7. Debido a que Dropbox no establece en sus políticas de privacidad distintas medidas de seguridad para la información de sus usuarios, no aplica el principio de seguridad.

Los riesgos enumerados se especifican en la Figura 16, pues cada uno de estos responde a la necesidad de implementar uno de los principios estándar expuestos en el capítulo segundo del presente trabajo, y analizados en el capítulo tercero, en la relación B2C por la prestación de servicios de *cloud computing* en el caso ejemplificativo de las políticas de privacidad de Dropbox.

Figura 16. **Riesgos para los usuarios de servicios de *cloud computing* por la falta de reconocimiento de los principios estándar del derecho a la protección de datos personales en Ecuador**

Del contenido de la Figura 16 podemos evidenciar que cada riesgo detectado, tiene relación directa con la falta de desarrollo en la normativa ecuatoriana de los principios estándar del derecho a la protección de datos personales. Entonces, si no se reconocen en Ecuador expresamente los principios estándar que son parte del conjunto de elementos que configuran el derecho a la protección de datos personales, es evidente que los usuarios ecuatorianos se hallan en estado de indefensión frente a los varios riesgos puntualizados.

Del análisis realizado se desprende que las implicaciones del *cloud computing* en las relaciones B2C no están siendo asimiladas profundamente, y por ende, no existe en Ecuador un sistema preventivo de protección de datos personales. El contenido de las políticas de privacidad de Dropbox, atenta a varias disposiciones expresas de la normativa del país, por lo tanto, proveedores de servicios de *cloud computing* tanto nacionales como internacionales (Dropbox), hacen caso omiso incluso a leyes vigentes en el ordenamiento jurídico

ecuatoriano. Ante estos riesgos el Estado ecuatoriano debe tomar acciones, es preciso que se brinden las garantías debidas al derecho a la protección de datos personales de los ciudadanos.

3.5 Propuesta para desarrollar principios estándares de protección de datos personales en la legislación Ecuatoriana

Luego de haber tratado todos los puntos relevantes de la investigación, es necesario conectar diversas ideas plasmadas en este trabajo, para así fundamentar adecuadamente la propuesta de desarrollar, en la legislación ecuatoriana, los principios estándar que generarían un sistema preventivo del derecho a la protección de datos personales.

Con el análisis del caso práctico de Dropbox, se ha logrado evidenciar que los ecuatorianos viven en una realidad globalizada, donde servicios en la nube cada día van difundiéndose más entre los consumidores. El *cloud computing,* sin lugar a dudas, ofrece facilidades inigualables y es importante que se continúe difundiendo, porque los avances tecnológicos son positivos para el desarrollo de la humanidad. Pero estas innovaciones deben servir de incentivo para que el accionar del Estado vaya encaminado a proteger preventivamente los derechos de los ecuatorianos, como el de protección de datos personales, materia de estudio del presente trabajo.

En el presente estudio se ha evidenciado la necesidad de que, desde la misma redacción de sus políticas de privacidad, los proveedores de servicios de *cloud computing,* ya deberían cumplir con los principios estándar que configuran debidamente un sistema preventivo del derecho a la protección de datos personales no solo para Ecuador, sino a nivel mundial. Este derecho, por ser de naturaleza compleja, solo podrá ser garantizado efectivamente por el ente estatal cuando se desarrollen y reconozcan sus elementos esenciales, y el principal de estos son los principios del derecho a la protección de datos personales que previenen posibles riesgos en casos como lo es el *cloud computing.*

Como se mencionó en el capítulo segundo, todas las funciones del Estado deben ser garantes de los derechos constitucionales, la Constitución del 2008 reconoce el derecho a la protección de datos personales de los ecuatorianos, que por ser un derecho complejo solo puede ser garantizado a través del desarrollo normativo de estándares que constituyen sus componentes esenciales. Proponemos entonces que, en atención a los riesgos detectados en el apartado 3.4.2 en el caso ejemplificativo de prestación de servicios B2C de *cloud computing* estudiado, a partir de las políticas de privacidad de Dropbox, el ente legislativo adopte medidas para velar por el desarrollo de sus principios, por medio de la implementación de una ley específica de protección de datos de carácter personal.

El derecho a la protección de datos personales por ser de naturaleza compleja se compone de varios elementos esenciales como: principios, garantías, derechos, entre otros. Como se ha venido evidenciando en este trabajo, la combinación de todos los componentes del derecho a la protección de datos personales generan un sistema preventivo y reactivo en conjunto.

Como se habló en el capítulo segundo, el *hábeas data* que existe en Ecuador constituye un mecanismo de garantía jurisdiccional, con el que ya se ha configurado en Ecuador un sistema reactivo de protección de datos personales. Con reactivo queremos hacer énfasis en que ya debía existir previamente un tratamiento de datos personales del usuario (ya se utiliza el servicio de *cloud computing*), y por lo tanto, la interposición de una acción de *hábeas data* solo puede ser realizada *a posteriori* al manejo de información.

Debido a que con el *hábeas data* la intervención del ente estatal se realiza de forma *ex-post* o reactiva, es decir, luego de algún incumplimiento en el tratamiento de datos, esto podría ser perjudicial cuando existe contratación B2C de servicios de *Cloud Computing* como la analizada en el caso ejemplificativo de Dropbox, por un lado, porque podrían causarse daños insubsanables a la información de los ecuatorianos (Melaños, 2013, p. 102), y, por otro lado, porque

para que exista un óptimo amparo preventivo del derecho a la protección de datos personales, los proveedores de servicios en la nube deben cumplir con requisitos y obligaciones que imponen los principios estándar definidos en el capítulo segundo, previo a realizar el tratamiento de la información de sus usuarios, es decir, deben sujetarse a normativa *ex-ante* o preventiva.

La garantía del *hábeas data* no es suficiente para prevenir posibles violaciones al derecho a la protección de datos personales de ecuatorianos, pues únicamente opera *a posteriori* del tratamiento de datos personales. Por no ser suficiente esta acción, el Estado deberá adoptar otras garantías para resguardar los derechos de los ecuatorianos.

Al ser un sistema reactivo el que se genera con el *hábeas data,* se sustenta la propuesta de este trabajo de desarrollar un sistema preventivo de protección de datos personales a través de la promulgación de una ley especial. Esa es la vía más adecuada para dar un debido amparo al derecho complejo, del numeral 19 del artículo 66 de la Constitución de la República, relativo a la protección de datos personales de los ecuatorianos.

Por todo lo mencionado en líneas previas, consideramos necesario que en Ecuador se implemente normativa que desarrolle el derecho a la protección de protección de datos personales. Únicamente una ley especial podría brindar definiciones claras de los principios estándar de protección de datos personales, analizados en el presente trabajo de titulación, y solo así será posible que en el Ecuador se ampare de forma adecuada a este derecho complejo.

Pero para implementar una ley que desarrolle a fondo el derecho a la protección de datos personales en el Ecuador, tendrán también que generarse varios debates en espacios académicos, políticos y jurídicos que briden ideas y pautas, para que el Estado ecuatoriano pueda amparar los derechos de sus habitantes incluso en casos de prestación de servicios tan novedosos como los de *cloud computing*.

Con el desarrollo de las tecnologías y nuevas innovaciones, como el *cloud coputing,* se va comprobando la importancia del derecho a la protección de datos personales y el papel elemental que juega la implementación de una ley específica que recoja y desarrolle todos los principios esenciales de este derecho.

Debemos ser realistas y hacer conocer al lector que el desarrollo de los principios de protección de datos personales en una ley específica ecuatoriana a pesar de ser vinculante y eficaz para proveedores de servicios de cómputo en la nube con domicilio o representante en Ecuador, no será el detonante para que en casos de empresas multinacionales como Dropbox se obligue a cambiar las políticas de privacidad que imponen a nivel mundial. Sin embargo, la implementación de este cuerpo normativo y el desarrollo de los principios del derecho a la protección de datos personales en su contenido harán conocer a los ecuatorianos los alcances de sus derechos y crearán conciencia social de los riesgos inmensos que implica aceptar políticas de privacidad de proveedores de servicios de *cloud compting* nacionales o internacionales como Dropbox.

Además, en Ecuador ya se están creando empresas que ofertan servicios de *cloud computing¸* y estarán obligadas a actuar conforme a una ley específica de protección de datos personales, así cuando estos proveedores de servicios de *cloud computing* recojan y traten la información de sus usuarios deberán regirse a un sistema preventivo de protección de datos personales en observancia de principios claramente definidos y desarrollados en la legislación ecuatoriana. Así estaremos desarrollando una buena cultura de protección de datos en los ecuatorianos, que empate con experiencias como la europea o la argentina, y poco a poco, en conjunto hagan fuerza frente a multinacionales inmensas como Dropbox, Google o Facebook.

Tanto el *cloud computing* como el derecho a la protección de datos personales son temas muy innovadores para la sociedad ecuatoriana, pero no por eso dejan de ser parte de nuestra realidad. Es hora de que el legislador actúe en pro de

los derechos de los ciudadanos, para marcar en Ecuador un antes y un después en desarrollo del derecho a la protección de datos personales. Debemos hacer fuerza ahora implementando una ley de protección de datos personales, para que así, junto con otros países pertenecientes a la Red Internacional de Protección de Datos, se promueva que los datos de las personas sean protegidos a nivel mundial. Hay que dejar de hacer caso omiso a los riesgos que existen para los usuarios de *cloud computing* en el mundo entero por miedo a enfrentarnos a grandes como Dropbox, Facebook o Google; solo así estos usuarios reforzarán su confianza en las tecnologías, lo que permitirá el constante desarrollo y expansión de sus maravillosas innovaciones como lo es el *cloud computing.*

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

1. El *cloud computing* o nube de cómputo es un modelo innovador compuesto por un conjunto de *hardware*, *software* e interfaces destinados a la prestación de servicios innovadores por medio de internet. Este paradigma se compone de cinco características esenciales que definen su naturaleza. Tiene tres modelos de servicios y cuatro modelos de implementación, que son independientes unos de otros y se identifican con las mismas características del *cloud computing*.

2. En este trabajo se ha expuesto un ciclo de vida de datos del *cloud computing* destinado a definir fases generales, de conformidad con las distintas funciones que podrá desempeñar el proveedor de servicios, respecto de la información de sus usuarios. Las fases del ciclo de vida de los datos en la nube siempre serán las mismas, pero no se rigen a un orden cíclico, pueden presentarse indistintamente, su finalidad es simplemente la de atribuir responsabilidades al proveedor de servicios de *cloud computing* de acuerdo a las funciones que éste puede realizar en cada fase.

3. El derecho a la protección de datos personales es independiente y complejo, y para ser tutelado efectivamente, precisa del reconocimiento de otros derechos, principios, garantías y deberes que conjuntamente lo componen. Además, el derecho a la protección de datos personales impone obligaciones a los responsables y encargados de tratamiento de datos, para que en el desempeño de sus actividades resguarden de forma preventiva este derecho.

4. En la relación B2C generada en la prestación de servicios de *cloud computing* existen contratos electrónicos de adhesión que facultan a sus proveedores a tratar información personal de sus usuarios (políticas de privacidad). Los proveedores en la redacción de dichas políticas deberían ceñirse de forma preventiva a la normativa ecuatoriana vigente relativa a defensa al

consumidor, contratación electrónica, y teniendo presente el derecho constitucional a la protección de datos personales de los ecuatorianos.

5. El Estado ecuatoriano, como garante de los derechos constitucionales, debe velar porque se proteja el derecho a la protección de datos personales reconocido a los ecuatorianos en la Constitución del 2008. Derecho que por ser de naturaleza compleja, debe ser garantizado a través del desarrollo normativo de todos sus elementos esenciales, entre estos los principios estándar que configuran un sistema preventivo de protección de datos personales.

6. Del estudio ejemplificativo de las políticas de privacidad que estipula Dropbox, en relaciones B2C por el uso de sus servicios en la nube, se puede concluir que, para prevenir posibles violaciones al derecho a la protección de datos personales de sus usuarios sería preciso que en la redacción de todas las cláusulas de sus políticas de privacidad se ciña a diversos principios estándar que constituyen elementos esenciales del derecho a la protección de datos personales.

7. Del análisis ejemplificativo realizado a las políticas de privacidad de Dropbox, se han detectado varios riesgos para los usuarios, que ponen en manifiesto la necesidad de implementar en Ecuador normativa que genere un sistema preventivo, a través del desarrollo de principios estándar del derecho a la protección de datos personales.

8. Debido a que la garantía del *hábeas data,* por únicamente operar *a posteriori* (sistema reactivo), no es suficiente para prevenir posibles violaciones al derecho a la protección de datos personales ecuatoriano, desde el momento de la redacción de políticas de privacidad de servicios de cómputo en la nube. Por no ser suficiente esta acción, el Estado deberá adoptar otras garantías para resguardar los derechos de sus habitantes, puntualmente para evitar los riesgos que se generan por relaciones B2C en la prestación de servicios de *cloud computing*.

9. Se ha evidenciado la necesidad de implementar en el Ecuador una ley que reconozca en su complejidad al derecho a la protección de datos personales, otorgado a los ecuatorianos con la actual constitución. Esta necesidad se ve reflejada en proyectos legislativos, en el reconocimiento formal de este derecho a nivel constitucional, en la implementación del *hábeas data* dentro de la legislación ecuatoriana, y en la obligación del Estado de garantizar efectivamente de forma preventiva y reactiva el derecho a la protección de datos personales, reconocido en la constitución ecuatoriana para sus ciudadanos.

10. Aunque el desarrollo de los principios de protección de datos personales en una ley específica ecuatoriana no sea el detonante para que en el caso ejemplificativo de Dropbox este proveedor de servicios de *cloud computing* cambie sus políticas de privacidad impuestas a nivel mundial. La implementación de este cuerpo normativo y el desarrollo de los principios del derecho a la protección de datos personales en su contenido, por un lado, tendrá eficacia y efectividad inmediatas para proveedores de servicios de *cloud computing* con domicilio o representante en Ecuador; y por otro lado, harán conocer a los ecuatorianos los alcances de sus derechos, creando así conciencia social de los riesgos inmensos que implica aceptar políticas de privacidad de proveedores de servicios de *cloud compting* como Dropbox o Google.

4.2 Recomendaciones

1. Se recomienda que la función legislativa del Ecuador promulgue una Ley de Protección de Datos Personales; el contenido de esta ley debería ser desarrollado tomando como referente a experiencias internacionales, y criterios que generen un sistema preventivo de protección de datos personales. Con la promulgación de un cuerpo normativo que desarrolle el derecho a la protección de datos personales en Ecuador será preciso que el contenido de este defina de forma clara y específica los principios estándar

del derecho a la protección de datos personales, para así generar un sistema preventivo de protección de datos personales en el Ecuador.

2. Debido a que la inobservancia de los principios estándar del derecho a la protección de datos personales en redacción de las políticas de privacidad que Dropbox estipula para la prestación de servicios de *cloud computing* en relaciones B2C, genera una variedad de riesgos para los usuarios. Se recomienda implementar normativa de protección de datos personales que desarrolle y defina claramente los principios estándar para prevenir violaciones a este derecho.

3. Se recomienda que a futuro se realicen investigaciones que desarrollen más a fondo el tema del *cloud computing.* Por un lado en este trabajo de investigación se evidenció la necesidad de que se conozca a fondo la relación B2B (*Bussines to Bissines),* por la prestación de servicios de *cloud computing* y las implicancias que esta puede tener en el derecho a la protección de datos personales de los ecuatorianos. También para precautelar los derechos de los ecuatorianos, deberían ser analizadas las políticas de privacidad que estipulan otros proveedores de servicios de *cloud computing* como Facebook, Google, Skydrive, entre otros.

4. Para que el Estado ecuatoriano brinde una adecuada tutela al derecho a la protección de datos personales deberá implementar garantías institucionales a través de la creación de una institución controladora independiente dedicada exclusivamente a velar por el derecho en cuestión. Dicha autoridad deberá implementar medidas para que se genere un sistema preventivo del derecho a la protección de datos personales, para lo cual deberá tener autonomía frente a las funciones estatales y facultades sancionadoras.

REFERENCIAS

Aalbers, H. (2013). Una introducción al *cloud computing*. Madrid, España: Marcial Pons.

Acevedo, H. (2010). ¿Qué es cómputo en la nube?. Magazcitum. Recuperado el 18 de octubre de 2014 de http://www.magazcitum.com.mx/?p=866

Acuña, A. y Cordero, E. (2014). *Los contratos de shrinkwrap, clickwrapy browsewrap: Un enfoque desde la perspectiva del Derecho del Consumidor* (Tesis de grado, Universidad de Costa Rica, San José, Costa Rica). Recuperado el 01 de septiembre de 2015 de http://iij.ucr.ac.cr/sites/default/files/documentos/los_contratos_de_shrinkwrap_clickwrap_y_browsewrap_un_enfoque_desde_la_perspectiva_del_derecho_del_consumidor.pdf

Agencia Española de Protección de Datos. (2013). *El derecho fundamental a la protección de datos: Guía para el ciudadano.* Agencia Española de Protección de Datos. Recuperado el 22 de julio de 2014 de www.agpd.es

Agencia Española de Protección de Datos. (2013). *Guía para clientes que contraten servicios de cloud computing.* Agencia Española de Protección de Datos. Recuperado el 22 de julio de 2014 de www.agpd.es

Agencia Española de Protección de Datos. (2013). *Orientaciones para prestadores de servicios de cloud computing.* Agencia Española de Protección de Datos. Recuperado el 22 de julio de 2014 de www.agpd.es

Agencia Española de Protección de Datos. Informe 0457/2008. Obligación del responsable del tratamiento de datos de velar que el encargado

cumpla las medidas de seguridad. Recuperado el 30 de mayo de 2015 de http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/medidas_seguridad/common/pdfs/2008-0457_Obligaci-oo-n-del-responsable-del-tratamiento-de-datos-de-velar-que-el-encargado-cumpla-las-medidas-de-seguridad.pdf

Agencia Española de Protección de Datos. Informe 287/2006. Conceptos generales. Delimitación del responsable del fichero y del encargado del tratamiento. Recuperado el 3 de mayo de 2015 de http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2006-0287_Delimitaci-oo-n-del-responsable-del-fichero-y-del-encargado-del-tratamiento.pdf

Aguirre, V. (2010). El derecho a la tutela judicial efectiva: una aproximación a su aplicación en los tribunales ecuatorianos. *Revista de derecho*, Núm. 14. Recuperado el 10 de mayo de 2015 de http://repositorio.uasb.edu.ec/bitstream/10644/2976/1/03-Aguirre.pdf

Almuzarra, C., Marzo, A., Coudert, F. y Navalpotro, Y. (2005). *Estudio práctico sobre la protección de datos de carácter personal*. Valladolid, España: Editorial LEX NOVA S.A.

Apple Team. (2014). Política de privacidad de Apple. Recuperado el 1 de febrero de 2015 de https://www.apple.com/icloud/

Armagnague, J. (2002). El derecho comparado en la protección de datos. En M., Ábalos y O., Arrabal (Coords.), *Derecho a la información, hábeas data e Internet*. Buenos Aires, Argentina: La Rocca.

Article 29 Data Protection Working Party. (2008). *Working Document Setting up a framework for the structure of Binding Corporate Rules*. Brucelas, Bélgica. Recuperado el 1 de febrero de 2015 de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_en.pdf

Ávila R., Grijalva A. y Martínez D. (2008). *Desafíos constitucionales: La Constitución ecuatoriana del 2008 en perspectiva.* Quito, Ecuador: Ministerio de Justicia y Derechos Humanos.

Balboni, P. (2010). Data Protection and Data Security Issues Related to Cloud Compunting in the EU. *Social Science Research Network Electronic Paper Collection.* Recuperado el 10 de diciembre de 2014 de file:///C:/Users/Princess%20Novoa/Downloads/SSRN-id1661 437.pdf

Barnitzke, B., Corrales, M., Forgó, N. (2011). *Aspectos legales de la Computación en la Nube (1.ª ed.).* Buenos Aires, Argentina: Albermática.

Bazán, V. (2012). El hábeas data, su autonomía respecto al amparo y la tutela del derecho fundamental de autodeterminación informativa. *Anuario de Derecho Constitucional Latinoamericano,* 37-76. Recuperado el 5 de noviembre de 2014 de http://www.juridicas.unam.mx/publica/ librev/rev/ dconstla/cont/2012/pr/pr4.pdf.

Bluzebra Technologies (s.f.). *Technology of tomorrow cloud computing.* Tics y formación. Recuperado el 29 de Agosto de 2015 de http://ticsyformacion.com/2013/04/14/cloud-computing-la-tecnologia-del-manana-infografia-infographic/

Briggette, C. (2011). *Cloud Computing* 101: Public Vs Private Clouds. *IT Consultants' Insight On Business Technology NSK Inc*. Recuperado el 03 de abril de 2015 de http://blog.nskinc.com/IT-Services-Boston/bid/56863/Iron-Mountain-Paper-Not-Plastic

Cámara Nacional en lo Civil. Sala D. Caso Lascano Quintana C. Veraz. Fallo de 23 de febrero de 1999.

Cerda, P. (2012). Qué es el *cloud computing* y cuáles son sus ventajas. *Tecnologías aplicadas.* Recuperado el 14 de mayo de 2014 de http://patriciocerda.com/2012/01/que-es-el-cloud-computing-y-cuales-son.html

Cesario R. (2001). *Hábeas data*. Buenos Aires, Argentina: Editorial Universidad.

Ciphercloud. (2013). *Where is your data?* The cloud infographic. Recuperado el 29 de Agosto de 2015 de http://www.thecloudinfographic.com/2015/05/04/legal-issues-that-affect-moving-information-to-the-cloud.html

Clarke, I., Miller, S., Hong, T., Sandberg, O., & Wiley, B. (2002). Protecting Free Expression Online with Freenet. *Journal IEEE Internet Computing, núm. 6*, 40-49. Recuperado el 20 de mayo de 2014 de https://freenetproject.org/papers/freenet-ieee.pdf

Clarke, R. (2013). Data risk in the Cloud. *Journal of theoretical and Applied Electronic Commerce Research*, Vol. 8, 59-73. Recuperado el 20 de octubre de 2014 de http://www.jtaer.com/

Clímaco, E. (2012). *"Génesis histórico-normativa del derecho a la protección de los datos personales desde el derecho comparado a propósito de su fundamento"* (Tesina de maestría, Universidad Carlos III de Madrid, Madrid, España). Recuperado el 20 de noviembre de 2014 de http://e-archivo.uc3m.es/bitstream/handle/10016/18785/TFM_MEADH_Ernesto_Climaco.pdf?sequence=1

Cloud Security Alliance (2011). *Cloud Compliance Report.* España. Recuperado el 20 de junio de 2015 de https://docs.google.com/viewer?a=v&pid=sites&srcid=Y2xvdWRzZWN1cml0eWFsbGlhbmNlLmVzfGNzYS1lc3xneDo2NWNhZWFiNTkwODI1N2I0

Código Civil. Registro Oficial 46 de 24 de junio de 2005.

Colom, J. (2012). *Cloud computing* y protección de datos personales. Regulando el desorden. *Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión*. Recuperado el 2 de febrero de 2015 de http://www.aspectosprofesionales.info/2012/05/cloud-computing-y-proteccion-de-datos.html

Conde, C. (2005). *La protección de datos personales: un derecho un derecho autónomo con base en los conceptos de intimidad y privacidad*. Madrid, España: DYKINSON.

Confederación de Empresarios de Andalucía. (2014). *Modelos de e-Business.* Confederación de Empresarios de Andalucía. Recuperado el 15 de julio de 2015 de http://www.cea.es/upload/ebusiness/modelos.pdf

Conferencia Internacional de Autoridades de Protección de Datos y Privacidad 31. (2009). Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Madrid, España. Recuperado el 10 de marzo de 2015 de https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/09-11-05_Madrid_Int_standards_ES.pdf

Constitución de la República del Ecuador, Registro Oficial 449 de 20 de octubre de 2008 y Registro Oficial 490, Suplemento de 13 de julio de 2011.

Contreras, M. (2015). *Dropbox ya tiene más de 400 millones de usuarios.* FayerWayer. Recuperado el 28 de agosto de 2015 de https://www.fayerwayer.com/2015/06/dropbox-ya-tiene-mas-de-400-millones-de-usuarios/

Corte Constitucional. *Sentencia 001-14-PJO-CC,* 23 de abril de 2014. Registro Oficial 007, Suplemento, de 3 de julio de 2014.

Cruz, K. (2012). *Historia del Cloud Computing*. RITS, núm. 7, 51-52. Recuperado el 10 de octubre de 2014 de http://www.revistasbolivianas.org.bo/pdf/rits/n7/n7a21.pdf

Davara, I. (2010). Protección de datos de carácter personal en México: problemáticas jurídicas y estatus normativo actual. En J. Corral y J. Peschard (Coords.), *Protección de datos personales*. México D.F., México: Tiro Corto Editores.

Davara, M. (2008). *Manual del derecho informático*. Madrid, España: ARANZADI.

De Miguel, P. (2011). *Derecho privado de Internet*. Navarra, España: Editorial Azandi.

Del Peso, Emilio. (2000). *Ley de Protección de Datos la nueva LORTAD.* Madrid, España: Ediciones Diaz de Santos S.A.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de las Comunidades Europeas No. L 281 /31.

Djemame, K., Jiang, M., Kiran, M., Amstrong, D., Barnitzke, B., Corrales, M., & Forgó, N. (2012). Inventario de riesgos de la computación en la nube: cuestiones legales. *El Dial Biblioteca Jurídica*, 1-2.

Dropbox Team. (2015). *Política de privacidad de Dropbox.* Recuperado el 7 de junio de 2015 de https://www.dropbox.com/privacy

Dropbox. (s.f.). *Planes de Dropbox.* Recuperado el 1 de febrero de 2015 de www.dropbox.com

Eclipse. (2015). *The Explosive Growth of Cloud Computing.* Cool infographics. Recuperado el 28 de agosto de 2015 de http://www.coolinfographics.com/blog/2014/5/5/the-explosive-growth-of-cloud-computing.html

Equipo de estudios del ONTSI. (2012). *Cloud Computing*, Retos y Oportunidades. *ONTSI.* Recuperado el 1 de abril de 2014 de http://www.ontsi.red.es/ontsi/sites/default/files/1_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf

Escamilla, J. (2012). *Antecedentes*. *Cloud computing* blog. Recuperado el 14 de octubre de 2014 de http://cloud-fi.blogspot.com/ 2012/11/ antecedentes-cloudcomputing-no-es-un.html

Fernández, J. (s.f.). Protección de datos personales y *cloud computing*. Proactivanet. Recuperado el 2 de febrero de 2015 de http://www.proactivanet.com/blog/it-service-management/proteccion-de-datos-personales-y-cloud-computing/

Freixas, G. (2001). *La protección de los datos de carácter personal en el derecho español.* Barcelona, España: Editorial Bosch, S.A.

Galindo, I. (1981). *Estudios de derecho civil.* México D.F., México: Universidad Autónoma de México.

Gamen, S. (2013). Sobre llovido mojado. *Cloud computing*: el tiro de gracia a la privacidad. *Eldial Biblioteca Jurídica, 1-3*.

García, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín mexicano de derecho comparado*, num. 120, 743-778. Recuperado el 5 de noviembre de 2014 de http://www.juridicas.unam.mx/publica/rev/boletin/ cont/120/ art/art3.htm.

Granero, H. (2014). Problemas legales del *cloud computing*. *Eldial Biblioteca Jurídica*, 1-2.

Grupo de Trabajo sobre Protección de Datos. (2013). Documento de observaciones de CEOE sobre la Propuesta de Reglamento General de protección de datos. *Confederación Española de Organizaciones Empresariales*. Recuperado el 2 de febrero de 2015 de http://www.ceoe.es/resources/image/documento_observaciones_ceoe_propuesta_reglamento_tratamiento_datos_2013_02_12.pdf

Grupo del artículo 29 sobre protección de datos. (2010). Dictamen 1/2010 sobre los conceptos de responsable del tratamiento y encargado del tratamiento. Brucelas, Bélgica. Recuperado el 4 de febrero de 2015 de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf

Guerrero, M. (2006). *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*. Navarra, España: Editorial Azandi.

Herrán, A. (2002). *El derecho a la intimidad en la nueva Ley Orgánica de Protección de datos personales.* Madrid, España: Editorial DYKINSON S.L.

Hurwitz, J., Kaufman, M., Halper, F. (2012). *Cloud Services for dummies*. United States, New Jersey: John Wiley & Sons, Inc.

Hustinx, P. (2010). Data Protection and *Cloud Computing* under EU law. *En Third European Cyber Security Awareness Day*, Parlamento Europeo, Bruselas.

Instituto Nacional de Estándares y Tecnología. (2013). La definición de *Cloud Computing* de NIST. *NIST.* Recuperado el 10 de octubre de 2014 de

http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

Instituto Nacional de Estándares y Tecnología. (2011). *La definición de Cloud Computing de NIST.* NIST. Recuperado el 19 de septiembre de 2014 de http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Instituto Nacional de Tecnologías de la Comunicación. (2011). *Guía para empresas: seguridad y privacidad del cloud computing.* INTECO. Recuperado el 20 de julio de 2014 de www.inteco.es

International Telecommunication Union. (2012). *Privacy in Cloud Computing. ITU-T Tecnology Watch Report*. Recuperado el 17 de mayo de 2014 de http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf

Internet Governance Forum. (2010). *Cloud computing for leaner and greener IT infrastructures in governments (and businesses).* Vilnius, Lithuania. Recuperado el 1 de febrero de 2015 de http://www.oecd.org/sti/ieconomy/45718361.pdf

Isaza, H. (2014). *El Amparo Informático Como Mecanismo Constitucional para una Tutela Efectiva de los Derechos Fundamentales en la Internet*. Bogotá, Colombia: Ediciones Nueva Jurídica.

IT Consultants' Insight On Business Technology. (s.f.). "Hybrid Clouds-The Best of Both Worlds". *NSK Inc.* Recuperado el 03 de abril de 2015 de http://blog.nskinc.com/hybrid-clouds-the-best-of-both-worlds?bi_campaign=Brightinfo&bi_medium=referral&bi_source=app.brightinfo.com

Joyanes, L. (2012). Computación en la nube. *Revista del Instituto Español de Estudios Estratégicos,* Núm. 00, 87-110. Recuperado el 19 de

septiembre de 2014 de http://dialnet.unirioja.es/servlet/articulo?codigo=4098278

Joyanes, L. (2012). *Computación en la nube: estrategias del cloud computing en las empresas.* México, México D.F.: Alfaomega.

Kerr, J., & Teng, K. (2012). Cloud computing: legal and privacy issues. *Journal of Legal Issues and Cases in Business*. Núm. 1, 1-9. Recuperado el 5 de abril de 2014 de http://www.aabri.com/manuscripts/111064.pdf.

Kesan, J., & Bashir, M. (2011). Privacy in the Cloud, Going Beyond the Contractarian Paradigm. *Annual Computer Security Applications Conference*. Recuperado el 25 de abril de 2014 de http://www.acsac.org/2011/workshops/gtip/Bashir.pdf

Khang, W. (2014). Cloud computing solutions: iaas, paas, saas. *WPTidBits.* Recuperado el 02 de abril de 2015 de http://wptidbits.com/techies/cloud-computing-solutions-iaas-paas-saas/

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Registro Oficial 557 de 17 de abril de 2002.

Ley del Sistema Nacional de Registro de Datos Públicos. Registro Oficial 162, 31 de marzo de 2010.

Ley Orgánica de Defensa del Consumidor. Registro Oficial 116 de 10 de julio de 2000.

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. Registro Oficial 52 de 22 de octubre de 2009.

Ley Orgánica de Protección de Datos de Carácter Personal española 15/1999 de 13 de diciembre. Boletín Oficial del Estado Núm. 298, de 14 de diciembre de 1999.

López Carballo, D. (2014). "Protección de datos y *hábeas data* en la legislación ecuatoriana: presente y futuro". *Revista Latinoamericana de Protección de Datos Personales.* Recuperado el 11 de diciembre de 2014 de http://www.rlpdp.com/2014/03/lopez-carballo-proteccion-de-datos-y-habeas-data-en-la-legislacion-ecuatoriana-presente-y-futuro/#_ftn1

López-Vidriero, I. y Santos, E. (2005). *Protección de datos personales manual práctico para empresas.* Madrid, España: Fundación Confemetal.

Lucas, P. (2008). El derecho a la autodeterminación informativa y la protección de datos personales. *Azpilcueta,* núm. 20, 43-58. Recuperado el 17 de febrero de 2015 de http://www.euskomedia.org/PDFAnlt/azpilcueta/20/20043058.pdf

Martínez, R. (2004). *Aproximación crítica a la autodeterminación informativa*. Madrid, España: Editorial Azandi.

Marzo, A. (2012). Privacidad y *cloud computing*, hacia dónde camina Europa. *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*, vol. I (núm. 8), 202-229. Recuperado el 31 de enero de 2015 de https://revistasocialesyjuridicas.files.wordpress.com/2012/02/08-tm-12.pdf

Mazuecos, A. (2013).*Breve historia del Cloud Computing*. Make soft tecnologies blog en la nube. Recuperado el 14 de octubre de 2014 de http://makesofttechnologies.blogspot.com/2013/05/breve-historia-del-cloud-computing.html

Melaños, C. (2013). *Análisis de los riesgos técnicos y legales de la seguridad en el cloud computing* (Tesis de maestría, Universidad Politécnica de Madrid, España). Recuperado el 19 de junio de 2015 de http://repositorio.educacionsuperior.gob.ec/bitstream/28000/1202/1/T-SENESCYT-000333.pdf

Miralles, R. (2010). *Cloud computing* y Protección de datos. *Revista de Internet, Derecho y Política*, núm. 11. Recuperado el 15 de mayo de 2014 de http://idp.uoc.edu/index.php/idp/article/view/n11-miralles/n11-miralles

Mohamed, A. (2009). *A history of cloud computing.* Computerweekly. Recuperado el 14 de octubre de 2014 de http://www.computerweekly.com/feature/A-history-of-cloud-computing

Molina, E. (2012). *Tratado de derecho informático*. Buenos Aires, Argentina: Ed. La Ley.

Naranjo, L. (2007). *La protección de datos personales en el CRM (Customer Relatioship Management)* (Tesis de maestría, Universidad Pablo de Olavide, Sevilla, España).

Navarro, M. [IBM Prensa]. (2009). *Cloud computing*: la visión de IBM (español) [*Archivo de video*]. Recuperado el 14 de octubre de 2014 de http://www.youtube.com/watch?v=5rBwfCf5LZE

Pérez Luño, A. (1996). *Manual de informática y derecho*. Barcelona, España: Editorial Ariel S.A.

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos. Procedimiento legislativo ordinario 2012/0011 (COD).

Puccinelli, O. (2004). *Protección de datos de carácter personal*. Buenos Aires, Argentina: Editorial Astrea.

Puente, X. (2010). La protección de datos personales en posesión de particulares en México: avances y desafíos. *XIV Congreso Iberoamericano de Derecho e Informática*. Recuperado el 15 de noviembre de 2014 de http://biblio.juridicas.unam.mx/libros/6/2941/26.pdf

Quintana, A. (2004). Introducción. *Revista arazandi de derecho y nuevas tecnologías, núm. 2, 25-43*

QuoteColo. (2015). *Cloud computing predictions for 2015 [Infographic].* Spacetel. Recuperado el 28 de agosto de 2015 de http://spacetel.co.uk/spacetel-insights/cloud-computing-predictions-for-2015-infographic/

Real Academia de la Lengua. (2014).”Intimidad” en Diccionario de la lengua española. *Real Academia de la Lengua*. Recuperado el de 29 noviembre de 2014 de http://lema.rae.es/drae/?val=intimidad

Redacción de Baquía. (2006). Intimidad, privacidad y protección de datos de carácter personal. *Baquía.* Recuperado el 30 de noviembre de 2014 de http://www.baquia.com/tecnologia-y-negocios/entry/emprendedores/intimidad-privacidad-y-proteccion-de-datos-de-caracter-personal

Reis, D. (2013). *Seguridad para la nube y la virtualización for Dummies*. United States, New Jersey: John Wiley & Sons, Inc.

Rengifo, E. (2013). Computación en la nube. *Revista la propiedad inmaterial*, Núm. 17, 223-245. Recuperado el 11 de septiembre de 2014 de

http://revistas.uexternado.edu.co/index.php?journal=propin&page=article&op=view&path%5B%5D=3587&path%5B%5D=3668

Research Centre on IT and Law. (2010). *Cloud computing and its implications on data protection*. Strasbourg, Francia. Recuperado el 10 de diciembre de 2014 de http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_y vespoullet1b.pdf

Rojas, V. (2007). El perfeccionamiento del consentimiento en la contratación electrónica. *Revista de Derecho Privado, Núm. 16-17.* Recuperado el 31 de agosto de 2015 de http://www.juridicas.unam.mx/publica/librev/rev/derpriv/cont/16/dtr/dtr6.pdf

Ryan, M. (2011). Cloud Computing Privacy Concerns on Our Doorstep. *Communications of the ACM*, Vol. 54 (Núm. 1), 36-38. Recuperado el 2 de febrero de 2015 de https://www.cs.bham.ac.uk/~mdr/research/papers/pdf/ 11-cacm.pdf

Salas, M. y Colombo, L. (2012). Cloud Computing: A review of Paas, IaaS, SaaS services and providers. *Revista Lámpsakos,* Núm. 07, 47-57. Recuperado el 19 de septiembre de 2014 de http://dialnet.unirioja.es/descarga/articulo/4490150.pdf

Salmón, C. (s.f.). Régimen Procesal del Hábeas Data en el Ecuador. *Revista Jurídica, Facultad de Derecho, Universidad de Guayaquil,* 133-188. Recuperado el 20 de noviembre de 2014 de http://www.revistajuridicaonline.com/images/stories/revistas/2008/24/24-regimen-procesal-del-habeas.pdf

Saltor, C. (2013). *La protección de datos personales: Estudio comparativo Europa-América con especial análisis de la situación argentina* (Tesis

doctoral, Universidad Complutense, Madrid, España). Recuperado el 20 de febrero de 2015 de http://eprints.ucm.es/22832/1/T34731.pdf

Sánchez, A. (1998). *La protección del derecho a la libertad informática en la Unión Europea*. Sevilla, España: Universidad de Sevilla, Secretariado de publicaciones.

Santos, D. (2005). *Nociones generales de la Ley Orgánica de Protección de Datos.* Madrid, España: Editorial Tecnos.

Sarango, C. (2013). *Reformas para garantizar los derechos de los usuarios o consumidores de servicios electrónicos* (Tesis de grado, Universidad Nacional de Loja, Loja, Ecuador). Recuperado el 30 de agosto de 2015 de http://dspace.unl.edu.ec/jspui/handle/123456789/4505

Schwabe, J. (2009). Jurisprudencia del Tribunal Constitucional Federal Alemán, Extractos de las sentencias más relevantes compiladas por Jürgen Schwabe. *Fundación Konrad Adenauer Stiftung*. Recuperado el 2 de diciembre de 2014 de http://www.kas.de/wf/doc/kas_16817-544-4-30.pdf

Serrano, M. (2003). *El derecho fundamental a la protección de datos*. Madrid, España: Editorial Azandi.

Skytap. (2011). Desmitificando SaaS, PaaS e IaaS. *Skytap.* Recuperado el 20 de octubre de 2014 de http://www.skytap.com/blog/ demystifying-saas-paas-and-iaas

Strickland, J. (2008). How Cloud Computing Works. *HowStuffWorks.* Recuperado el 01 de abril de 2015 de http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm

Tecayehuatl, E. (2012).*El origen de: cómputo en la nube.* FayerWayer. Recuperado el 14 de octubre de 2014 de http://www.fayerwayer.com/ 2012/01/el-origen-de-el-computo-en-la-nube/

Téllez, V. (2013). *Lex cloud computing*. México, México D.F.: Instituto de Investigaciones Jurídicas UNAM.

TGG Legal. (2013). *Cloud computing* y sus implicaciones jurídicas. *Circular informativa mercantil.* Recuperado el 12 de octubre de 2014 de http://www.tgglegal.es/wp-content/uploads/2013/04/TGG_CIRC_03_ 13_BCN1.pdf

The Economist. (2008). Let it rise. *The economist.* Reccuperado el 3 de septiembre de 2014 de http://www.economist.com/ node/12411882

Trujillo, J. y Ávila, R. (2008). Los derechos en el proyecto de Constitución. En Instituto Latinoamericano de Investigaciones Sociales (Coord.), *Análisis: Nueva Constitución.* Quito, Ecuador: Friedrich Ebert Stiftung y La Tendencia.

Ureña, N. (2004). Desafíos Jurídicos de los Servicios de Computación en la Nube. *Eldial Biblioteca Jurídica, 1-2.*

V3. (2015). *Top 10 cloud computing risks and concerns.* V3, Recuperado el 29 de agosto de 2015 de http://www.v3.co.uk/v3-uk/news/2343547/top-10-cloud-computing-risks-and-concerns/page/5

Vizcaíno, M. (2001). *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal.* Madrid, España: Civitas Ediciones, S.L.

Winkler, V. (2013). *Cloud Computing*: Privacy, confidentiality and the cloud. *Technet Mahazine*. Recuperado el 20 de mayo de 2014 de http://technet.microsoft.com/en-us/magazine/dn235775.aspx

ANEXOS

Anexo 1. Entrevista Dr. José Luis Barzallo

Nombre del entrevistado: Dr. José Luis Barzallo

Nombre del entrevistador: Eugenia Novoa

Tema: El *cloud computing* y el derecho a la protección de datos personales en Ecuador

Lugar y fecha de la entrevista: Quito, 15 de mayo de 2015

Tiempo de duración: 15 min 06 seg

1. ***Podría detallar ampliamente ¿en qué consiste la característica de "servicio supervisado" del cloud computing y cómo opera la misma?***

   El servicio supervisado de *cloud computing* es prestado por algunas empresas como un servicio específico, que generalmente tiene un costo adicional, y en relación al cliente implica el conocimiento de la información que tiene en sus servidores. Esta supervisión desde el punto de vista comercial tiene dos implicaciones, la primera es que las empresas que brindan este servicio ofrecen el conocimiento detallado respecto de qué es lo que está almacenado en sus servidores, y por ende, deducimos que ellos deberían conocer lo que tiene ahí y lo que están manejando. Y por el otro lado, está el manejo de la información, para efectos de seguridad, la información que uno les brinda y que ellos como parte de su servicio ampliado, lo que hacen es decir "yo tengo estos archivos suyos y se los voy a mantener de esta o de esta, u otra forma".

   Adicionalmente, en lo que concierne o se vincularía con la protección de datos personales, el manejo de los datos de los individuos, entonces ellos manejan esa información, tienen conocimiento y podrían incluso hasta procesarla con autorización del titular.

Entonces, ¿podría incluir un tratamiento de datos extra?

No tanto, ellos no se preocupan por el tratamiento de datos extra, el tratamiento de datos que dan es de los intereses de la empresa que brinda el servicio, sino más bien, el servicio extra está por ejemplo en: recuperación de archivos, cuidado de archivos, notificaciones respecto de cambios que pueden haber.

Pero no nos olvidemos que el *cloud computing* no está destinado exclusivamente al archivo de datos personales, sino es un servicio genérico, que al momento en el cual yo establezco una relación con esta empresa tenga que proporcionar ciertos datos, es muy diferente. Entonces, hay que diferenciar eso, para no confundirnos. Es decir, el *cloud computing* me guarda mis datos personales, como parte de cien mil otros datos, también lo hace con respecto de los personales

2. ***En el desarrollo de la investigación se ha acogido y expuesto ampliamente las diferencias entre las figuras de responsable y encargado de tratamiento de datos personales.***

   Sin embargo, en un conversatorio relativo al derecho a la protección de datos personales el expositor indicó que en Europa ya no existen diferencias entre encargado y responsable de tratamiento de datos. El expositor supo manifestar que ahora solo hay un responsable frente a los titulares de datos, independientemente de los subcontratos que este celebre para prestar sus servicios.

   ¿Sabe usted si en realidad dicha aseveración tiene fundamentos en algún cuerpo normativo europeo o no tiene conocimiento de esto

   No, no tengo conocimiento de esto cambios que se han producido en la legislación europea, tal vez se está unificando o manejando de otra forma la terminología, pero cambio normativos al respecto no.

3. ***El derecho de autodeterminación informativa ¿es un sinónimo de libertad informática, o existen distinciones entre ambas?***

Definitivamente existen distinciones, son figuras totalmente diferentes. La autodeterminación informativa es una figura que se ha venido desarrollando en el transcurso del tiempo desde podríamos decir 1890, cuando se escribe el primer trabajo sobre el derecho a mantener la información propia alejada de las demás personas de Warren y Brandeis.

El derecho a la autodeterminación informativa sigue la línea de los derechos de la persona, el individuo tiene la opción para decidir qué hacer con su información, tiene la libertad para decidir qué come, qué bebe, y qué informa. Mientras que la libertad informática es un término muy genérico y ambiguo que puede llevar hacia lo que es la neutralidad tecnológica, hacia lo que puede ser el ejercicio de ciertos derechos a nivel informático, es decir a nivel de selección. Porque aquí también tenemos que identificar que la palabra informática está referida a lo que es el manejo y procesamiento de la información por medios digitales.

Entonces, si bien es un término que nos puede resultar bastante genérico, pero también dentro del espectro relacionado con el uso de la tecnología. La autodeterminación nos lleva a los ejemplos de libertad de expresión, donde hablamos de pornografía, el uso de armas Estados Unidos y algunos otros tópicos que ya han sido analizados a nivel internacional.

4. ***¿Por qué se considera al modelo de reconocimiento del derecho a la protección de datos latinoamericano como un híbrido de los modelos europeo y estadounidense?***

Para responder esta pregunta quisiera que inicie comentándome si usted considera que existe un modelo latinoamericano de protección de datos personales

Si, el modelo latinoamericano de protección de datos personales se deriva directamente del derecho de *hábeas data* desarrollado en nuestras legislaciones en Latinoamérica, es de ahí de donde parte, pese a existir el derecho a la protección de datos personales como un derecho ya individual en Europa y claramente determinado. En Latinoamérica lo que se hizo es, a falta de legislación que trate sobre el tema, acoplar y adaptar las normas que se tenían del habeas data a la protección de datos personales.

¿Es un híbrido?

Si es un híbrido, y yo creo que es un híbrido. Bueno, porque no es tan estricto o tan exagerado como el derecho de la protección de datos europeo. Sin decir por esto que el europeo sea malo, sino que nosotros por la cercanía que tenemos con los Estado Unidos de América, obviamente manejamos ese pensamiento mucho más liberal respecto del manejo de la información, y por el otro lado, como derecho jurídico, derecho continental, manejamos la línea europea. Pero a mí me gusta el latinoamericano definitivamente, aunque algunos países no han terminado de desprenderlo del *hábeas data*, de todas maneras me parece bueno.

…y cree que el Ecuador debería seguir la línea del modelo latinoamericano

Si creo que el Ecuador debería seguir esa línea de pensamiento jurídico, y que es precisa mente esa combinación de la teoría norteamericana con la teoría europea.

En realidad existe normativa argentina que a mi criterio es muy similar a la europea, pero también hay casos como el colombiano o mexicano que se distinguen entre sí. Entonces como modelo de protección de datos personales me parece que si difiere de país a país.

Sí, pero de todas maneras, por ejemplo en el caso argentino que efectivamente es más similar al europeo no llega a ser tan estricto. Entonces no tienes ese terror en las empresas respecto del responsable y encargado del manejo de los datos personales., no lo tienes, si, normativamente estableces ciertos parámetros, pero en la práctica no lo tienes.

México pese a tener una Ley nueva que ha puesto en orden a los mexicanos y que obviamente tienen que establecer registros e identificar los ficheros o los archivos y demás, tampoco llaga a ser tan estricta como lo es la española, que es casi el tope en lo rígido de este tema.

5. ***Por ser el derecho a la autodeterminación informativa el núcleo del derecho a la protección de datos personales, ¿ambos derechos son equiparables, o se diferencian entra sí?***

Se diferencian, y de hecho hace un momento mencioné el tema de la autodeterminación informativa en el tema de libertad de expresión. Donde también se lo considera un derecho importante que forma parte de la libertad de expresión y a la vez también de la protección de datos personales, entonces es un derecho independiente.

6. ***¿De qué forma concibe el modelo latinoamericano de protección de datos personales al dato con respecto a su titular?***

Se lo considera como un derecho, intrínseco al titular en Argentina, Mexico, Colombia, no como un bien jurídico. Lo seguimos manejando como un derecho incluso la fuente primaria y desarrollo de este derecho esta en las constituciones de dichos países.

Entonces, en este punto, no nos asemejaríamos al modelo estadounidense

No, porque esa es la conceptualización, y es en estos detalles en los que nos asemejamos a los europeos, seguimos la línea de pensamiento continental europea al considerarlo como un derecho. Y en la aplicación es en donde nosotros nos inclinamos por la línea norteamericana o anglosajona.

No, el *hábeas data* no es suficiente, porque si bien podemos ya ejercer el derecho, necesitamos establecer cuáles son estos parámetros. Porque en este momento dato personal es si me gusta o no jugar al futbol, pero no es sensible y no es pertinente, o es pertinente a qué.

Entonces, si no tenemos esa determinación estamos jugando a que la protección de datos personales se convierta en un instrumento de riesgo para los ecuatorianos.

Ahora, si damos una interpretación correcta sobre esto y tomamos lo que nos dice la Constitución respecto de la información que es protegida y que no se puede dar a terceros que es: sexo, salud, política y religión, entonces estamos en la línea correcta. Y si hablamos de acceso a la información añadiríamos datos migratorios y étnicos.

7. ***Finalmente, usted cree que cuando se implemente normativa de protección de datos personales en Ecuador, es importante, para que esta sea actual, conforme al avance tecnológico que se implementen pautas específicas que contemplen casos específicos que podrían generarse por el uso de servicios de cloud computing.***

   Sí, pero un si condicionado a que esas pautas sean acordes con la realidad jurídica y la practica o costumbre de los ecuatorianos.
   Que sean reales y no tan doctrinarias.

Anexo 2. Entrevista Dra. Lorena Naranjo

Nombre del entrevistado: Dra. Lorena Naranjo

Nombre del entrevistador: Eugenia Novoa

Tema: El *cloud computing* y el derecho a la protección de datos personales en Ecuador

Lugar y fecha de la entrevista: Quito, 31 de julio de 2015

Tiempo de duración: 12 min 23 seg

1. **Podría explicar cuál es la diferencia sustancial para usted entre la corriente de protección de datos europea y la corriente latinoamericana (*hábeas data*)**

   En el mundo existen tres corrientes claramente diferenciadas: la primera es la corriente europea, donde se reconoce al derecho a la protección de datos personales como un derecho humano de corte constitucional que permite el desarrollo de la personalidad, y por eso concibe a los datos de titularidad y como un elemento que conforma la personalidad del individuo. La segunda es la corriente estadounidense o norteamericana, en la que se concibe a los datos de carácter personal como bienes de propiedad de las personas, no como parte de su identidad, ni de su titularidad, sino que se refieren a la posibilidad de que estos datos puedan ser transferidos, cedidos, tratados, en la medida en que conformen bases de datos que logren el intercambio de información y recursos económicos en movimiento. Finalmente, la tercera es la corriente latinoamericana que toma una postura intermedia entre estas dos posiciones, pues acepta que, luego de una larga discusión entre intimidad, privacidad y protección de datos personales como derecho autónomo, este se convierte en un derecho de reconocimiento constitucional en casos como el ecuatoriano, o reconocimiento legislativo en el caso de Argentina. Y le otorga

otros elementos constitucionales que permiten brindar protecciones específicas a través del habeas data. Esta corriente también toma en consideración ciertas prácticas americanas, como códigos de conductas, prácticas de buena fe, y principios de puerto seguro.

Tipo de protección del hábeas data

La protección de datos personales tiene tres regímenes de forma de tutela del derecho: el primero es el de tutela básica, ante juzgados ordinarios, operara para el reconocimiento de una omisión en el cuidado de los datos, este régimen existe en Europa. El segundo sistema es el de acciones administrativas a través de las que brinda protección el Estado, estas acciones operan en una esfera reactiva y una preventiva, intentando regular de forma preventiva para evitar daños, así como sancionarlos en caso de producirse. Finalmente, tenemos al sistema desarrollado en Latinoamérica que es el de *hábeas data*. Tal como está concebido en las constituciones latinoamericanas es de primero y de ultimo nivel, es decir, se puede activar directamente por medio de una acción jurisdiccional frente a una transgresión. Sin embargo este es un sistema de clausura, que solo puede usarse cuando hay un inminente peligro o una transgresión específica, y en ese sentido solo opera cuando ya se ha producido el daño, es por eso que la garantía del *hábeas data* constituye un mecanismo reactivo para defender derechos como la intimidad, protección de datos personales, honor imagen, entre otros.

2. Podría detallar Qué garantías configuran para usted el derecho a la protección de datos personales

El derecho a la protección de datos personales es el ejemplo típico de un derecho complejo, y es un derecho complejo porque no tiene un núcleo unívoco, sino que lo conforman varios principios, derechos e incluso garantías. Su desarrollo es constante en la medida en que la sociedad evoluciona.

El núcleo primigenio, aunque no único, de este derecho puede ser la autodeterminación informativa. Las personas pueden decidir qué datos entregan, con qué finalidad, siempre que hayan sido debidamente informadas, y que hayan dado su consentimiento para que estos sean tratados y utilizados. Si existe un abuso la persona puede retirar el permiso brindado previamente, o si ya no hay voluntad del titular de los datos, esta persona puede simplemente retirarlos, cancelarlos, actualizarlos u oponerse a su recogida o tratamiento. En todos estos casos se visualizan lo que en legislaciones de corriente europea reconocen como derechos ARCO (actualización, rectificación, cancelación u oposición), y que en otros lugares, especialmente en Latinoamérica se han reconocido a través de la acción de *hábeas data,* que tutela estos derechos a nivel jurisdiccional a través de una garantía jurisdiccional.

Igualmente, el derecho a la protección de datos personales se puede violentar por acción u omisión, y en consecuencia, es también una obligación del Estado procurar que no se produzcan los daños, para lo cual será preciso que establezca institucionalidad y regularización interna que determinen el no mal uso de los datos personales en sus sistemas de recogida, tratamiento, seguridad, etc.

3. Para usted cuál es la naturaleza del derecho a la protección de datos personales que lo diferencia de otros derechos

Como es hijo de la intimidad al principio se lo confundía como la recopilación de datos íntimos en bases informáticas. Paulatinamente nos dimos cuenta que, no solo por el avance de la tecnología y con los datos que se almacenan en bases públicas, que se producen abusos, sino que se puede violentar la información de las personas incluso en recogida en ficheros físicos.

En consecuencia, la protección datos personales comienza a independizarse y a encontrar autonomía de otros derechos en la medida en la que encuentra

un elemento de titularidad, de desarrollo de la personalidad, al descubrir que tenemos una identidad digital y que esta se encuentra almacenada en bases de datos. También podemos tener una identidad conformada en ficheros, y esta debe estar actualizada, no debe estar equivocada, y puede ser mal tratada o mal procesada. En cualquiera de estas situaciones hay la posibilidad de vulnerar derechos fundamentales. Entonces, el derecho a la protección de datos personales se aparta de la intimidad, debido a que para violentar esta es preciso que exista una agresión a la esfera íntima del individuo, mientras que el derecho a la protección de datos personales ampara al individuo y cómo este quiere construir o determinar su información en el mundo real y en el mundo virtual.

4. **Considera que en la actualidad hay un mal manejo de la información de los ecuatorianos debido a que los proveedores de servicios de *cloud computing* no reflejan en el contenido de sus políticas de privacidad lo dispuesto en el numeral 19 del artículo 66 de la Constitución de la República del Ecuador**

   Yo no quisiera hablar de mal manejo, pero sí debo decir que no hay normas claras que permitan tener una regulación transparente, y por lo tanto, tampoco hay una aplicación directa de estas por parte de uno de los tantos usuarios de *cloud computing* titulares de datos personales.

   En el Ecuador, si bien hay una norma constitucional, que recoge un buen contenido sobre protección de datos personales, no se ha logrado definir todos los principios y estándares que se encuentran desarrollados a nivel internacional y aplicarlos.

   En Ecuador, el *hábeas data* se utiliza como único mecanismo de protección de datos personales. Esta garantía jurisdiccional si bien evita transgresiones directas a través de los derechos de acceso, rectificación, cancelación y oposición; no permite proteger otros derechos que pueden verse conculcados

por la elaboración de perfiles con datos erróneos de las personas. Por lo que es indispensable nutrir de contenidos esenciales al derecho a la protección de datos personales a través de normativa, jurisprudencia, definición y aplicación de políticas públicas, y de la creación de una institución dedicada exhaustivamente a proteger el derecho de los titulares de estos datos.

5. **Considera usted que en Ecuador debería expedirse una Ley de Protección de Datos Personales que ampare a los ecuatorianos frente al manejo de su información debido a las innovaciones tecnológicas como el *cloud computing***

Creo que es fundamental e imperiosa la necesidad de dictar una normativa que regule esto. Primero, porque aunque en Ecuador los derechos constitucionales son de aplicación directa, el contenido, la forma de eficacia de esos derechos se pueden construir desde la norma pero también desde jurisprudencia, es decir, es importante la existencia de una norma constitucional, para que la Corte Constitucional pueda desarrollar dictámenes que vayan definiendo el derecho. Lamentablemente ninguna de estas dos posibilidades de regularlo se están cumpliendo actualmente en Ecuador, lo que hace que sobre este tema haya un ámbito de desprotección que se debe comenzar a regular.