ISSN 1510-3714 ISSN en línea 2393-6193
DOI: https://doi.org/10.22235/rd.vi22.2239

El derecho a la protección de datos de personales en la prestación de servicios de *cloud computing.* Una perspectiva ecuatoriana

The Right to Personal Data Protection for the Provision of Cloud Computing Services. An Ecuadorian Perspective

Eugenia Novoa
ORCID: 0000-0001-5098-6304
Universidad Central del Ecuador.
Correo: epnovoa@uce.edu.ec

Recibido: 18/08/2020
Aceptado: 21/10/2020

Resumen: El presente 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 podrían ser establecidas por el Estado para que este derecho los ampare de forma preventiva. Inicialmente se explicará el modelo de prestación de servicios del *cloud computing*, estableciendo las fases para el tratamiento de datos personales. También se definirán pautas estandarizadas para comprender el derecho a la protección de datos personales y su aplicabilidad para los consumidores ecuatorianos. Finalmente, se intentará dilucidar si existe la necesidad de implementar en Ecuador normativa que prevenga y ampare en relaciones B2C frente al *cloud computing*.

Palabras clave: protección de datos; almacenamiento en la nube; *cloud computing*; políticas de privacidad.

Abstract: The present work seeks to clarify how the provision of cloud computing services can affect the right to data protection granted to Ecuadorian consumers, and the measures that could be established by the State so that this right guards them in a preventive manner. Initially, the model for provision of cloud computing services are explained, setting up phases for the processing of personal data. Standard guidelines will also be defined to understand the right of data protection and its enforceability by Ecuadorian consumers. Finally, we will attempt to clarify the need to implement in Ecuador a preventive framework that protects B2C relations in face of cloud computing.

Keywords: data protection; cloud storage; cloud computing; privacy policies.

Cómo citar: Novoa, E. (2020). El derecho a la protección de datos de personales en la prestación de servicios de *cloud computing*. Una perspectiva ecuatoriana. *Revista de Derecho*, *22*, 64-89. https://doi.org/10.22235/rd.vi22.2239

Introducción

El *cloud computing* o nube de cómputo es un paradigma de Internet que, sin lugar a duda, facilita y optimiza el funcionamiento de esta última. 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 el *cloud computing* no está exento de problemas, especialmente porque involucra manejo de información.

Con el avance de la tecnología crecen las problemáticas jurídicas. En el caso particular de la nube de cómputo, existen diversas situaciones frente a las cuales el derecho debe dar respuestas, por ejemplo, en temas de propiedad intelectual, aspectos penales, sobre derechos del consumidor, violaciones a derechos intrínsecos de los particulares, como el de protección de datos personales.

Este trabajo aborda el derecho a la protección de datos personales, en relación con las problemáticas y sus consecuencias, que se evidencian por el mal manejo de información de los usuarios de internet respecto al uso de servicios de *cloud computing*.

Es importante mencionar que esta investigación intenta vislumbrar la posibilidad de proteger a los usuarios ecuatorianos que viven en estado de indefensión, de un incesante y enigmático avance tecnológico. Enfatizamos el hecho de que los datos de la mayoría de los usuarios de internet están en la nube, lo que motiva adentrar en el *cloud computing*, ligándolo con un derecho muy discutido en la actualidad, la protección de datos personales desde la perspectiva digital.

Se analizará específicamente la relación *business to consumer* (en adelante B2C) generada por las políticas de privacidad de proveedores de servicios de *cloud computing*, que estipulan la utilización y tratamiento de datos personales de consumidores ecuatorianos, sin que estos últimos 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 se considera elemental para precautelar este derecho.

La Constitución de la República de Ecuador reconoce el derecho a la protección de datos de carácter personal. Para que este derecho sea precautelado, es preciso observar

la aplicación de ciertos principios para el manejo de la información, promoviendo así la conformación de un sistema preventivo de protección de datos personales. De esta forma será factible brindar un óptimo amparo a casos particulares de relación B2C con proveedores de servicios de *cloud computing*.

El servicio de *cloud computing*

La famosa "nube" surge como una metáfora de los diagramas de flujo de red utilizados para ilustrar al internet (Téllez, 2013) 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 Valencia, 2012, p. 51). Comprender la razón de ser de este término es indispensable para entender que, aunque imaginamos nuestra información almacenada en una "nube", ella siempre precisará de un soporte físico (*hardware*) de acopio (IBM, 2020).

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 lo puntualiza como aquel modelo que "permite el acceso oblicuo, conveniente y bajo demanda de red a un conjunto de recursos informáticos configurables que puedan ser rápidamente proveídos con esfuerzos mínimos de administración o interacción con el proveedor de servicios" (Instituto Nacional de Estándares y Tecnología, 2011).

Varios autores se basan en esa definición para configurar una propia. Tal es el caso de Téllez, 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" (Téllez, 2013, p. 5).

Para Joyanes (2012a), 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 (Joyanes, 2012a).

Conforme a las definiciones brindadas, se puede deducir que el *cloud computing* 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.

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 (Huilbert, 2013). 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. 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 ella.

Características distintivas del *cloud computing*

Con 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 mayoría de los autores concuerda con las cinco propuestas por el Instituto Nacional de Estándares y Tecnología (2011) que son las siguientes:

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 al proveedor únicamente por la cantidad de servicio que consume (Instituto Nacional de Estándares y Tecnología, 2011).

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* (Instituto

Nacional de Estándares y Tecnología, 2013). 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* (Téllez, 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.

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— (Benno, Corrales y Forgó, 2011). 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). 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 (Instituto Nacional de Tecnologías de la Comunicación, 2012).

La mayoría de las dificultades que presenta el *cloud computing*, respecto a la aplicabilidad del derecho a la protección de datos personales, emergen de esta característica porque, debido al dinamismo con que viaja la información, en ciertas circunstancias puede resultar complicado determinar la ubicación exacta de los datos personales; quiénes efectivamente tienen acceso a ellos y qué estándares de seguridad que deberán implementar para cada caso.

Si bien la trazabilidad de datos hoy por hoy a disminuido su complejidad, la determinación de responsabilidad no deja de ser complicada por la diversidad de ubicaciones en las que puede estar la información. Cabe resaltar que al momento existen estándares ISO que precautelan la protección de datos, sin embargo, su implementación representa un alto costo para pequeñas y medianas empresas. Si bien tales estándares ayudan a desarrollar y mejorar los procesos de gestión de la información de carácter personal de las organizaciones (Secure IT, 2019), estos no garantizan a cabalidad determinar la información transferida por medios electrónicos transnacionales.

De modo que resultará complejo determinar el ámbito de aplicación de la normativa, así como establecer responsabilidades a los actores, 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.).

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 alguien precisa más espacio en la nube, para lo cual sólo deberá realizar el pago en línea y automáticamente lo recibirá. Esta característica —según Joyanes (2012a)—, da la impresión de que los servicios de *cloud computing* son ilimitados y pueden ser adquiridos en cualquier momento.

Servicio supervisado: Los sistemas de cómputo en la nube controlan el uso de recursos para hacerlos óptimos de forma automática (Instituto Nacional de Estándares y Tecnología, 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, 2014).

Para Melaños (2013), 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.

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

Expertos en *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" (Securosis, 2011; TBC, 2019). Existen varias formas de delimitar dicho ciclo de vida; pero las que buscan en general especificar las diversas funciones que puede desempeñar el proveedor de servicios de *cloud computing* de forma que se logre distinguir las responsabilidades y obligaciones del derecho a la protección de datos personales para el responsable de tratamiento de datos.

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. En este caso particular, se toman en consideración las siguientes fases basadas en

los criterios de Seguridad informática utilizados ampliamente en el medio (Securosis, 2011; TBC, 2019).

Fase 1: Creación. También se la puede llamar creación/actualización, pues a través de esta 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 ella 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 por medios físicos o digitales.

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.

También se deben entender las distintas funciones que los actores en el sistema de *cloud computing* pueden desempeñar, conforme a cada fase expuesta. A tal efecto hay tres tipos de operaciones que ligadas con el tratamiento de datos (Securosis, 2011; TBC, 2019); es importante tener en cuenta que tales operaciones no forman parte de las fases del ciclo de vida de los datos previamente 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.

Es importante prestar atención a las fases que brindan funciones de procesamiento a los proveedores de servicios de *cloud computing*, pues será en estas fases cuando se podrían elaborar perfiles de sus usuarios.

Se debe también enfatizar que dentro del ciclo de vida de datos en el *cloud computing* existe tratamiento de datos personales de los usuarios de dichos servicios. Por tal razón, es menester que el Estado precautele el derecho a la protección de datos personales para aquellos titulares de información personal perfilada.

El derecho a la protección de datos personales en Ecuador para la prestación de servicios de *cloud computing*

El análisis del derecho de protección de datos de carácter personal, en Ecuador, se hará a la luz de la relación B2C, en la prestación de servicios de *cloud computing*.

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). 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.

Con la finalidad de contextualizar jurídicamente al lector respecto al foco del análisis de la investigación, 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. Sin embargo, 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*.

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

El proveedor de servicios de cómputo en la nube, en la órbita del derecho a la protección de datos personales podrá ser, de acuerdo con el caso, responsable de tratamiento o encargado de tratamiento. (Kohnstamm, 2010; Cloud Security Alliance, 2011).

Responsable de tratamiento (*data controller*): 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" (Confederación de Empresarios de Andalucía, 2014). En la misma línea, la Regulación 2016/679 del Parlamento Europeo y del Consejo Europeo (GDPR) define al responsable de tratamiento de en el número 7 del artículo 4 como

> la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

La figura de responsable de tratamiento hace alusión a aquella persona (en la mayoría de los 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 (Kohnstamm, 2010).

De acuerdo con 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.

Encargado 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" (Agencia Española de Protección de Datos, 2009). En la misma línea, la Regulación 2016/679 del Parlamento Europeo y del Consejo Europeo define al encargado de tratamiento en el número 8 del artículo 4 como "la persona física o jurídica, autoridad pública, servicio u otro organismo" que trate "datos personales por cuenta del responsable del tratamiento".

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, 2011). 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 este (Kohnstamm, 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.

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

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.

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 los casos es el destinatario final del servicio, aunque en otros puede no serlo (Van Gyseghem et al., 2010). Para fines de aplicación preventiva de la normativa de protección de datos personales, será preciso identificar a los usuarios suscriptores de los interesados (*data subject).*

En lo concerniente al 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), en otras palabras, la empresa suscribe el contrato, lo acuerda, pero no es la empresa quien usa per se los servicios de *cloud computing*.

Es justamente en casos como este, al existir una divergencia entre quien es suscriptor y quien usuario, donde nacen dificultades para determinar responsabilidad. En caso como el ejemplificado la responsabilidad será determinada en base a qué clase de modelo es el presentado en el servicio.

Por otro lado, 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 (Regulación 2016/679, art. 4).

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.

Por otro lado, el usuario de servicios de *cloud computing*, para la aplicación de normativa de protección de datos personales, podrá ser el suscriptor o el interesado (Van Gyseghem et al., 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, es decir a "Toda persona natural o jurídica que como destinatario final, adquiera, utilice o disfrute bienes o servicios, o bien reciba oferta para ello" (Ley Orgánica de Defensa del Consumidor, 2000, art. 2).

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 (Kohnstamm, 2010, pp. 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.

Contratos electrónicos de adhesión generados por la relación B2C en la prestación de servicios de *cloud computing* en Ecuador

La contratación electrónica por medio de contratos de adhesión, es un tema bastante amplio que amerita un trabajo de investigación específico para desarrollarlo. Sin embargo, debido a que la relación B2C en 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) "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 (2007) reflexiona sobre la necesidad de que estos contratos existan, pues para el empresario sería imposible negociar individualmente con cada uno de sus usuarios.

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 (Rojas, 2007).

El consentimiento en los contratos *click wrap* se manifiesta de forma expresa cuando el consumidor acepta los términos y condiciones de un contrato, haciendo un clic en el botón de "Acepto", "*Agree"* o "Estoy de acuerdo" (Rojas, 2007, p. 278; Acuña y Cordero, 2014, pp. 121-122). El consumidor manifiesta su consentimiento simplemente al pulsar un botón.

Con base en la teoría de los contratos de adhesión por medios electrónicos o *click wrap*, es importante tener en cuenta las disposiciones del ordenamiento jurídico ecuatoriano; pero se debe precisar 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, las que se encuentran recogidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; y, en la Ley Orgánica de Defensa del Consumidor. Esta afirmación es aplicable a los casos en los que el proveedor es una empresa ecuatoriana, por otro lado, si el proveedor es una empresa extranjera la legislación aplicable será la establecida en las cláusulas contractuales y el foro que convengan las partes acorde a tratados de derecho internacional privado.

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 (Ley Orgánica de Defensa del Consumidor, 2000, art. 2).

Igualmente, del texto de la Ley Orgánica de Defensa del Consumidor se desprende la importancia de que los proveedores de servicios de *cloud computing* —a la hora de elaborar sus políticas de privacidad—, tengan en cuenta lo establecido en los artículos 41, relativo a los contratos de adhesión, y 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, distingue a la "incorporación por remisión" como un método para instrumentalizar el consentimiento del usuario en la contratación electrónica. Esta figura legal introduce indirectamente los contratos electrónicos de adhesión o *click wrap* en el ordenamiento jurídico ecuatoriano. En los casos en que usuarios ecuatorianos contraten servicios de *cloud computing* con sus proveedores, 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 (Asamblea Nacional, 2005).

Finalmente, 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 habilitan a recoger, almacenar, procesar, perfilar y archivar la información de sus usuarios instrumentalizándose en contratos electrónicos de adhesión o *click wrap*.

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 como referencia los principios estándar del derecho a la protección de datos personales, aceptados a nivel mundial como elementos esenciales para la configuración de este derecho, los que serán descritos a partir de la relación B2C por la prestación de servicios de *cloud computing*.

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 deberán observarse por el legislador para la debida tutela de tal derecho.

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.

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). El consentimiento variará conforme a los tipos de datos que sean tratados, en ciertos casos de interés público, incluso no será necesario que este sea 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).

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 la legislación ecuatoriana relativas al consentimiento de *e-consumers,* al igual que a la ley aplicable y foro en contratos internacionales.

La Ley Orgánica de Defensa del Consumidor ecuatoriana en su artículo 4 numeral 4 reconoce a los usuarios el derecho especial de información, 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.

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.

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, esta plataforma cuenta con más de 4,5 mil millones de conexiones (Dropbox, 2020) 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.

Principio de finalidad

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 (Agencia Española de Protección de Datos, 2009).

Previa la creación de un fichero de datos personales será preciso conocer su finalidad; para Del Peso (2000) este principio es tan amplio que incluso engloba otros principios como el de utilización no abusiva y el de pertinencia. 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).

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 de este derecho. Es a partir de la información inicial que brinda el proveedor de servicios de *cloud computing* respecto 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), y que el mercado de *cloud* crece exponencialmente alcanzado aproximadamente 26 billones de dólares americanos al segundo semestre del 2019 (Statista, 2019), es evidente que una inmensa cantidad de información recogida de la nube se provee a compañías para su toma de decisiones. Los proveedores de servicios de cómputo en la nube deberían actuar conforme al principio de finalidad en la misma redacción de sus políticas de privacidad, esto se puede alcanzar activando Ecuador un sistema preventivo de protección de datos personales, mediante el que se evite que los usuarios de estos servicios desconozcan de las finalidades del tratamiento de sus datos.

Principio de lealtad y licitud

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. Del Peso (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 la 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 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.

El responsable de tratamiento deberá cumplir con las obligaciones que le impone este principio en el desempeño de 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 este 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* y la amplia transferencia de datos en el mundo, especialmente considerando que al 2022 se estima un tráfico global de IP de 150,700 GB por segundo (UNCTAD, 2019). Es evidente la necesidad de que se active un sistema preventivo de protección de datos personales en Ecuador. Este sistema exigiría al proveedor de servicios de *cloud computing* a cumplir con el principio de lealtad y licitud a partir de la redacción de sus políticas de privacidad y en el desarrollo de sus actividades de tratamiento de información.

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 (Agencia Española de Protección de Datos, 2009), 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). 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.

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, 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). Un sistema preventivo incentivaría 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.

Al respecto, existe en Ecuador el Proyecto de Ley Orgánica de Protección de Datos Personales que aún no ha sido aprobado, y al hablar del principio de calidad este proyecto hace especial énfasis en la veracidad de los datos, los cuales deben ser comprobables y actualizados, lo que es concordante con lo que dice el artículo 25 de dicho proyecto normativo, sobre el derecho a la rectificación de los datos que hayan sido consignados de manera errónea.

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.

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

Los proveedores de servicios de *hosting* en la nube año 2015 aproximadamente almacenan ocho zettabytes de contenido digital (Bluzebra Technologies, 2013). 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*, siguiendo estándares preventivos, 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.

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, 2000, 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).

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.

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 ya descrito en este trabajo.

Según encuestas, el 95% de personas diariamente utiliza algún servicio de *cloud computing* (Bluzebra Technologies, 2013). Habrá que imaginar entonces lo que representaría para estos usuarios que toda su información no sea tratada conforme al principio de utilización no abusiva. Es preciso que en Ecuador no solo se promueva la protección preventiva del consumidor electrónico, sino también se optimicen sus sistemas de reclamo con las autoridades de defensa al consumidor correspondiente.

Principio de seguridad

El principio de seguridad en la normativa comunitaria europea se incorpora y desarrolla en el artículo 32 de la Regulación 2016/679 del Parlamento Europeo y del Consejo Europeo. 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). 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.

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 (Vizcaíno, 2001). 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 con el 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.

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 ya definido en 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, 2015). Además, los proveedores de servicios de

cloud computing al año 2013 invirtieron 150 billones de dólares en el desarrollo de este paradigma (Bluzebra Technologies, 2013). Es preciso que las medidas de seguridad sean estipuladas en las políticas de privacidad de cada proveedor, de acuerdo con los distintos niveles de seguridad que manejen, a la par del tipo de datos que se recojan (inocuos, sensibles, etc.).

Conclusiones

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*.

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* conforme a las funciones que éste puede desempeñar en cada fase.

El derecho a la protección de datos personales es al momento una gran corriente en la Unión Europea, y para ser tutelado efectivamente, precisa del reconocimiento de otros derechos, principios, garantías y deberes que conjuntamente lo componen. Además, dicho derecho impone obligaciones a los responsables y encargados de tratamiento de datos, para que en el desempeño de sus actividades lo resguarden de forma preventiva. Sin embargo, este derecho en la legislación ecuatoriana ya ha sido reconocido de forma constitucional y precisa ser desarrollado con precedentes y políticas públicas, sin necesidad de crear más leyes.

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.

El Estado ecuatoriano, como garante de los derechos constitucionales de sus habitantes, debe velar porque se proteja el derecho a la protección de datos personales reconocido en la Constitución del 2008. Derecho que, por ser de naturaleza compleja en base a su falta de desarrollo normativo y continuo progreso, debe ser garantizado a través del desarrollo de políticas de gobiernos centrales y locales que fomenten los principios estándar que configuran un sistema preventivo de protección de datos personales que ampare a usuarios de servicios de *cloud computing* en relaciones B2C. Como se mencionaba con anterioridad, si bien existe ya un proyecto de normativa alrededor de este tema, su simple aprobación no es la solución a los problemas que todo este marco fáctico genera, es preciso ser pragmáticos y dar respuestas de relevancia transfronteriza desde la cultura de los proveedores y consumidores de *cloud* en Ecuador.

Referencias

Acuña, A., y Cordero, E. (2014). *Los contratos de shrinkwrap, clickwrapy browsewrap: Un enfoque desde la perspectiva del Derecho del Consumidor* (Tesis de pregrado). Universidad de Costa Rica. Recuperado de https://iij.ucr.ac.cr/wp-content/uploads/bsk-pdf-manager/2017/06/Los-contratos-de-shrinkwrap-clickwrap-y-browsewrap-Un-enfoque-desde-la-perspectiva-del-Derecho-del-Consumidor.pdf

Agencia Española de Protección de Datos. (05 de noviembre de 2009). *Estándares Internacionales sobre Protección de Datos Personales y Privacidad*. Recuperado de https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf

Alcocer, S. (20 de mayo de 2014). ¿Qué es 'cloud computing'? Definición y concepto para neófitos. *Zona Cinco.* Recuperado de http://zonacinco.org/alcocer/?p=31074

Armagnague, J. (2002). El derecho comparado en la protección de datos. En M. Ábalos y O. Arrabal, *Derecho a la información, hábeas data e Internet* (pp. 375-415). Buenos Aires, Argentina: La Rocca.

Asamblea Nacional. (2005). *Código Civil.* Quito, Ecuador: Registro Oficial No. 46.

Benno, B., Corrales, M., y Forgó, N. (2011). *Aspectos legales de la computación en la nube: Protección de datos y marco general sobre propiedad intelectual en la legislación europea*. Buenos Aires, Argentina: Editorial Albremática.

Bluzebra Technologies. (14 de abril de 2013). Technology of tomorrow cloud computing. Recuperado de http://ticsyformacion.com/2013/04/14/cloud-computing-la-tecnologia-del-manana-infografia-infographic/

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

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

Cloud Security Alliance. (2011). Cloud Compliance Report. Recuperado de https://docs.google.com/viewer?a=v&pid=sites&srcid=Y2xvdWRzZWN1cml0eWFsbGlhbmNlLmVzfGNzYS1lc3xneDo2NWNhZWFiNTkwODI1N2I

Confederación de Empresarios de Andalucía. (2014). *Modelos de e-Business*. Recuperado de http://www.cea.es/upload/ebusiness/modelos.pdf

Cruz Valencia, K. (2012). Historia del Cloud Computing. *Revista de Información, Tecnología y Sociedad, 7*, 49-69.

Del Peso, E. (2000). *Ley de Protección de Datos la nueva LORTAD*. Madrid, España: Ediciones Diaz de Santos S.A.

Dropbox. (2020). *Clients*. Recuperado de https://www.dropbox.com/business/customers

Eclipse. (05 de mayo de 2015). The Explosive Growth of Cloud Computing. *Cool Infographics*. Recuperado de http://www.coolinfographics.com/blog/2014/5/5/the-explosive-growth-of-cloud-computing.html

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

IBM. (2020). *Cloud Computing.* Recuperado de https://www.ibm.com/cloud/learn/cloud-computing

Instituto Nacional de Estándares y Tecnología. (junio de 2011). *La definición de Cloud Computing de NIST*. Recuperado de http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Instituto Nacional de Estándares y Tecnología. (18 de junio de 2013). *La definición de Cloud Computing de NIST*. Recuperado de http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_ 2013_June18_FINAL.pdf

Instituto Nacional de Tecnologías de la Comunicación. (2011). *Guía para empresas: seguridad y privacidad del cloud computing*. Recuperado de https://northsecure.es/wp-content/uploads/2013/05/guia_cloud_computing.pdf

Joyanes, L. (2012a). Computación en la nube. *Revista del Instituto Español de Estudios Estratégicos, 0*, 87-110.

Joyanes, L. (2012b). *Computación en la nube: estrategias del cloud computing en las empresas*. Mexico D.F., Mexico: Alfaomega.

Kohnstamm, J. (16 de febrero 2010). *Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento».* Recuperado de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_es.pdf

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (17 de abril de 2002). Registro Oficial 557. Quito, Ecuador.

Ley Orgánica de Defensa del Consumidor (10 de julio de 2000). Registro Oficial 116. Quito, Ecuador.

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.

Molina, E. (2012). *Tratado de derecho informático*. Buenos Aires, Argentina: La Ley.

Puccinelli, O. (2004). *Protección de datos de carácter personal*. Buenos Aires, Argentina: Editorial Astrea.

QuoteColo. (2015). Cloud computing predictions for 2015 [Infographic]. *Spacetel*. Recuperado de http://spacetel.co.uk/spacetel-insights/cloud-computing-predictions-for-2015-infographic/

Regulación 2016/679 del Parlamento Europeo y del Consejo, relativa a la protección de las personas naturales en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (27 de abril de 2016). Diario Oficial de las Comunidades Europeas, núm. L 119/32.

Rojas, V. (2007). El perfeccionamiento del consentimiento en la contratación electrónica. *Revista de Derecho Privado, 16-17*, 165-206.

Sánchez, Á. (1998). *La protección del derecho a la libertad informática en la Unión Europea*. Sevilla, España: Universidad de Sevilla.

Sarango, C. (2013). *Reformas para garantizar los derechos de los usuarios o consumidores de servicios electrónicos* (Tesis de grado). Universidad Nacional de Loja, Ecuador.

Securosis. (2014 de octubre de 2011). Data Security Lifecycle. Recuperado de https://securosis.com/tag/data+security+lifecycle

Secure IT. (2019). *ISO/IEC 27701: la estandarización de la protección de datos*. Recuperado de https://www.secureit.es/iso-iec-27701-la-estandarizacion-de-la-proteccion-de-datos/

Statista. (2019). *The Cloud Market Keeps Moving Upwards*. Recuperado de https://www.statista.com/chart/19039/cloud-infrastructure-revenue/

TBC. (17 de enero de 2019). What are the 6 Phases of the Data Lifecycle? Recuperado de https://blog.tbconsulting.com/what-are-the-phases-of-the-data-lifecycle

Téllez, J. (2013). *Lex cloud computing*. México D.F., México: Instituto de Investigaciones Jurídicas UNAM.

UNCTAD. (2019). *The digital economy report*. Recuperado de https://unctad.org/system/files/official-document/der2019_en.pdf

V3. (28 de agosto de 2015). *Top 10 cloud computing risks and concerns*. Recuperado de http://www.v3.co.uk/v3-uk/news/2343547/top-10-cloud-computing-risks-and-concerns/page/5

Van Gyseghem, J-M., Gerard, J., Gayrel, C., Moiny, J-P., y Poullet, Y. (2010). *Cloud computing and its implications on data protection.* Conseil de l'Europe. Recuperado de http://www.crid.be/pdf/public/6471.pdf

Vizcaíno, M. (2001). *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid, España: Civitas Ediciones.

Contribución autoral

a) Concepción y diseño del trabajo; b) Adquisición de datos; c) Análisis e interpretación de datos; d) Redacción del manuscrito; e) revisión crítica del manuscrito.

E. N. ha contribuido en a, b, c, d, e.

Editor científico responsable

Dra. María Paula Garat