

Aproximación integral al contrato de *Cloud Computing* en la economía digital

Comprehensive approach to the Cloud Computing contract in the digital economy

Alberto Pulido Lock, Natalia Jara¹ y María Ignacia Torres²

Resumen: En el mundo actual, la transformación digital de las empresas es un paso necesario e impostergable, para que estas sobrevivan en un nuevo mercado digital y golpeado por los cambios que nos trajo la pandemia del coronavirus. En este contexto, la implementación de nuevas soluciones tecnológicas como el *cloud computing*, son claves para facilitar estos procesos de transformación, porque permiten a los clientes almacenar grandes cantidades de datos en una nube que está disponible en todo momento, desde cualquier dispositivo con acceso a la red.

Sin embargo, los contratos que regulan la implementación de esta solución tecnológica no siempre son estudiados con detenimiento, para efectos de determinar los riesgos y ventajas que ofrecen las distintas modalidades de *cloud*. Por esta razón, en este artículo, se propone analizar los riesgos y ventajas de los contratos de almacenamiento en la nube, analizando su naturaleza jurídica desde un enfoque integral que incluya comprender la solución tecnológica y los activos de las empresas que están en juego, específicamente los datos, para identificar y mitigar adecuadamente los riesgos de esta tecnología, a través de una adecuada regulación contractual.

Abstract: *In today's world, the digital transformation of companies is a necessary and unpostponable step, for them to survive in a new digital market hit by the changes brought to us by the coronavirus pandemic. In this context, the implementation of new technological solutions such as cloud computing, are key to facilitate these transformation processes, because they allow customers to store large amounts of data in a cloud that is available at all times, from any device with access to the network.*

However, the contracts that regulate the implementation of this technological solution are not always fully studied, to determine the risks and advantages offered by the different cloud modalities. For this reason, this article proposes to analyze the risks and advantages of cloud storage contracts analyzing its legal nature from a comprehensive approach that includes understanding the technological solution and the company assets at stake, specifically the data, in order to identify and adequately mitigate the risks of this technology through appropriate contractual regulation.

Palabras clave: Computación en la nube - Datos - Datos Personales – Contratos de suministro en la nube – Transformación digital

Keywords: *Cloud Computing - Data - Personal Data - Cloud Supply Contracts - Digital Transformation*

Sumario: 1. Introducción. 2. Almacenamiento en la Nube: Aproximaciones técnicas y jurídicas. 3. Naturaleza Jurídica del Contrato de *Cloud*. 4. El valor de la información en la era de los datos masivos. 5. Datos: El fin último de los contratos de cloud computing. 6. Ventajas y riesgos de la transición a la computación en la nube. 7. Conclusiones.

¹ Abogada de la Universidad de Chile. Asociada del equipo de Energía y TMT en Philippi Prietocarrizosa Ferrero DU & Uría. Diplomado en Protección de Datos Personales de la Pontificia Universidad Católica de Chile. Diplomado Entendiendo China del Instituto de Relaciones Internacionales de la Universidad de Chile. Contacto: Email, natalia.jara@ppulegal.com.

² Abogada de la Pontificia Universidad de Católica de Chile. Asociada del equipo de Corporativo y M&A en Philippi Prietocarrizosa Ferrero DU & Uría. Contacto: Email: mariaignacia.torreso@ppulegal.com.

1. Introducción

La transformación digital es un proceso que se ha visto fuertemente acelerado por la urgencia y necesidad que impuso la pandemia del COVID-19. El confinamiento obligatorio llevó a empresas de todos los rubros a implementar el teletrabajo, muchas sin tener una planificación o estudio previo sobre cómo adoptar exitosamente esta nueva modalidad. Sin embargo, este proceso de implementación fue exitoso, en la mayoría de los casos, gracias a la flexibilidad, la posibilidad de adaptación, la agilidad, el dinamismo y la tecnología que es, y seguirá siendo, nuestro mejor aliado.

De hecho, los nuevos desarrollos tecnológicos y la pandemia cambiaron para siempre la manera cómo trabajamos, pues ahora es muy difícil de imaginar volver a un trabajo cien por ciento presencial, sin tener todas los documentos y herramientas tecnológicas a nuestra disposición, en cualquier momento y desde cualquier lugar. Por esto, la conectividad pasó a ser un aspecto fundamental para toda empresa, ya que hemos aprendido a trabajar en forma remota durante meses prescindiendo de documentos físicos.

La relevancia de la transformación digital de las empresas ha aumentado a niveles tan grandes, que un estudio de *International Data Corporation*³ (*IDC*) *FutureScape: Worldwide IT Industry 2021 Predictions*⁴ indicó que el 65% del PIB mundial estará digitalizado en 2022, impulsando un gasto en TI de 6.8 billones de dólares entre 2020 y 2023. En efecto, Latinoamérica va en camino a tener el 40% de su PIB digitalizado para el 2022, generando un gasto en TI de 460 mil millones de dólares entre 2020 y 2023, del cual un 35%, estará relacionado con la nube.

Por esta razón, Rick Villars, vicepresidente del grupo de investigación mundial de *International Data Corporation*, concluyó: “*la pandemia COVID-19 puso de manifiesto que la capacidad de adaptarse y responder rápidamente a las interrupciones imprevistas del negocio será un factor determinante del éxito en nuestra economía cada vez más digitalizada. Un gran porcentaje de los ingresos de una empresa futura depende de la capacidad de respuesta, escalabilidad y resistencia de su infraestructura, aplicaciones y recursos de datos*”⁵. Es decir, la economía y las empresas, requieren implementar, rápidamente, un proceso de transformación digital y, en dicho proceso, deberán contratar nuevas tecnologías, como el almacenamiento en la nube o “*cloud*”, para transitar exitosamente hacia un nuevo modelo de trabajo con conectividad total.

Por consiguiente, este artículo tiene por objetivo demostrar que el análisis conjunto de la solución tecnológica a implementar, específicamente el modelo de servicio a contratar (SaaS, PaaS, IaaS) con el tipo de datos que se almacenarán en la nube, son fundamentales al momento de elegir o negociar las condiciones del contrato de *cloud*. Pues, independiente que se trate de un contrato libremente negociado o de adhesión, es esencial tener una mirada integral entre solución tecnológica y los activos de la empresa, para escoger adecuadamente al proveedor del servicio de *cloud* y satisfacer realmente las necesidades de la empresa.

Para lograr este objetivo, en la primera sección, se expondrán las características del *cloud computing* y el contrato que regula la implementación de esta tecnología. Asimismo, se analizará el contrato de almacenamiento en la nube con las figuras contractuales civiles y comerciales típicas, para efectos de facilitar su comprensión e interpreta-

³ *International Data Corporation*, la principal firma mundial en inteligencia de mercado, servicios de consultoría y eventos para los mercados de Tecnologías de la Información, Telecomunicaciones y Tecnología de Consumo.

⁴ Rick Villars y otros, 2021. “*IDC FutureScape: Worldwide IT Industry 2021 Predictions*” *International Data Corporation*. Acceso 28 de mayo de 2021. Disponible en: <https://www.idc.com/getdoc.jsp?containerId=US46942020&pageType=PRINTFRIENDLY>

⁵ *Ibid.*

ción en casos complejos. Posteriormente, en la segunda sección, se desarrollará un breve análisis de los datos como activos valiosos para la empresa y que, dependiendo de su contenido, pueden existir otros elementos normativos a considerar en el contrato de *cloud*. Por último, en la tercera sección, se realizará un análisis sobre el impacto de comprender los riesgos de la solución tecnológica, en conjunto con los riesgos de la transacción, originados por el tipo de dato de que se trate.

2. Almacenamiento en la Nube: Aproximaciones técnicas y jurídicas.

En el contexto de la transformación digital, tecnologías como la nube o “*cloud*” son claves, porque nos permiten transformar digitalmente a empresas y espacios de trabajo gracias a una gran capacidad de almacenamiento de datos e información, disponible en todo momento, desde cualquier dispositivo con acceso a la red.

En este contexto, según distintos especialistas, actualmente la nube es infraestructura crítica necesaria para operar una empresa. Sin embargo, ¿en qué consiste exactamente esta nueva tecnología que revolucionó la capacidad de almacenamiento y el acceso de la información? El Instituto Nacional de Estándares y Tecnología (“NIST”) de Estado Unidos, define la computación en nube como “*un modelo que permite el acceso en red, cómodo y a la carta, a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios*”⁶.

En otras palabras, consiste en un servicio digital por el cual un proveedor pone a disposición del usuario recursos informáticos a través de internet, permitiéndole procesar, gestionar, compartir, acceder y almacenar su información, datos o aplicaciones conforme a sus necesidades en tiempo real, a modo de autoservicio, sin que el usuario deba adquirir o mantener la infraestructura soporte física ni digital.

En la literatura, el *cloud computing* es una tecnología que posee cinco características esenciales. Primero, es un tipo de **autoservicio bajo demanda**, porque el consumidor dispone unilateralmente de las capacidades informáticas, según sus necesidades. Segundo, por entregar **acceso a la red on-demand**, se puede acceder a sus servicios a través de mecanismos estándar como computadores, *tablets* o teléfonos móviles. Tercero, la **puesta en común de recursos**, que permite a múltiples consumidores servirse de la plataforma mientras que los recursos son asignados de manera dinámica en función de la demanda de los consumidores, esto implica que el cliente del sistema de almacenamiento generalmente no tiene control sobre la ubicación exacta de los recursos que se le proveen. Cuarto, **elasticidad rápida**, que implica que las capacidades pueden aprovisionarse y liberarse rápidamente o incluso automáticamente, para escalar hacia dentro o fuera en función de la demanda. Quinto, es un **servicio medido**, que controla y optimiza automáticamente el uso de recursos aprovechando su capacidad de medición según un nivel de servicio, como el almacenamiento, procesamiento, ancho de banda o cuentas de usuario activas⁷.

Por otro lado, cabe destacar que la nube o *cloud computing* usualmente se provee en tres modali-

6 Mell, Peter; Grance, Timothy. 2011 “*The NIST Definition of Cloud Computing*”. Instituto Nacional de Estándares y Tecnología. Acceso 27 de mayo de 2021. Disponible en: <http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf>

7 Mell, Peter; Grance, Timothy. 2011 “*The NIST Definition of Cloud Computing*”. Instituto Nacional de Estándares y Tecnología. Acceso 27 de mayo de 2021. Disponible en: <http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf>

dades de implementación, según el tipo de servicio que se está contratando. A saber:

1. **Infraestructura como Servicio** (“IaaS”): Esta modalidad consiste en proporcionar al cliente la infraestructura y otros elementos de hardware desde una modalidad virtual. Es decir, se facilita la maquinaria y los servidores, para que el cliente pueda almacenar en forma virtual sus archivos y datos digitales en una infraestructura que administra el proveedor del servicio *cloud*⁸. En este caso, el cliente no gestiona, ni controla, la infraestructura de la nube, pero sí tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones desplegadas, e, incluso en ciertos casos, posiblemente un control limitado de determinados componentes de red.
2. **Plataforma como Servicio** (PaaS): Esta modalidad permite desplegar en la nube aplicaciones creadas o adquiridas por el cliente, utilizando herramientas soportadas por el proveedor⁹. El cliente no gestiona ni controla la infraestructura de la nube, pero sí las aplicaciones y, posiblemente, los ajustes de configuración del alojamiento de aplicaciones.
3. **Software como servicio** (SaaS): En esta modalidad se contrata un software ofrecido como un servicio. Es decir, contrata un “*entorno operativo completo con aplicaciones, administración o interfaz del usuario*”¹⁰.

Entre estos modelos de *cloud*, existe una clara tendencia a preferir el modelo SaaS. En efecto, para el año 2018 -pre pandemia- se preveía un 59% de los servicios de almacenamiento en la nube como

SaaS, frente a un 28% de modalidad IaaS y 13% de la modalidad PaaS.

Por consiguiente, podemos concluir que, en esencia, la nube es una tecnología que permite al usuario almacenar información, compartirla y acceder a ella en todo momento. Asimismo, permite procesar la información almacenada, permitiendo generar bases de datos, reproducir aplicaciones y también desarrollar softwares y aplicaciones. Sin perjuicio de ello, los modelos de *cloud* se distinguen según la capacidad de almacenamiento y gestión de datos e información que se le entrega al usuario, los servicios que puede acceder y el nivel de control sobre los sistemas operativos de la nube y configuraciones.

Atendido lo anterior, si bien, la clasificación evidencia que el contrato de *cloud* puede tomar distintas formas, todos tienen una misma base. Así, se puede definir como aquel instrumento jurídico que regula la modalidad de *cloud* elegida por el usuario, estableciendo los derechos y deberes del prestador de la solución tecnológica y su cliente. No obstante, no se encuentra regulado en la legislación chilena y, por ende, es necesario caracterizarlo conforme a las clasificaciones del derecho civil y mercantil, para comprender los derechos y obligaciones de las partes.

3. Naturaleza Jurídica del Contrato de *Cloud*

Como veníamos adelantando, el objeto del contrato de *cloud*, la prestación, será diferente según tipo de servicio que se le entrega al cliente. La distinción que realizamos anteriormente, en cuanto a si es un contrato que provee de infraestructura

8 Navas Navarro, Susana, 2016. “El almacenamiento de los datos “*cloud computing*” al ADN Sintético”. En: Mercado Digital Principios y Reglas Jurídicas. Tirant Lo Blanch, p. 42.

9 *Ibid.*

10 Navas Navarro, Susana. *El almacenamiento de los datos “cloud computing” al ADN Sintético*. En: Mercado Digital Principios y Reglas Jurídicas. Tirant Lo Blanch, p. 42. 2016.

(IaaS), plataforma (PaaS) o software (SaaS) tiene implicancias jurídicas además de técnicas.

El tipo de servicio contratado determinará en gran medida la distribución de obligaciones y responsabilidades entre proveedor y cliente. Aunque no será un tema estático, pues no existe un modelo único para cada tipo de servicio, y porque, al ser un servicio tecnológico, está en constante evolución y desarrollo. Los servicios descritos (SaaS, PaaS e IaaS) no son los únicos modelos que existen, además en la práctica en un mismo contrato puede convenirse la prestación mixta de servicios. Sin embargo, aun con sus diferencias, tienen un elemento en común: la contratación de recursos computacionales de forma escalable, a los cuales se accede a través de Internet, y que se gestiona a modo de autoservicio.

Si bien no existe regulación específica, nacional o internacional, para determinar el alcance de las obligaciones en este contrato, las normas generales del derecho comercial y civil nacionales son plenamente aplicables. Con lo cual, debemos analizar las características del contrato y sus figuras afines. De este modo, podremos establecer cuáles son sus puntos más relevantes, los cuales pueden cambiar toda la estructura de derechos y obligaciones que emanan del contrato de *cloud*.

Para llegar a la naturaleza jurídica del contrato de *cloud*, dividiremos este capítulo en dos. Primero, veremos los contratos típicos que guardan similitudes con el contrato de *cloud*, para dirimir qué normas podrían aplicarle por medio de una interpretación analógica de la ley. Luego, estudiaremos desde la perspectiva de la clasificación de los contratos, las características particulares de los contratos de *cloud*, para enmarcar los derechos, obligaciones y responsabilidad aplicables.

No obstante, desde ya, adelantamos que, en nuestra opinión, el contrato de *cloud* se configura por una figura atípica y compleja de prestación de ser-

vicios que, si bien guarda semejanzas con contratos típicos, tiene una naturaleza distinta de la que emanan derechos y obligaciones propias. Estos tendrán matices o grados de exigibilidad en atención al tipo de servicio contratado, los datos que han de almacenarse en la nube, y las necesidades y recursos del cliente.

3.1 Figuras afines al Contrato de *cloud*

Antes de comenzar esta sección, es menester aclarar que, si bien existen otras figuras contractuales asimilables al contrato de *cloud*, como el contrato de *outsourcing* tecnológico, el contrato de host, o el contrato de suministros mercantil, para efectos de este artículo solo analizaremos las semejanzas del contrato de *cloud* con los contratos de depósito y arrendamiento, dado que son los que se encuentran regulados en el marco jurídico chileno.

Esta comparación la haremos tomando el objeto del contrato de *cloud* para determinar qué contratos típicos tienen una regulación similar y, por ende, podrían dar luces en casos complejos para interpretar el contrato de almacenamiento. Esto sin perder de vista de que el objeto del contrato está íntimamente relacionado con el valor de la información y los datos que se subirán a la nube.

Como mencionamos anteriormente, el objeto del contrato de *cloud* se configura por los servicios que se contratan a través de él. Estos se pueden sintetizar en lo siguiente: procesar, gestionar, compartir, acceder y almacenar su información, datos o aplicaciones a través de Internet.

El primer contrato típico que analizaremos tiene relación con el servicio de almacenamiento de cosas, las cuales deben cuidarse y restituirse al término del contrato. Esta figura existe en nuestro derecho como depósito, regulado en la ley civil y mercantil. El artículo 2211 del Código Civil Chileno define el depósito como aquel “*contrato en el*

*que se confía una cosa corporal a una persona que se encarga de guardarla y de restituirla en especie*¹¹.

En la definición anterior encontramos dos elementos que coinciden con el contrato de *cloud*. Por un lado, el *confiar* una cosa, en una persona para que esta la *guarde*, por otro lado, la obligación de custodia y debido cuidado que ha de tener el depositante para luego restituir las cosas en especie.

No obstante, el contrato de depósito recae sobre cosas corporales, y bien sabemos que, en el contrato de *cloud*, la cosa que se entrega para su guarda y custodia son bienes inmateriales¹², y la entrega consiste en la migración de datos desde un ordenador a otro. A pesar de las evidentes diferencias entre ambos contratos, y las limitaciones del clásico contrato de depósito para contener lo complejo del contrato de *cloud*, la comparación nos parece útil a efecto de vislumbrar el estándar de responsabilidad que tiene el proveedor de *cloud* respecto de los datos almacenados en la nube.

En ese sentido, el artículo 248 del Código de Comercio¹³ establece que el depositario es responsable de la custodia y conservación de los efectos que se pongan bajo su cuidado, tiene la obligación de indemnizar cualquier daño o pérdida que se produzca mientras las cosas existen en su poder, y solo puede exonerarse de responsabilidad probando que el daño se produjo a causa de un

caso fortuito o por vicio inherente a las mismas mercaderías. Esta norma podría sernos útil en un caso de pérdida o daño a la información almacenada por un contrato de *cloud*, en caso de que la materia no esté específicamente regulada por el propio contrato.

Por otra parte, la ley mercantil establece que “*el depositario que hace uso de la cosa depositada, aun en los casos que se lo permita la ley o la convención, pierde derecho a la retribución estipulada o la usual*”¹⁴. Este artículo es interesante de analizar en el caso de un contrato de *cloud*, porque en caso de aplicarse, el proveedor de los servicios perdería derecho a su retribución si es que llegase a utilizar los datos guardados en la nube, cosa que es bastante usual en los contratos de *cloud* y que en la mayoría de ellos se permite expresamente al proveedor hacer uso de la información para variados fines¹⁵.

Sin embargo, el contrato de *cloud* es mucho más complejo que el de depósito, pues nos permite acceder y gestionar las cosas almacenadas en la nube. En este sentido, mediante el contrato de *cloud*, el cliente accede a una infraestructura digital, aspecto que, en ningún caso, podría ser parte del contrato de depósito. En otras palabras, almacenar contenido en la nube es uno de los elementos esenciales del contrato de *cloud*, pero no es el único, ya que también son cosas esenciales a este

11 Código Civil Chileno, Artículo 2211.

12 En general, los datos son difíciles de clasificar desde el punto de vista civil, porque no son cosas corporales, ya que, no tienen un ser real, capaz de ser percibido por los sentidos; pero tampoco son una cosa incorporeal, porque no consisten en meros derechos. Artículo 565 del Código Civil. Sin embargo, para efectos del presente artículo, sólo nos limitaremos a reconocer que los datos son bienes o activos inmateriales, porque no son corpóreos. y tampoco consisten en meros derechos.

13 Este artículo que regula las obligaciones del comisionista es aplicable al depósito mercantil según lo dispuesto en el artículo 808 del Código de Comercio.

14 Código de Comercio Chileno, Artículo 810.

15 A modo de ejemplo, citamos la licencia de uso de la información del usuario que exige Google en los Términos y Condiciones de sus aplicaciones, incluida su nube o “Google Drive”: “*Esta licencia abarca su contenido está protegido por derechos de propiedad intelectual. Esta licencia permite a Google: alojar, reproducir, distribuir, comunicar y usar su contenido; por ejemplo, para guardarlo en nuestros sistemas y acceder a él desde cualquier lugar*”. Disponible en: <https://policies.google.com/terms?hl=es-419>

tipo de contrato la posibilidad de acceder, compartir, gestionar y procesar la información.

Por eso, otro contrato típico que es equiparable a este tipo de servicio es el contrato de arrendamiento. En este caso, lo arrendado es el espacio virtual, la infraestructura, que permitirá al cliente acceder, gestionar y compartir los datos como estime conveniente. Recordemos que este espacio virtual es también un espacio físico o centro de datos (servidores). Un lugar que puede estar ubicado en cualquier lugar del mundo al que el cliente accede solo a través de un dispositivo con conexión a internet.

Recordemos que el arrendamiento es un contrato por el cual se concede el goce sobre una cosa, que puede ser corporal o incorporeal, mientras pueda usarse sin consumirse¹⁶. La calificación del contrato de *cloud* como un arrendamiento de cosa, tiene, a su vez, interesantes posibilidades a la hora de interpretar el alcance de las obligaciones de las partes en este tipo de relación comercial. Respecto del proveedor, es útil el artículo 1924 del Código Civil, que establece las obligaciones del arrendador (proveedor en este caso), las cuales son: (i) La entrega de la cosa; (ii) mantenerla en estado de servir; y, (iii) librar al arrendatario (usuario) de toda turbación o embarazo en el goce de la cosa arrendada.

Nos parece acertado que a un proveedor de servicios en la nube se le exija garantizar el acceso a la nube en todo momento, o “mantenerla en estado de servir”, y también librar al usuario de toda turbación en el servicio. Si en el contrato de *cloud* no se establecen estas obligaciones para el proveedor, podríamos entender que son elementos de la naturaleza del contrato y que, por tanto, se encuentran incluidos en él sin necesidad de mención expresa. Así, el cliente podría argumentar que una falla en el servicio o una caída del sistema le da

derecho a ser indemnizado de todo perjuicio. Lo anterior, es de gran relevancia si consideramos que los sistemas computacionales son esenciales para el funcionamiento de la empresa moderna y que este tipo de riesgos pueden producir importantes pérdidas para cualquier negocio.

Sin embargo, este contrato tampoco es suficiente para abarcar todas las implicancias que tiene un contrato de *cloud*, sobre todo considerando la importancia de la información que el cliente resguarda en la nube. En un contrato de arriendo típico no existe un deber de cuidado para con las cosas que se guarden dentro de la infraestructura arrendada, lo cual resulta inconcebible si pensamos en la importancia que tienen los datos para una empresa.

En conclusión, el contrato de *cloud* es complejo y no encaja perfectamente en ninguna figura contractual tradicional, aunque si tiene ciertos elementos comunes con ciertos contratos típicos. Por esta razón, hay quienes postulan que se trata de un contrato híbrido, que combina elementos de distintos contratos. No obstante, la variabilidad de servicios que pueden ofrecerse a través de este contrato hacen que la única solución sea determinar que es un contrato completamente independiente de otros, atípico y complejo, con su propia naturaleza jurídica.

3.2 Características y clasificación del contrato de *cloud*

Para desentrañar esta naturaleza jurídica particular, y así establecer los elementos de la esencia, naturaleza y accidentales del contrato de *cloud*, a continuación, realizaremos un breve estudio de las características del contrato, enmarcándolo dentro de las clasificaciones generales del contrato contenidas en los artículos 1439 y siguientes del

16 Código Civil Chileno, Artículos 1915 y 1916.

Código Civil, y otras clasificaciones doctrinarias relevantes.

En primer lugar, es un contrato bilateral, pues las partes se obligan recíprocamente. Por el lado del proveedor, es claro que este se obliga a prestar los servicios de *cloud* según la modalidad pactada. El cliente, por otro lado, estará obligado a utilizar la plataforma del servicio conforme a las condiciones de uso del propio proveedor y la ley. Otro tipo de obligaciones para el cliente varían según cada contrato, por ejemplo, puede pactarse una prestación de dinero a cambio por los servicios.

Sin perjuicio de ello, la bilateralidad del contrato de *cloud* no implica que las partes estén en igualdad de condiciones para negociar las prestaciones a las que quedarán obligados. Es por esta desigualdad en las condiciones de las partes que, muchas veces, los contratos de *cloud* toman la forma de contrato de adhesión, en el cual el cliente no tendrá poder para negociar las cláusulas del contrato. Por lo tanto, en este punto es relevante reconocer que, en ciertos casos, la única libertad que tendrá el cliente del servicio de *cloud* será la de celebración y no del contrato. Por lo mismo, si la modalidad no le satisface sus necesidades, lo recomendable será cambiar de proveedor y optar por aquel que ofrezca mejores condiciones.

En tercer lugar, el contrato de *cloud* es oneroso porque “*tiene por objeto la utilidad de ambos contratantes, gravándose cada uno en beneficio del otro*”¹⁷. Como ya adelantábamos, en muchos de los casos el cliente pagará una suma de dinero por el servicio, ya sea con un pago único o, lo que es más común, mediante un cargo periódico (similar a un arrendamiento). Sin embargo, muchos proveedores parecen ofrecer el acceso “gratuito” a la nube, ya que no debe pagarse una suma de dinero. No obstante, esto no quiere decir que el contrato sea, en esencia, gratuito, pues el provee-

edor sí obtendrá alguna utilidad a partir del contrato, por ejemplo, el acceso o una licencia de uso sobre los datos del cliente, lo cual, como se explicará en la siguiente sección, puede ser aún más valioso que un pago en dinero.

En cuarto lugar, el carácter mercantil o civil del contrato va a depender de quién sea el cliente. Por lo tanto, no es de la esencia del contrato de *cloud* el ser caracterizado como mercantil. De hecho, muchos los proveedores de *cloud* contratan con privados no comerciantes, en cuyo caso, el contrato será civil. Si el cliente es una empresa, en cambio, el contrato será de naturaleza mercantil, pues se integrará a su actividad empresarial. Si bien esta clasificación no es parte de la esencia del contrato de *cloud*, es relevante para distinguir la normativa aplicable al momento de interpretar sus disposiciones.

Por último, es relevante destacar que es un contrato de tracto sucesivo, es decir, tiene un cumplimiento que se va desarrollando durante un lapso prolongado de tiempo, produciendo una relación contractual de cierta permanencia. En efecto, es usual que en los contratos de *cloud* se incluya una cláusula de “tácita reconducción”, por la cual, los efectos del contrato se van renovando por periodos similares de tiempo si las partes nada dicen en sentido contrario.

Esta característica es relevante, porque un problema común para los clientes de este servicio es la dependencia de sus proveedores, y la poca claridad en cuanto a la terminación del contrato o expiración de los servicios. Una posible estrategia para mitigar este riesgo de dependencia puede ser el de contratar servicios de varios proveedores, de modo que ninguno tenga el poder de desmantelar o eliminar sus cuentas con todos los datos dentro.

3.3 Labor interpretativa.

17 Código Civil Chileno, Artículo 1440.

Al finalizar nuestro análisis sobre la naturaleza jurídica del contrato de *cloud*, hemos podido apreciar cómo sus distintas interpretaciones pueden generar efectos muy diferentes en cuanto al régimen de derechos y obligaciones de las partes. De ahí la importancia de la labor interpretativa de las cláusulas del contrato, con foco en el tipo de servicios que van a requerirse y los datos que van a almacenarse.

En consecuencia, es posible concluir que el contrato de *cloud* es un contrato de prestación de servicios atípico complejo, pues sus prestaciones no pueden enmarcarse en ningún contrato regulado, porque tiene una naturaleza propia y compleja en cuanto a su estructura base y combinaciones. Sin embargo, por sus características principales y las normas generales en la clasificación de los contratos, hemos podido definir sus elementos esenciales, de la naturaleza y accidentales. Con esta estructura base, podremos evaluar con mayor detalle las necesidades del cliente en particular y cómo satisfacerlas mitigando los riesgos que existen al entregar a un tercero la custodia de datos y sistemas claves en el funcionamiento de la empresa.

4. El valor de la información en la era de los datos masivos.

Actualmente, el valor de la información ha aumentado exponencialmente gracias a los importantes avances tecnológicos vinculados con la recopilación y almacenamiento de todo tipo de datos, los cuales pueden provenir de todo tipo de fuentes, como sensores, *smartwatches*, *smartphones*, correos electrónicos, etc. Asimismo, se han desarrollado importantes avances en las tecnologías de procesamiento, las cuales permiten realizar tratamientos de grandes volúmenes de datos -también conocido como “macrodatos”-, a una

gran velocidad, lo cual permite obtener información de gran valor para automatizar procesos, ofrecer productos y servicios en forma customizada a los clientes y, en general, potenciar un modelo de negocios preexistente en el contexto del mercado digital.

En este contexto, es imprescindible reconocer que los datos se han transformado en un activo intangible de gran valor para las empresas, porque permiten a cualquier negocio que se desenvuelve en una economía digital, prosperar, obtener ventajas competitivas, mejorar sus procesos, optimizar las experiencias de los clientes, etc; y, en consecuencia, garantizar su adecuada protección y almacenamiento es fundamental para resguardar la integridad de un modelo de negocios o la posición de un actor en el mercado.

Atendido lo anterior, cuando se negocien y celebren contratos de *cloud computing*, no solo será necesario tener presente la naturaleza jurídica o las obligaciones que nacen del instrumento que regula la relación entre el proveedor del servicio y el usuario, sino también el valor de los datos que se almacenará en la nube, ya que el nivel de confidencialidad, protección o niveles de acceso a la información son elementos relevantes al momento de determinar los términos y condiciones del servicio que se contrata.

5. Datos: El fin último de los contratos de cloud computing.

En general, los datos se han definido como la “*información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho*”¹⁸. De esta manera, existe una directa relación entre el concepto dato con la información, ya que el dato es la forma en que

18 Real Academia Española, s.v. “dato”, actualización 2020, <https://dle.rae.es/dato>.

un conocimiento, comunicación o contenido, se expresa en algo comprensible o interpretable.

Ahora bien, en virtud de la propia definición de dato, es posible concluir que estos pueden provenir de cualquier fuente – como encuestas, sitios web, drones, dispositivos conectados a la red, etc.- y, pueden expresarse mediante diversos soportes –imágenes, libros, videos, mensajes, pedidos, visitas a un sitio web-. Por ende, tienden a acumularse en la medida que los avances tecnológicos facilitan su recolección y procesamiento¹⁹.

Sin embargo, para otorgarles valor y transformarlos en un activo de utilidad para una empresa, estos datos necesariamente deben ser recopilados, organizados y procesados, de forma que faciliten la extracción de información. Para esto, generalmente se utilizan “metadatos”, los cuales se definen como una “*descripción estandarizada de las características de un conjunto de datos*”²⁰, para que sea posible “ubicar” y extraer conocimientos de valor, según las preguntas o necesidades del interesado en el procesamiento de los datos recolectados.

En este punto, surge el denominado “ciclo de vida del dato”, el cual consiste en un proceso que tiene por objeto transformar datos en información, dicha información en conocimiento y, finalmente, dicho conocimiento en comprensión, mediante diversas actividades de procesamiento. Todo procesamiento de datos responde a una pregunta o necesidad determinada por una empresa, investigador, u órgano público, que busca conocer de mejor forma su propia realidad y, en definitiva, explicar y gestionar el mundo a través de los datos²¹. Por tanto, dependiendo de las capacidades

y el objetivo que tenga la persona o entidad que realice el procesamiento de datos, el conocimiento extraído puede variar e incluso, puede mejorar o ser utilizado en contra de quien originalmente había realizado una recopilación de información para su negocio.

Por esta razón, para efectos del presente artículo, es relevante tener presente que cualquier persona que tenga acceso a una base de datos, incluido un proveedor de servicios *cloud*, puede realizar un procesamiento no autorizado de los datos, lo cual puede generar, en sí mismo, un perjuicio para el dueño de la base de datos. Pues, toda información puede ser utilizada en favor o en contra de quien originalmente tenía un derecho sobre esta. De esta manera, cuando se celebre un contrato de *cloud* será necesario evaluar cuáles serán los estándares de seguridad de la información que asumirá el proveedor del servicio y, regular expresamente, cuáles son los límites que se le exigirán al proveedor, en términos del acceso y uso de la información almacenada en la nube.

Con todo, previo a desarrollar el alcance de las obligaciones de un proveedor de un servicio *cloud*, es necesario exponer brevemente cómo pueden clasificarse los datos que una empresa recopila en el desarrollo de su negocio. El objetivo de esta exposición es identificar si existen riesgos asociados a ciertas categorías de datos que deben ser mitigados en los contratos de *cloud*, así como identificar algunas exigencias normativas especiales asociadas al contenido de los datos almacenados en la nube.

19 En la literatura se habla de un verdadero de “diluvio de datos”, el cual se acrecienta por el desarrollo de tecnologías como el Internet de las Cosas, redes sociales, plataformas digitales, etc.

Puyol, Javier, 2015, *Aproximación jurídica y económica del Big Data*, Tirant Lo Blanch, 2015, p. 9.

20 Real Academia Española, s.v. “metadatos”, actualización 2020, <https://dpej.rae.es/lema/metadato>.

21 Datificación: Es una tendencia tecnológica relacionada con el Big Data en virtud de la cual se busca gestionar el mundo desde la información.

Puyol, Javier, Op. Cit., p. 10.

5.1 Clasificación según su importancia o sensibilidad.

Por otra parte, los datos se pueden clasificar según su nivel de importancia o sensibilidad, conforme a los perjuicios que podría generar su filtración, divulgación no autorizada, pérdida o robo. Este criterio, se puede expresar de diversas formas, ya que, las instituciones o empresas son libres de clasificar en base a los niveles de criticidad o confidencialidad de la información.

Para ilustrar el ejercicio de clasificar los datos según su importancia, se tomarán como referencia las categorías utilizadas por el Instituto Nacional de Estándares y Tecnología (“NIST”) de Estado Unidos, en la cual se identifica la criticidad baja, media y alta. Sin perjuicio que, como se advertía anteriormente, existen distintos criterios de clasificación igualmente válidos²².

Los datos de **criticidad baja** son aquellos que son comúnmente conocidos por cualquier persona o empleado de organización y, cuya modificación no autorizada, puede ser reparada fácilmente sin comprometer los intereses de una organización²³. La **criticidad media**, consiste en aquellos datos e información que la propia organización la cataloga como “reservada”, porque es utilizada por algunos empleados dentro de la organización, sin ser este grupo necesariamente “selecto”. Es decir, es reservada para los terceros y en general, para diversos empleados de la empresa que no necesitan conocer su contenido para realizar sus labores²⁴. Este nivel de criticidad supone un mayor riesgo que el leve para organización, porque el uso no

autorizado puede comprometer los intereses de la empresa y, en caso de pérdida (temporal o definitiva), puede generar daños significativos sus operaciones. Por último, la **criticidad alta** está relacionada con un secreto, que solo es conocido por un grupo selecto de la organización -por ejemplo, altas gerencias, jefes de áreas o proyectos-, ya que, tanto su divulgación no autorizada, como pérdida, puede generar daños significativos y permanentes a la organización²⁵.

Por consiguiente, se puede concluir la importancia de preparar la celebración de un contrato de *cloud* considerando el valor de la información que el cliente busca almacenar en la nube. En efecto, es trascendental conocer la importancia de los datos, el nivel de confidencialidad que se debe guardar en virtud de su contenido, cuáles son los niveles de acceso a la información disponible en la nube, y si será necesario exigir respaldos de seguridad para evitar pérdidas económicas relevantes para la empresa si los datos sufren daños irreparables²⁶.

5.2 Clasificación según su contenido.

Por último, también es relevante clasificar los datos de la empresa según su contenido, específicamente si consisten en bases de datos personales, pues esto impone un marco normativo más exigente para el responsable de los datos, que, en este caso, corresponderá al cliente que busca almacenar sus datos en la nube. De esta manera, a diferencia de lo que ocurre cuando se tratan datos no personales, las legislaciones normalmente exigen obligaciones adicionales que serán relevantes

22 Esta clasificación ha sido implementada por los departamentos de seguridad en Estados Unidos y en Reino Unido (se distingue en este caso entre la información oficial, secreto y alto secreto).

Información disponible en: Almagro, Luis, 2019: “La clasificación de los datos”, *Revista White Paper Series*, Edición 6, 10-11.

23 Almagro, Luis, 2019, “La clasificación de los datos”, *Revista White Paper Series*, Edición 6, 12.

24 *Ibid.*

25 *Ibid.*

26 Amazon Web Services (AWS), *Data Classification* (Amazon, 2020), https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf

en los contratos de *cloud*, como el consentimiento previo y por escrito del titular de los datos personales o que la empresa responsable informe a los titulares sobre las condiciones de su tratamiento, incluida la posibilidad de que estos sean almacenados en una nube, cuyos servidores podrían encontrarse en el extranjero.

Atendido lo anterior, es necesario definir el concepto de datos personales para distinguirlos de aquellos datos cuyo tratamiento no tiene una regulación normativa especial. Para esto, tomaremos la definición del Reglamento General de Protección de Datos, con el objeto de optar por un instrumento referente en esta materia, independiente que puedan presentar variaciones mínimas respecto del resto de las legislaciones en Latinoamérica. Así pues, los **datos personales** consisten en *“toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador²⁷”*. Por ende, lo esencial es que se trate de información que identifique o permita identificar la identidad de una persona natural, como su imagen, su número de identificación nacional, el número de un pasaporte, nombre, domicilio, nacionalidad, sexo, hábitos de compra, dirección IP, etc.

A *contrario sensu*, serán **datos no personales** toda información que no identifica o no permita identificar -ni aún con ingeniería inversa- a una persona natural. Por ejemplo, información de las empresas o modelos de negocios, contabilidad de una empresa, datos anonimizados, datos estadísticos, estudios científicos, etc.

En general, el tratamiento de la información no personal no siempre se encuentra regulada en las legislaciones. Sin perjuicio que, en ciertas circuns-

tancias, los datos no personales pueden ser tanto o más valiosos que los datos personales, como en los casos que están protegidos por secretos empresariales, constituyen un *know-how* valioso de la empresa, consisten en información financiera, etc. Por lo mismo, pese a que su procesamiento no requiere de una fuente de licitud, ni tampoco tiene otro tipo de limitaciones -como requisitos para su transferencia internacional o derechos de acceso, información, rectificación, etc.-, es igualmente importante entender que su contenido puede requerir de medidas especiales en un contrato de almacenamiento en la nube.

5.3 Tratamiento de datos personales

Ahora bien, retomando la importancia del marco normativo que regula el contenido de los datos personales, en este punto, es necesario desarrollar algunos aspectos esenciales a considerar en el tratamiento en este tipo de datos y, otras medidas que permiten facilitar el tratamiento de datos, como la “anonimización”, cuando el objetivo del procesamiento no necesite identificar a personas naturales. De igual forma, se relacionarán los conceptos “responsable del tratamiento” y “encargados del tratamiento” de datos personales, con las partes de un contrato de *cloud*, ya que, como se explicará a continuación, el almacenamiento en la nube será una de las tantas formas en que se puede realizar el tratamiento de datos personales.

El **tratamiento de datos** se define como *“cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión,*

27 Reglamento General de Protección de Datos (“GDPR”), Artículo 4, N°1.

*limitación, supresión o destrucción*²⁸”. Es decir, el tratamiento de datos puede consistir en cualquier actividad sobre los datos, desde la recolección hasta su transferencia, ya que el objetivo es ofrecer un concepto lo suficientemente amplio, capaz de incluir todo tipo de acciones y ofrecer mayor protección a los titulares de dichos datos.

En este punto, cabe señalar que, precisamente, un contrato *cloud*, a través del cual se regula el almacenamiento de datos personales en la nube, cae dentro de la definición del tratamiento de datos personales y, como tal, debe ajustarse a las exigencias impuestas por la legislación aplicable. Asimismo, como consecuencia de esta calificación, necesariamente debemos concluir que la relación entre las partes del contrato de *cloud* adquirirá una nueva dimensión si se almacenan datos personales, pues el cliente de los servicios de *cloud* será el responsable del tratamiento y, el proveedor del servicio será un encargado del tratamiento.

En efecto, el responsable del tratamiento es la “*persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento*”²⁹ y, el encargado de los datos es la “*persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento*”³⁰. En virtud de estas definiciones, en la mayoría de las jurisdicciones, se regula la relación entre el responsable y el encargado del tratamiento, como un **mandato** mediante el cual, el primero le encarga al segundo, la realización de una determinada gestión, como el almacenamiento de dichos datos en la nube³¹.

Como consecuencia de lo anterior, el responsable del tratamiento y, para efectos de este artículo, el cliente del servicio de *cloud*, será el único obligado a cumplir con los requisitos de licitud del tratamiento o garantizar, a los titulares de los datos, el ejercicio oportuno de sus derechos de Acceso, Rectificación, Cancelación y Oposición³² (en adelante, derecho “ARCO”). Sin perjuicio que, en este artículo, no se tratarán específicamente los requisitos para realizar un tratamiento de datos personales adecuado, pues no es el objeto de estudio de la investigación, sí es relevante destacar las obligaciones que le empecen al responsable del tratamiento. Esto porque, por una parte, no son exigibles al encargado del tratamiento que, en este caso concreto, será el proveedor de servicios de *cloud*; y, por otra parte, porque naturalmente invita a considerar ciertas medidas de disponibilidad de la información en la nube, para que el responsable pueda cumplir en forma eficiente y eficaz con las obligaciones impuestas en las legislaciones de protección de datos personales. Por ejemplo, será conveniente asegurar en el contrato que la información de la nube se encuentre disponible, en todo momento, si contiene datos personales, considerando los plazos que establecen las distintas legislaciones para dar respuesta al ejercicio de los derechos ARCO.

Por otro lado, otro aspecto relevante a considerar en materia de contratos de *cloud*, cuando recaigan sobre el almacenamiento de datos personales, es el hecho de que esto constituya una transferencia internacional de datos. En general, las legislaciones exigen requisitos especiales cuando se realice una transferencia de datos de un país a otro, o a una organización internacional, por ejemplo, que esto sea conocido y autorizado expresamente por

28 Reglamento General de Protección de Datos (“GDPR”), Artículo 4, N°2.

29 Reglamento General de Protección de Datos (“GDPR”), Artículo 4, N°7.

30 Reglamento General de Protección de Datos (“GDPR”), Artículo 4, N°8.

31 En Chile, esta figura está regulada en el artículo 8 de la Ley N°19.628 sobre la “Protección de datos de carácter personal”.

32 En general, se habla de los derechos ARCO. Sin embargo, en legislaciones más avanzadas en estas materias, como la Unión Europea, existen otros derechos como el de información, limitación del tratamiento, derecho al olvido, etc.

su titular. Sin embargo, en la normativa chilena vigente, esto aún no se encuentra regulado, por lo que no representa un aspecto relevante, pese a que una buena práctica de tratamiento de datos personales igualmente impone al responsable del tratamiento, la obligación de informar sobre esta posible transferencia a los titulares de los datos personales.

Con todo, sobre este punto cabe destacar que una **transferencia internacional de datos** en un contrato de *cloud* es bastante probable, porque usualmente los servidores de la nube se encuentran en un país distinto al del cliente y, en especial, de donde provienen los datos personales recolectados por el responsable del tratamiento. Por tanto, pese a la falta de corporalidad de la información ubicada en la nube, el simple hecho de que el servidor se encuentre en un país distinto implica, para algunas legislaciones, una transferencia internacional de datos. Por ende, esta información debe ser considerada antes de celebrar el contrato de *cloud* para evitar que el cliente del servicio de almacenamiento infrinja las normas de protección de datos personales al subir la información a la nube.

Por último, también es necesario mencionar que, en virtud de todas las exigencias impuestas para el tratamiento de datos personales, en ciertas ocasiones, los clientes de servicios *cloud* pueden optar por transformar sus datos personales en datos no personales, para mitigar los riesgos jurídicos en su procesamiento. En efecto, es posible, a través de un proceso de **anonimización de datos**, en virtud del cual, se efectúan procesos irreversibles que impiden volver a identificar a una persona natural; y, una vez que esto ocurre, ya no es objeto de la regulación especial.

Atendido lo anterior, es posible concluir que, comprender el alcance de la computación de nube y la naturaleza jurídica del contrato que la regule, no es suficiente para mitigar todos los riesgos que puedan producirse cuando se contrata esta solución tecnológica. En efecto, debido al gran valor de los datos y la información que se puede extraer de ellos, es absolutamente indispensable considerar sus características al momento de celebrar un contrato de *cloud*. Pues, el soporte, la importancia y el contenido de los datos, nos pueden orientar para exigir mejores condiciones en los contratos de *cloud*, ya sea cuando elegimos un proveedor y modalidad de almacenamiento de nube, negociamos el contrato -si es posible- o, nos encontramos en la fase de ejecución del contrato de *cloud*.

De esta manera, en la siguiente sección, se desarrollarán las ventajas y riesgos presentes en la figura de *cloud*, para finalizar exponiendo las principales herramientas jurídicas a considerar en los contratos de *cloud*, para mitigar los riesgos identificados, tanto desde el punto de vista de la solución tecnológica, como desde los datos almacenados en la nube.

6. Ventajas y riesgos de la transición a la computación en la nube

El constante aumento de demanda y gasto en recursos de TI, por parte de las empresas, responde a una necesidad inmediata de estas a transitar hacia un modelo basado en lo digital que les permita mantenerse vigentes y competitivas en su industria. De hecho, el estudio de *International Data Corporation* prevé que, para finales de este año, 2021, el 75%³³ de las grandes empresas latinoamericanas implementarán un cambio hacia infraestructuras y aplicaciones centradas en la nube.

33 Villars, Rick y otros, 2021. "IDC FutureScape: Worldwide IT Industry 2021 Predictions" *International Data Corporation*. Acceso 28 de mayo de 2021. Disponible en: <https://www.idc.com/getdoc.jsp?containerId=US46942020&pageType=PRINTFRIENDLY>

Con las cifras anteriores a la vista, está claro que los servicios de *cloud* son beneficiosos para las compañías. Dentro de las ventajas de contratar este tipo de servicios encontramos: (i) La posibilidad de externalizar servicios de IT a bajo costo, pues el cliente paga conforme a su nivel consumo; (ii) Servicio flexible, que permite escalar y aumentar o disminuir el consumo de acuerdo con las necesidades reales de la empresa; (iii) Servicio de fácil acceso, no se necesita, en general, invertir en la instalación de softwares sofisticados para comenzar a trabajar con ellos.

No obstante, también existen riesgos asociados a este tipo de solución tecnológica, que debemos tener en cuenta al momento de contratar servicios de *cloud*. El problema se origina en que un tercero, completamente ajeno a la empresa, puede tener el control de la plataforma en que se gestiona toda su información relevante o sensible de una organización, genera una serie de alertas, sobre todo en materia de seguridad.

Otro riesgo para las empresas, derivado de la naturaleza de la tecnología empleada, es la dependencia que se genera con el proveedor de los servicios de almacenamiento. Pues, al tratarse de contratos de largo plazo, o de tracto sucesivo que se renuevan automáticamente, se genera una dependencia con el proveedor de los servicios al aumentar el volumen de información almacenada en la nube, lo que hace difícil resolver o terminar anticipadamente la relación contractual en caso de incumplimientos a las obligaciones de seguridad o confidencialidad del proveedor. Además de los costos asociados a la implementación de nuevos sistemas de trabajo colaborativo, que conllevan inversión en capacitación de personal y la respectiva fase de “marcha blanca” hasta que el entorno de trabajo se acostumbre a los cambios.

Por lo mismo, para mitigar este tipo de riesgos asociados a la naturaleza de la tecnología contratada, se recomienda estudiar el alcance de la mo-

dalidad de *cloud*, en función del tipo de datos e información que se busca almacenar. Pues, como ha sido explicado en la primera sección, no es indiferente que la empresa, usuaria de la nube, solo contrate el uso de una infraestructura o un servicio para procesar y almacenar sus datos.

Asimismo, es diferente someterse a un régimen de términos y condiciones que no se puede negociar e impone al usuario, que el proveedor del servicio pueda acceder o usar la información almacenada en la nube confidencial. Por lo tanto, es indispensable comprender la naturaleza de la modalidad de *cloud*, el tipo de información que se busca almacenar y los objetivos de la empresa para negociar -si es que es posible- o celebrar un contrato que regule este tipo de servicio informático en la forma más eficiente posible.

En primer lugar, si toda o parte de la información que se pretende almacenar en la nube es confidencial y no debe ser conocida por el proveedor del servicio, sea porque contiene datos sensibles o datos personales sobre los cuales no se tiene autorización para compartir información con tercero, se recomienda comprobar si existe una cláusula que limite el acceso del prestador del servicio a la información, si el contrato no se puede negociar. Por el contrario, en caso de que el contrato de *cloud* pueda ser libremente discutido entre las partes, ya sea porque se está contratando una solución customizada o porque existe mayor igualdad entre los futuros contratantes, se recomienda incorporar esta limitación respecto del acceso la información del proveedor.

En segundo lugar, considerando el nivel de importancia de la información almacenada en la nube, también se recomienda regular -en la medida de lo posible- el nivel de cuidado que se le exigirá al prestador del servicio frente a posibles filtraciones, pérdidas o robos de los datos almacenados. Pues, a mayor nivel de importancia, naturalmente se debiese exigir mayor diligencia para

cumplir con su deber de conservación de la cosa “entregada”. De igual forma, será relevante definir los alcances de las obligaciones del prestador del servicio vinculadas con las copias de seguridad, reacción o notificación en caso de incidentes de seguridad y situaciones en imprevistas, que pongan en riesgo la integridad de la información almacenada en la nube, porque en la mayoría de los casos, el proveedor de *cloud* es el único encargado de generar copias de seguridad de la información almacenada en la nube.

En tercer lugar, considerando el contenido de los datos almacenados en la nube, también se recomienda tomar medidas de seguridad para proteger datos cuya filtración es más grave según la normativa vigente. Por ejemplo, en el caso de los datos personales, la negligencia del proveedor de servicios de *cloud* puede significar una infracción normativa a la Ley de Protección de Datos Personales.

Por otro lado, el ejercicio de los derechos de los titulares de datos personales, que consagran las normas sobre protección de datos personales, también le impone al usuario de los servicios de *cloud* la necesidad de exigir al proveedor del servicio que asegure el acceso ininterrumpido de la información almacenada en la nube, pues, de esta forma, se puede responder dentro de plazo el ejercicio del derecho de acceso de un titular. A su vez, la ubicación del servidor puede implicar una transferencia internacional de datos personales, lo cual, en ciertas jurisdicciones, requiere autorización expresa del titular.

Por último, aunque no menos importante, como vimos en el apartado sobre tratamiento de datos personales, dado que la relación de un contrato de *cloud* necesariamente se transformará en un mandato para realizar tratamiento de datos personales, por cuenta y riesgo del cliente del servicio de almacenamiento en la nube, también es recomendable celebrar el mandato por escrito, que en la generalidad de los casos debiera incluirse en el mismo texto

del contrato *cloud*. Sin perjuicio de los deberes que impone la Ley de Protección de Datos Personales al responsable del tratamiento de datos, como la obtención del consentimiento, informar sobre las condiciones y objetivos del tratamiento, etc.

7. Conclusiones

La transformación digital ha incrementado la importancia de analizar el contrato de *cloud* desde una perspectiva integral, que incluya tanto los aspectos jurídicos, como el valor de la información que se busca almacenar en la nube, porque justamente el traslado de los activos intangibles más valiosos a espacios virtuales, privados o públicos, impone la necesidad de definir estrategias adecuadas para proteger dichos bienes y regular el servicio de almacenamiento en la nube.

En este sentido, en el presente artículo se ha demostrado que contratar una infraestructura o un servicio de nube, establecer obligaciones de confidencialidad, seguridad, respaldos de información o restricción de acceso a los datos por parte del proveedor del servicio son solo un ejemplo de cómo una mirada integral al servicio de almacenamiento en la nube permite identificar y mitigar riesgos asociados a la filtración, pérdida o robo de información.

Por consiguiente, es primordial considerar en el análisis de los contratos de este tipo de servicio informáticos, las condiciones de la nube, las necesidades tecnológicas de la empresa, el tipo de datos que se estarán alojando en la nube y las normas civiles o mercantiles que puedan ser aplicables en la prestación de este servicio informático. Pues, los términos y condiciones del contrato de *cloud* no sólo se traducen en las normas contractuales que resguardan el activo más valioso en la era digital, los datos e información, sino también en la forma en que el usuario de este servicio puede cumplir

con obligaciones legales íntimamente relacionadas con el contenido o tipo de dato objeto del servicio de almacenamiento en la nube. Por ejemplo, el cumplimiento de obligaciones relacionadas con el ejercicio de derechos de los titulares de datos personales o el respaldo y confidencialidad de información sensible o crítica para el funcionamiento de una empresa.

En consecuencia, es posible concluir que, el contrato de *cloud* no puede analizarse en forma aislada al valor de los datos del usuario del servicio y de las exigencias normativas que están sujetos los mismos, toda vez que estos son un activo de la empresa, que cada vez adquiere mayor valor en la economía digital. Por ende, deben tenerse a la vista al momento de determinar qué requisitos o prestaciones se les exigirán a los prestadores de servicios y, especialmente, cuál va a ser el estándar de cuidado del proveedor de este servicio informático, ya que, solo de esa manera, podremos obtener el mayor provecho de las ventajas de este tipo de soluciones tecnológicas.

Bibliografía

Villars, Rick, Holly Muscolino, Wayne Kurtzman, Ritu Jyoti, Dan Vesset, Mario Morales, Jennifer Cooke, Deepak Mohan, Jonathan Lang, Mickey North Rizza, Ashish Nadkarni, Carrie MacGillivray, <<Worldwide IT Industry 2021 Predictions>>. *IDC FutureScape* (2021) Disponible en: <https://www.idc.com/getdoc.jsp?containerId=US46942020&pageType=PRINTFRIENDLY>. 2021. International Data Corporation.

Mell, Peter, Timothy Grance. <<The NIST Definition of Cloud Computing>>. *Instituto Nacional de Estándares y Tecnología* (2011). Acceso 27 de mayo de 2021. Disponible en: <http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf>

Navas, Susana. <<El almacenamiento de los datos “cloud computing” al ADN Sintético>> En *Mercado Digital Principios y Reglas Jurídicas* (2016). Valencia: Tirant Lo Blanch, p. 42.

Ontiveros, Emilio, Verónica López. <<Economía de los Datos>>. *Riqueza 4.0* (2017). Madrid: Ediciones por Ariel y Fundación Telefónica.

Jones, Brian, *Digitaliza tus datos analógicos para un trabajo más rápido y eficiente*. (Microsoft, 2019) <https://www.microsoft.com/es-cl/microsoft-365/blog/2019/05/29/insert-data-from-picture-take-analog-data-digital/> .

Puyol, Javier. <<Aproximación jurídica y económica del Big Data>> *En Tirant Lo Blanch* (2015), p. 9, 10.

Almagro, Luis <<La clasificación de los datos>> *Revista White Paper Series* (2019), Edición 6, 12.

Amazon Web Services (AWS), *Data Classification* (Amazon, 2020), https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf