CLOUD COMPUTING Y SEGURIDAD: DESPEJANDO NUBES PARA PROTEGER LOS DATOS PERSONALES

CLOUD COMPUTING AND SECURITY: CLEARING CLOUDS TO PROTECT PERSONAL DATA

RODOLFO HERRERA BRAVO [*]
Universidad de Concepción
Chile

RESUMEN

Una fuerte tendencia actual en gestión tecnológica se basa en modelos de servicios digitales a través de Internet, esquema conocido como *cloud computing*. Su materialización a través de contratos abre la posibilidad de externalizar el tratamiento de bases de datos personales a un tercero, disminuyendo considerablemente el control del responsable del banco de datos, especialmente en cuanto al nivel de seguridad que pasa a tener esa información. Por tal motivo, en este trabajo se destacan ciertas ideas fundamentales sobre el papel de la legislación de protección de datos personales en estos modelos contractuales, aclarando el rol que asumen las partes y las obligaciones legales que les rigen.

Palabras clave: *datos personales, cloud computing, privacidad por diseño, seguridad de información.*

ABSTRACT

A strong current trend in technology management is based on models of digital services over the Internet, scheme known as cloud computing. Its materialization through

[*] Abogado. Master en Derecho Informático por la Universidad Complutense de Madrid. Magíster en Derecho Público con Mención en Derecho Constitucional por la Pontificia Universidad Católica de Chile. Profesor del Magister en Derecho de la Facultad de Ciencias Jurídicas de la Universidad de Concepción, Chile y del Diplomado en contratación pública de la Carrera de Derecho de la Universidad Viña del Mar, Chile. Dirección postal: Badajoz N°100, Oficina N°1110, Las Condes, Santiago. Correo electrónico: rodolfo.herrera@vtr.net

contracts opens the possibility of outsourcing the processing of personal databases to a third, significantly reducing control responsible for the database, especially regarding the level of security is going to have that information. Therefore, this study highlights certain fundamental ideas about the role of legislation for the protection of personal data in such contractual models, clarifying the role which the parties and the legal obligations governing them.

Key words: *personal data, cloud computing, privacy by design, information security.*

I. INTRODUCCIÓN: EL MODELO DE GESTIÓN TECNOLÓGICA EN LA NUBE (*CLOUD COMPUTING)*

La influencia de Internet como paradigma tecnológico es evidente en las estrategias de negocio. Ella ha facilitado la convergencia de dispositivos y la prestación de servicios digitales a medida. Además, entre otros cambios, ha permitido aligerar a las empresas gracias a la externalización, que amplíen su cobertura y presencia con la tecnología móvil y que disminuyan sus costos mediante la deslocalización.

En este esquema, la Nube o *cloud computing* constituye uno de los principales modelos de gestión tecnológica hacia el cual se dirigen las organizaciones, con proyecciones de crecimiento sostenido[1]. En términos generales consiste en ofrecer acceso a amplios servicios digitales a través de Internet, según demande el cliente, desde cualquier dispositivo periférico interconectado para recibir en su caché temporal los datos almacenados permanentemente en el proveedor.

Ahora bien, a través de la Nube se proveen distintos servicios que suelen ser agrupados en:

i) Software como servicio (SaaS): acceso a aplicaciones del proveedor, administradas, actualizadas y mantenidas por éste, pero ejecutadas por el cliente en sus dispositivos. Una variable es el Dato como servicio (DaaS), que permite el acceso a grandes volúmenes de datos a demanda del cliente.

ii) Plataforma como servicio (PaaS): acceso a todas o algunas de las fases del ciclo de

[1] El estudio *The cloud revolution,* publicado por Cloud Hypermarket en septiembre de 2011, señala datos interesantes. Por ejemplo, actualmente existen más de 33.000 *data centers* en el mundo y más de 50 millones de servidores. Se calcula que el año 2013 el *cloud computing* ascenderá a más del tercio del total de inversión informática mundial. Además, más del 70% de los usuarios de estos servicios estima que la Nube ha simplificado sus procesos de Tecnologías de Información, ha mejorado su relación con clientes y ha reducido costos. Finalmente, el 56% de los usuarios de Internet usan servicios webmail; el 34% almacena fotos personales en línea; el 29% utiliza aplicaciones en línea; el 7% almacena videos personales; el 5% paga almacenamiento de archivos en línea; y el 5% respalda el disco duro en línea. Cloud Hypermarket, *The cloud revolution,* 2011. Disponible en: http://www.cloudhypermarket.com/whatiscloud/CloudUptake. [Consulta: 30 noviembre 2011].

desarrollo y pruebas de software o a la administración de contenido en la infraestructura del proveedor.

iii) Infraestructura como servicio (IaaS) o Hardware como servicio (HaaS): acceso a servicios estandarizados en los que el proveedor ofrece almacenamiento, procesamiento, redes y equipos para manejar tipos específicos de cargas de trabajo del cliente.

La elección de alguno de estos servicios permite a las empresas mayor integración, reducción de costos en hardware y software, mayor capacidad de adaptación, mejor respuesta ante incidentes y recuperación de desastres. Del mismo modo es un modelo interesante para los órganos públicos (*G-cloud)* y para empresas dinámicas en su primera etapa de crecimiento, que no pueden establecer grandes estructuras tecnológicas, pero que requieren alta disponibilidad de servicios, con seguridad y a un costo que puedan manejar.

A su vez, para llevar a cabo un servicio *cloud computing* el proveedor puede desarrollarlo en distintos tipos de redes, lo que abre alternativas a los clientes más acordes con su realidad. Por ejemplo, optar por redes públicas manejadas por terceros, con trabajos de muchos clientes diferentes que se mezclan en los servidores, aunque garantizándose su confidencialidad. También existen redes privadas en donde la infraestructura del proveedor la maneja un solo cliente o nubes híbridas en las que el cliente tiene exclusividad de una parte y comparte otras, aunque de forma controlada. De hecho, es tal la diversidad de escenarios que ya han comenzado a ofrecerse servicios de corretaje de Nubes, para aprovechar la eficiencia en un mercado global y elegir los mejores servicios en distintos *data center.*

II. PRONÓSTICO PARA LA SEGURIDAD: AMENAZA DE TORMENTA

Un modelo tecnológico como el descrito se sustenta en la externalización de servicios vinculados al núcleo del negocio que van, por ejemplo, desde el acceso a servidores de un proveedor para utilizar aplicaciones para la gestión diaria, hasta la entrega de activos de información a ese tercero para su almacenamiento y procesamiento.

Por ese motivo el *cloud computing* genera dependencia para quien lo contrata porque los servicios están centralizados en el proveedor y es necesario contar con acceso a Internet para que las aplicaciones o la información estén disponibles. Asimismo, el cliente pierde exclusividad sobre la información que externaliza, asumiendo como un nuevo riesgo las posibles vulnerabilidades que presente el proveedor ante amenazas de ataques. Es más, como el modelo hace necesario que los datos circulen por nodos de Internet cada vez que se requiera un servicio en la Nube, eventualmente podrían ocurrir intercepciones por terceros no autorizados.

Con esta participación de un proveedor de servicios en operaciones críticas que demanda una organización, resulta innegable que el cliente de la Nube se expone peligrosamente a riesgos cuya ocurrencia puede llegar a costarle, incluso, su desaparición. En efecto, si un incumplimiento del proveedor se traduce en la indisponibilidad o interrupción de los servicios que presta el cliente, incluso por fallas técnicas o fenómenos externos de fuerza mayor, podría impedir la continuidad del negocio de éste.

También podrían existir fugas de los datos que el cliente entregó al proveedor, hecho que a lo menos minaría la confianza en aquél y, según el caso, podría provocar un daño irreparable en imagen. No olvidemos que es tal el impacto que puede experimentar una compañía que aparezca públicamente como víctima de espionaje informático, accesos no autorizados a sus sistemas o de tráficos no autorizados de bases de datos, que suelen no perseguirse penalmente elevando la cifra negra de estos ilícitos.

Además, si sumamos la mayor movilidad en la prestación de los servicios, el acceso a ellos desde múltiples dispositivos y su operación a través de flujos de datos, se presentan amenazas contra la integridad y la confidencialidad de la información, por ejemplo, a través de alteraciones no autorizadas de datos o vulneración de controles de identidad y autenticación.

Dentro de este panorama nuboso y amenazante existe una especial preocupación sobre la seguridad de los datos personales de terceros que administra una empresa, cuando decide tratarlos bajo modelos de *cloud computing*. ¿Estos datos gozan de algún tipo de resguardo jurídico? ¿Tiene alguna limitación legal el externalizar el tratamiento de datos personales, por ejemplo de una base de datos de clientes?

Cloud computing es una expresión tecnológica de nuestras comunidades reticulares. Ellas se componen, entre otros, por flujos de datos cuyo contenido concierne a personas naturales, sea porque las identifica, caracteriza o describe. Son los denominados datos de carácter personal, una categoría de la mayor relevancia por su incidencia en los derechos fundamentales de sus titulares, de hecho, gozan de un régimen de garantía especial frente al tratamiento que otros puedan realizar con ellos.

Es evidente que la libre circulación de datos personales debe ser reconocida y garantizada como un principio indispensable para nuestra actual forma de convivir. Sin embargo, no sólo hay que reconocer la facultad de recolectar, procesar y comunicar datos personales, sino también la de exigir simultáneamente un alto nivel de respeto hacia el titular de esa información, porque si ello no ocurriera, la persona a quien conciernen los datos vería disminuida su capacidad de control frente a usos abusivos.

En ese sentido, si los datos personales se transan con total prescindencia de la voluntad y conocimiento de su titular, por ejemplo luego de externalizar los servicios de procesamiento de bases de datos en la Nube, se expone en exceso una multiplicidad de huellas sobre los vínculos que mantiene una persona, la información que selecciona, el detalle de sus comunicaciones, su localización física, sus gustos, necesidades, creencias y pensamientos. Por lo tanto, la amenaza no se limita sólo a las molestias y perjuicios que se sufren cuando las direcciones de correo electrónico o los números de teléfono

circulan entre las empresas y se utilizan para enviar publicidad no solicitada, bajo la forma de *spam.* También hay cuestiones más graves, por ejemplo al revelar situaciones patrimoniales o características físicas o morales íntimas del titular que dan pie a tratos discriminatorios o inhibición en el ejercicio libre de los derechos.

III. LA LEY N°19.628 Y SU APLICACIÓN A SERVICIOS EN LA NUBE

A partir de la década de los setenta se han dictado legislaciones específicas sobre protección de datos personales[2]. Ellas reconocen que al no ser viable el control sobre los equipos que contienen las bases de datos se debe permitir el tratamiento, pero garantizando al titular de datos el acceso a éstos para que conserve un cierto control. Es decir, estos sistemas jurídicos son igualmente celosos en conciliar el control del titular sobre sus datos y en reconocer la libre circulación de éstos, evitando que su protección se transforme en un obstáculo excesivo.

En Chile, la Ley N° 19.628, sobre Protección de la Vida Privada se hace cargo de establecer en qué condiciones deben utilizarse las bases de datos personales en servicio *cloud computing.* Por supuesto, no menciona expresamente a este modelo tecnológico, pero constituye la normativa legal aplicable al tratamiento de datos personales que se realice en virtud de estos servicios.

En términos generales este cuerpo legal comienza reconociendo que toda persona puede efectuar el tratamiento de datos personales de otro, siempre que lo haga de manera concordante con esa ley y para finalidades permitidas por el ordenamiento jurídico[3]. De esta forma se excluye *ab initio* toda interpretación que pretenda mirar a los derechos individuales del titular como un muro infranqueable para la circulación de los datos. Esto significa que en este sistema jurídico de garantía el derecho a tratar datos requiere, necesariamente, que se respeten límites precisos dados por la Ley de Protección de la Vida Privada, la finalidad lícita del tratamiento, y el pleno ejercicio de los derechos fundamentales de los titulares de datos y de las facultades específicas que se le reconocen[4].

[2] Una primera generación de este tipo de leyes se ejemplifica con los modelos implantados inicialmente por la *Datenschutz*, del Land de Hesse, en 1970; la *Data Lag* de Suecia, en 1973; o la *Landesdatenschutzgesetz*, de Renania-Palatino, en 1977. En una segunda generación destacan la *Privacy Act*, de Estados Unidos de 1974; la *Informatique aux fichiers et aux libertés* de Francia, de 1978; y las Constituciones de Portugal y España, de 1976 y 1978, respectivamente. Luego, durante los años ochenta destacan el Convenio europeo N°108, de 1981; la *Data Protection Act* de Inglaterra, de 1984 y toda la elaboración legislativa de tercera generación, bajo el modelo de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[3] Ley N°19.628, art.1°, inciso segundo: *"Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce".*.

[4] Los límites legales a la facultad de tratar datos personales sin vulnerar el ejercicio de otros derechos, constituyen para el profesor Raúl Bertelsen una reiteración del principio de supremacía constitucional consagrado en el artículo

Ahora bien, en la relación de la Ley N°19.628 con los servicios *cloud computing* hay que tener presente que ese ordenamiento jurídico no actúa como un régimen de seguridad de la información en general, sino que se circunscribe exclusivamente a la existencia de datos personales. El legislador, siguiendo la tendencia internacional dominante[5], los define generosamente como los datos *"relativos a cualquier información concerniente a personas naturales, identificadas o identificables"* [6]. Con ello incluye no sólo aquella información objetiva sobre una persona de la especie humana, como su nombre, domicilio, profesión o grupo sanguíneo, sino también aquella referida a una opinión o evaluación subjetiva, verídica o no[7], esté o no demostrada[8]. Lo importante es que el dato haga referencia a la identidad de la persona, sus características o su comportamiento, o bien, se utilice para determinar o influir en la manera en que se la trata o evalúa[9].

"Cualquier información" también se interpreta ampliamente respecto del formato, porque el dato personal puede incluir texto alfanumérico, sonidos o imágenes, como ocurre con aquellas que se obtienen por medio de un sistema de cámaras de video vigilancia, en la medida que las personas grabadas sean reconocibles. Incluso puede tratarse de datos biométricos como las huellas dactilares u otros rasgos físicos o fisiológicos de la persona como el grupo sanguíneo o el iris de sus ojos. Además, no sólo comprende datos en soporte digital sino también en papel u otro análogo.

Por último, la persona natural a quien concierne el contenido del dato puede estar identificada si se distingue dentro de un grupo o puede ser identificable a través de datos identificadores que demuestran una relación cercana con una persona, tales como la apariencia –contextura, vestimenta– o alguna cualidad no perceptible de inmediato –profesión, cargo u otra–. Evidentemente, el tipo y número de identificadores necesa-

6° de la Constitución Política de la República. A su juicio, el tratamiento de datos es una lícita actividad económica lucrativa, cuyo marco legal se encuentra contenido en el artículo 1° de la Ley N° 19.628, en concordancia con el derecho a desarrollar cualquier actividad económica que no sea contraria a la moral, al orden público o a la seguridad nacional, respetando las normas legales que la regulen, reconocido en el artículo 19 N°21, inciso primero, de la Constitución Política de la República. BERTELSEN REPETTO, Raúl, "Datos personales: propiedad privada, libre iniciativa particular y respeto a la vida privada", en *Cuadernos de Extensión Jurídica,* 5, (2001), pp.113-118.

[5] Dicha tendencia la marca la normativa europea sobre protección de datos, que constituye el estándar internacional de mayor exigencia mundial, sobre todo a partir de las reglas que establece para la existencia de flujos transfronterizos de datos con países extra comunitarios, quienes han adaptado sus legislaciones para facilitar los lazos transaccionales con la Unión Europea. Al respecto destaca la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; y el Convenio N°108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.

[6] Ley N°19.628, artículo 2°, letra f).

[7] De hecho, en caso de falsedad el titular goza de la facultad de exigir su corrección.

[8] Las afirmaciones subjetivas sobre una persona conforman parte significativa de los mercados de datos existentes, sobre todo en materia crediticia y laboral. Por ejemplo, la calificación de un cliente como "sujeto riesgoso para el otorgamiento de un crédito", tras evaluarse su comportamiento como deudor.

[9] Documento N° WP 105, del Grupo de Trabajo: "Documento de trabajo sobre las cuestiones relativas a la protección de datos relacionados con la tecnología RFID", adoptado el 19 de enero de 2005, p.8; citado por el Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio de 2007, por el Grupo de Trabajo del Artículo 29, de la Unión Europea. [en línea], p.11. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf, [Consulta: 7 de abril 2011].

rios para distinguir a una persona del resto dependerá del contexto de la situación y que sean razonablemente empleados para ese objetivo, teniendo en cuenta diversos factores, tales como lo costoso de la identificación, el tiempo de conservación de los datos, los intereses individuales en juego o los riesgos involucrados y, en especial, la finalidad del tratamiento.

Por otra parte, para aplicar la Ley N° 19.628 a un servicio *cloud computing* es necesaria la presencia de un registro o banco de datos personales, esto es, un *"conjunto organizado de datos de carácter personal, sea automatizado o no*[10] *y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos"* [11]. Ello significa que no todo documento con información personal se rige por esta legislación, se excluye la documentación no estructurada porque no organiza los datos personales para su cruce y utilización.

Por lo tanto, esta legislación, más que proteger datos personales en sí mismos, tiene por objeto regular cómo se utilizan. En ese sentido, sus normas se aplican cuando existe algún tratamiento sobre los datos, es decir, cuando se realiza *"cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma"* [12]. Sin duda, con un concepto tan amplio como éste, es fácil encontrar algún tipo de tratamiento de datos al contratar un servicio *cloud computing*, si el proveedor almacena, respalda o procesa la base de datos del cliente.

IV. EL TRATAMIENTO DE DATOS EN UN MODELO DE NUBE

La aplicación de esta normativa en un esquema de contratos *cloud computing* se comprende de mejor manera en la medida que se distinguen los roles de cada parte desde el punto de vista de la protección de datos personales y se establece quién efectúa el tratamiento de datos.

Al respecto, observamos tres actores en la Nube: por un lado, el cliente que contrata estos servicios y que entrega una base de datos personales a la contraparte. Del otro, el proveedor del servicio, quien recibe esos registros dentro de la información asociada a la ejecución del contrato, por ejemplo, para almacenarla, para realizar cruces, comparaciones o evaluaciones, o para comunicar datos a terceros si así lo contempla la prestación contratada. Por último, están las personas naturales a quienes se refieren los datos

[10] Los registros de datos personales pueden ser manuales o en soporte papel –como un sistema organizado de fichas, por ejemplo–, porque el concepto legal no es exclusivo de las bases de datos electrónicas, aunque ellas son las que despliegan el mayor potencial de uso y de riesgo.

[11] Ley N°19.628, artículo 2, letra m).

[12] Ley N°19.628, art. 2, letra o).

contenidos en la base que entrega el cliente al proveedor.

Desde el punto de vista de la Ley N°19.628, el cliente *cloud computing* que entrega la base de datos personales al proveedor es el responsable del registro o banco de datos, es decir, *"la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal"* [13]. Efectivamente, en él descansa la decisión de externalizar algún tipo de tratamiento a través de servicios en la Nube y, precisamente, la materializa en el contrato que suscribe con el proveedor, estableciendo la forma en que ello se desarrollará.

En tal calidad, el cliente asume las obligaciones específicas que dispone esa legislación, tales como el respeto de la finalidad del tratamiento[14] y la calidad de los datos, el deber de informar al titular del dato personal y la obligación de cuidado, especialmente en este caso, porque su entrega a terceros en virtud de una externalización encierra uno de los mayores riesgos para el titular, debido a que el control que puede ejercer sobre ellos se distancia o incluso desaparece por completo si no se respetan mínimas garantías de seguridad y debida diligencia al utilizarlos.

Cabe advertir que para el legislador chileno no es determinante la titularidad sobre la base de datos para ser el responsable del registro[15], lo importante es la capacidad para decidir sobre los fines y medios del tratamiento. En el *cloud computing* esa situación sólo ocurriría en el caso del cliente y no del proveedor, ya que este último efectúa un tratamiento por cuenta del cliente, sin que sus decisiones puedan exceder de lo acordado contractualmente con éste. Dicho de otro modo, el proveedor no actúa como responsable del banco de datos sino como un mandatario de éste.

El papel de este mandatario –desarrollado con detalle en otras legislaciones bajo la denominación "encargado del tratamiento"–, lamentablemente tiene una escueta mención en la Ley N° 19.628. El artículo 8° se limita a reenviar el tema al derecho común al señalar: *"En el caso de que el tratamiento de datos personales se efectúe por mandato, se aplicarán las reglas generales".* A partir de ello, las disposiciones de tratamiento de datos

[13] Ley N°19.628, art.2°, letra n).

[14] Atendida su importancia, la Organización para la Cooperación y Desarrollo Económicos (OCDE) exige: 1) que el propósito se especifique a más tardar en el momento en que se produce la recogida de datos; 2) que el uso de los datos se limite a cumplir los objetivos u otros que no sean incompatibles con el propósito original; 3) que no se introduzcan arbitrariamente nuevos propósitos al tratamiento y la libertad para realizar cambios implique necesariamente compatibilidad con el fin original; 4) que se indique en cada momento el cambio de objetivo, pudiendo ser utilizadas diversas vías alternativas o complementarias, como las declaraciones públicas, la notificación al titular o a través de disposiciones legales o reglamentarias, por ejemplo; y 5) que se eliminen los datos o se comuniquen en forma anónima cuando dejan de servir a la finalidad. ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICOS, OCDE*, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* Francia, OCDE Publications, 2002, pp.41-42.

[15] En la legislación argentina, en cambio, se define al responsable como *"la persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos"*. Según Oscar Puccinelli, eso lleva a un conflicto interpretativo porque no se sabe si la expresión titular está en un sentido de propietario o de persona formalmente a cargo. En su opinión, la ley argentina debió definir con mayor exactitud, porque titular es un término de significación no decisiva en orden a las operaciones a las que pueden ser sometidos los datos y hace posible la utilización de las formas para soslayar las responsabilidades establecidas en la ley. PUCCINELLI, Oscar, *Protección de datos de carácter personal,* Buenos Aires, Editorial Astrea, 2004, p.176.

personales que se contemplen en un servicio de la Nube tendrían carácter *intuito personae*, toda vez que existe un acto de confianza de parte del cliente (mandante) respecto del proveedor (mandatario), en la gestión de esas operaciones.

Asimismo, el mandatario –al igual que el responsable del registro– responderá hasta la culpa leve en su obligación de cuidar los datos personales, es decir, deberá indemnizar los daños que ocasione por la falta de la debida diligencia y cuidado que se emplea ordinariamente en los negocios propios.

Sin embargo, a nuestro juicio el principal aporte de este artículo 8° sobre el tratamiento a través de un mandatario se recoge en el inciso segundo, cuando le da un carácter de mandato especial con facultades específicas, al establecer, primero, que *"El mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos"* y luego, al indicar en el inciso final que el mandatario "*deberá respetar esas estipulaciones en el cumplimiento de su encargo"*, evitando así que se interprete que las obligaciones de protección de datos no le incumben por el hecho de que el tratamiento se realiza por cuenta y riesgo del mandante.

En consecuencia, el contrato de servicios en la Nube debe mencionar expresamente el encargo de tratamiento de datos personales si lo hubiere, no siendo suficiente una cláusula genérica de mandato. Por el contrario, es recomendable la redacción de un módulo específico en el contrato, referido al tratamiento de datos personales que incluya, a lo menos, la finalidad precisa del registro, la duración y vigencia del tratamiento, la posibilidad o no de comunicación a terceros y las obligaciones de confidencialidad y cuidado de la información.

Esta exigencia legal también puede ser vista como una restricción legítima a la libertad de contratación, ya que el cliente, en cuanto responsable del registro y sujeto obligado a cuidar los datos personales, no podría suscribir un contrato de servicio *cloud computing* del tipo contrato de adhesión si éste no estipula las condiciones específicas de tratamiento bajo las cuales aquél está autorizado. En ese sentido, estimamos que el cliente no podría limitarse a adherir contratos con cláusulas tipo elaboradas por el proveedor de servicios en la Nube, porque difícilmente abordarían el tratamiento por mandato en la forma exigida por la Ley N°19.628 y, con ello, la externalización significaría una infracción legal del cliente responsable del banco de datos que lo expone a indemnizar los perjuicios que cause al titular.

Por último, desde el punto de vista de la seguridad de la información en un contrato *cloud computing* destaca la figura del titular[16] de los datos contenidos en el registro que el cliente entrega al proveedor. Si bien ese titular no es parte del contrato, cobra especial relevancia porque el cliente y el proveedor deberán garantizar pleno respeto a los derechos

[16] El legislador chileno considera únicamente a personas naturales, nacionales o extranjeras, registradas en la base de datos, como titulares. En nuestra opinión es un término más correcto que hablar de "afectado" –como ocurre en la legislación española–, en donde evoca un sentido de lesión permanente y a priori. Sin embargo, no es menos cierto que hablar de titular podría presentar una connotación de pertenencia o propiedad sobre la información, como referido al "dueño de los datos", pero no compartimos esa concepción privatista-propietaria de derechos.

fundamentales de ese tercero, así como a las facultades que le reconoce la Ley N°19.628.

Sobre esto último, esos derechos subjetivos permiten al titular mantener un cierto control sobre los datos y se resumen en: derecho de acceso (para exigir información sobre los datos relativos a su persona); derecho de rectificación o modificación (para que se cambien los datos erróneos, inexactos, equívocos o incompletos); derecho de cancelación o eliminación (para que se destruyan efectivamente los datos cuando su almacenamiento carezca de fundamento legal o estuvieren caducos por haber perdido actualidad); derecho de oposición (para que cese un tratamiento); derecho de bloqueo (para suspender temporalmente cualquier operación sobre los datos almacenados); y derecho a indemnización (para demandar reparación de daños patrimoniales y morales sufridos a consecuencia de un tratamiento indebido de datos personales).

Estos derechos son independientes entre sí y suelen ser personalísimos, pese a que la Ley N°19.628 no es muy clara para calificarlos de ese modo. Eso significa que sólo podrán ser ejercidos personalmente por el titular de los datos, a quien se le debe exigir que compruebe fehacientemente su identidad.

En otro orden de ideas, es importante establecer quiénes de estos actores realizarán un tratamiento de datos regido por esta legislación. Para comenzar hay que analizar la entrega de la base de datos que hace el cliente al proveedor, para determinar si dicha operación puede ser considerada o no como una comunicación o transmisión de datos personales[17]. Si lo fuera, el traspaso que pretenda realizar el cliente hacia el proveedor de servicios en la Nube requeriría una habilitación previa, ya sea que la obtenga por escrito de cada titular de los datos contenidos en el registro o bien porque el legislador considera que esa base de datos es una fuente accesible al público que admite la comunicación sin necesidad de consentimiento.

Evidentemente, si esta garantía fuera exigible en los contratos de servicios *cloud computing,* el modelo sería poco viable por la dificultad que implica recolectar las autorizaciones, más aún si los registros que se externalizan suelen no ser fuentes accesibles al público[18]. Además, supondría que a través del contrato *cloud computing* se estarían proporcionando los datos al proveedor para que los utilice por cuenta propia, bajo el rol y con las obligaciones de un responsable del registro.

Sin embargo, en el modelo de servicios en la Nube las bases de datos personales que se traspasen al proveedor se entregan para que éste actúe sobre ellos por cuenta del cliente, sin tomar decisiones propias diferentes a las prestaciones contratadas. Por lo tanto, como hemos dicho, sólo cabe concluir que el cliente no realiza una comunicación o transmisión de datos propiamente tal hacia el proveedor, sino más bien le encarga un tratamiento por cuenta y riesgo de aquél, efectuado a través de un mandato.

No obstante, en el tratamiento por mandato el mandatario debe asumir por vía

[17] Ley N°19.628, artículo 2, letra c) define a la comunicación de datos personales como "*dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas*".

[18] Ley N° 19.628, artículo 2, letra i): *"Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes".*

contractual las mismas obligaciones que por ley se exigen al mandante, en su calidad de responsable del registro. Por ese motivo la Ley N° 19.628 establece que el mandato conste por escrito y deje especial constancia de las condiciones de la utilización de los datos.

En definitiva, la principal diferencia entre realizar un tratamiento de datos personales tras haberlos recibido a partir de una comunicación y el que se realice en ejecución de un contrato de mandato se encuentra en la necesidad o no de habilitación previa, sea del titular o de la ley. Por ese motivo, en un contrato *cloud computing* el cliente no requerirá una nueva autorización del titular de datos para encargar el tratamiento al proveedor.

V. CONSIDERACIONES LEGALES SOBRE SEGURIDAD DE LOS DATOS PERSONALES EN LA NUBE

Como hemos visto, el cliente de un servicio de la Nube debe ajustarse en la forma y fondo a lo dispuesto en la Ley N° 19.628 cuando externaliza el tratamiento de datos personales, entre otros aspectos, explicitando el alcance del mandato y cuidando la información con debida diligencia, haciéndose responsable de los daños tanto él como el mandatario.

Esa obligación de cuidado de los datos implica la implementación de medidas de seguridad efectivas, aunque el legislador no señala cuáles. Por esa razón, a falta de reglas específicas, el cliente y el proveedor *cloud computing* necesitan determinar las medidas técnicas, organizativas y normativas a establecer.

Uno de los criterios que pueden considerar se refiere a los riesgos a que se exponen los datos en la Nube. En ese sentido, como el cliente entrega la base al proveedor para que realice el tratamiento de los datos, resulta lógico que las medidas se dirijan a garantizar la confidencialidad y la integridad de los datos, previniendo situaciones de fuga de información y alteraciones no autorizadas. Además, como el acceso a los datos que solicite el cliente en virtud del contrato con el proveedor se realizará mediante una transmisión por Internet, hay que proteger la operación frente a posibles interceptaciones no autorizadas.

Otro criterio para determinar las medidas de seguridad idóneas que permitan cumplir la obligación legal de cuidado se basa en el tipo de dato personal. El legislador establece distintas intensidades en la protección de los datos a través de categorías. Así, junto con el régimen general de resguardo y comunicación de datos personales, simultáneamente admite casos de excepción con garantías más robustas para los datos sensibles[19], y más morigeradas para el acceso y utilización de ciertos datos personales

[19] Ley N°19.628, art.2, letra g): *"aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual"*..

contenidos en fuentes accesibles al público, es decir, en registros de acceso no restringido o reservado a los solicitantes.

Evidentemente las medidas de seguridad del registro se deben implementar a partir de la regla general de los datos personales y con el objeto de resguardarlos de los riesgos a que se exponen. Sin embargo, si el legislador dispone una protección reforzada para los datos sensibles, basada en la prohibición para su tratamiento, salvo autorización legal específica o consentimiento escrito del titular, será necesario que ciertas medidas de seguridad también sean más rigurosas para garantizar esos datos. Por ejemplo, parece imprescindible disponer de algún sistema de cifrado de los datos sensibles, tanto para su almacenamiento como para su transmisión, incluso si el destinatario es el cliente o el propio titular, ya que mitiga el riesgo de conocimiento no autorizado en caso de una interceptación.

Sin embargo, clasificar un dato personal como sensible no resulta del todo fácil. A diferencia del derecho extranjero que construye listados cerrados y objetivos, *numerus clausus* apropiados para una categoría de excepción como ésta, el legislador chileno lo deja abierto con la desafortunada expresión "tales como". Así, sobre la base de sus desaciertos en la regulación, estimamos que la Ley N° 19.628 ha establecido un régimen subjetivo para calificarlos, de manera que en Chile podría admitirse que el carácter sensible o no de un dato depende, en gran medida, de lo que estime como tal el propio titular o un juez.

Esa mirada subjetiva del sistema chileno genera diversos problemas entre los que se cuenta la contradicción con la garantía de categorizar los datos personales, el no respeto del carácter excepcional de los datos sensibles, la imposibilidad de interpretar restrictivamente sus normas y la dificultad para un reforzamiento *a priori,* ya que normalmente su calificación la realizará el titular luego de que un tercero utilice esos datos. En el caso que nos ocupa, ¿qué certeza tiene el responsable del registro y el mandatario sobre la naturaleza sensible de un dato, si no figura en los ejemplos mencionados por la definición legal? ¿Pueden ser responsables de culpa leve si, de buena fe, no extienden las medidas de seguridad para datos sensibles a esos casos? ¿Cómo se puede reparar el perjuicio causado por la utilización de un dato que legítimamente el responsable del registro estimó que no era sensible, pero después un juez señaló lo contrario? Creemos que estas interrogantes demuestran que el mayor perjudicado con el régimen subjetivo de datos sensibles es, en último término, el propio titular.

En otro orden de ideas, el contrato del servicio en la Nube constituirá un documento fundamental para la seguridad de los datos personales, toda vez que el legislador obliga a especificar las condiciones para el tratamiento por mandato y, en consecuencia, exige estipular cláusulas de seguridad para cuidar los datos. Veamos algunas de ellas.

En primer lugar, el contrato *cloud computing* que contenga el mandato para tratar los datos personales proporcionados por el cliente debe exigir equivalencia entre la seguridad ofrecida por el proveedor y la que tiene implementada el cliente. Sólo si el nivel de seguridad, tanto técnica como organizativa, es igual o superior a la del cliente,

éste podrá externalizar el tratamiento sin infringir su obligación de cuidado. En caso contrario, expondría los datos a una situación más precaria que no es razonable esperar respecto de sus propios datos, es decir, actuaría de manera negligente.

Además, se debe incluir alguna cláusula de confidencialidad que considere no sólo una disposición general frente a terceros, sino más bien que recoja lo dispuesto en la Ley N°19.628, en orden a que todas las personas que trabajan en el tratamiento de datos personales están obligadas a guardar secreto sobre los mismos, cuando provengan de fuentes no accesibles al público. Esta obligación busca impedir que los datos sean conocidos ilícitamente, a través de revelaciones, infidencias o fugas de datos. Por ese motivo, se aplica no sólo al responsable del registro o al mandatario, sino a todos los que trabajen con esa información y no cesa por haber terminado el contrato o sus actividades en ese campo. Es decir, quien interviene en cualquier fase del tratamiento y deja de interactuar con la base de datos o, incluso, de prestar servicios al proveedor, debe guardar secreto de la información personal que conoció, indefinidamente.

De no hacerlo, la vulneración se sanciona indemnizando los perjuicios causados al titular del dato, en la medida que éste los acredite, e incluso hasta podría configurarse un delito de revelación o difusión maliciosa de datos, que se castiga con presidio en su grado medio, pudiendo aumentarse en un grado si lo comete el responsable del registro o el mandatario[20].

Por otra parte, como los derechos subjetivos del titular de los datos son, a su vez, obligaciones legales que deben ser cumplidas de oficio por el responsable del registro y, consecuentemente, por el mandatario, el contrato debe estipular expresamente el deber de velar por la calidad de los datos, rectificándolos o actualizándolos cuando se advierta que son erróneos y, por supuesto, eliminándolos tan pronto hayan perdido vigencia, caduquen o cuando termine el contrato.

Del mismo modo, hay que estipular la obligación de avisar a los terceros a quienes les ha transmitido los datos, el hecho de la eliminación o modificación que experimenten aquellos que están en su registro. En ese caso, el responsable del banco de datos y el mandatario deberán avisarles a la brevedad sobre la operación efectuada y, si no fuese posible determinar las personas a quienes se les hayan comunicado, pondrán un aviso que pueda ser de conocimiento general para quienes usen la información del banco de datos.

Además, cabe recordar que la Ley N°19.628 prohíbe que estos derechos subjetivos del titular puedan ser limitados por medio de algún acto o convención, de manera que el proveedor del servicio *cloud computing* no podría dificultar el acceso a los datos a sus titulares alegando que el tratamiento que efectúa restringe contractualmente la entrega sólo al cliente. Éste tampoco podría impedir el ejercicio de cualquiera de los derechos del titular porque la base de datos se encuentre externalizada. En ese caso

[20] Ley N° 19.223, que Tipifica Figuras Penales relativas a la Informática, artículo 4°: *"El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado"*..

estimamos que es deber del cliente, en su calidad de responsable del registro, adoptar todas las medidas necesarias para facilitar el adecuado ejercicio de los derechos del titular de datos.

Como el tratamiento de datos personales es una actividad legítima, necesaria e, incluso, podría ser beneficiosa para el propio titular, su externalización a través de *cloud computing* requiere un resguardo contractual que garantice su continuidad. En efecto, la disponibilidad de la información de dicha base de datos no puede verse resentida por el hecho de su entrega a un mandatario. Por lo tanto, es necesario exigir que éste adopte planes de contingencia que permitan al responsable del registro continuar su gestión o sus servicios, incluso frente a fuerza mayor o caso fortuito que experimente el mandatario.

Finalmente, como el proveedor asume un mandato y se obliga a cumplir el encargo, se justifica incorporar una cláusula de auditabilidad de parte del cliente hacia el proveedor. Ello porque, como todo mandatario, el proveedor debe rendir cuentas de la gestión del negocio encomendado, por lo que la posibilidad de visitas o de auditorías a cargo del cliente resultan medidas contractuales razonables para cuidar los datos personales.

VI. PALABRAS FINALES

El modelo *cloud computing* constituye una interesante tendencia en materia de gestión tecnológica, en la que no se debe desatender la seguridad que demandan las bases de datos personales que se utilicen. Preocupan en especial los riesgos de manipulaciones no autorizadas, la infracción a las obligaciones de confidencialidad y secreto, las contingencias que afecten la disponibilidad de la información y las posibles interceptaciones indebidas de los datos cuando circulen entre las partes de un contrato de servicios en la Nube.

La legislación sobre protección de datos personales se aplica a la relación contractual que surge entre el cliente y el proveedor *cloud computing* a través de la figura del tratamiento por mandato, de manera que el mandatario asume por ley todas y cada una de las obligaciones impuestas al responsable del registro, debiendo indicarlas expresamente en el contrato.

Sin perjuicio de lo anterior, esta figura contractual para garantizar los derechos del titular de los datos personales no queda satisfecha únicamente con su reconocimiento en el marco regulatorio. Dado el alto componente tecnológico contenido en un tratamiento de datos en la Nube, nos permite proyectar, a modo de conclusión de este trabajo, que la seguridad de los datos en los servicios *cloud computing* se desarrolla de mejor manera bajo un modelo de privacidad por diseño (*privacy by design*)[21], a la luz de

[21] CAVOUKIAN, Ann, *Privacy by Design, Los 7 Principios Fundamentales,* Canadá, 2011. Disponible en:

los principios fundamentales que lo inspiran:

i) En el *cloud computing* es necesario anticiparse y prevenir contingencias que afecten los derechos del titular de datos, antes de que ocurran. Las medidas de privacidad por diseño son proactivas, no esperan que los riesgos se materialicen.

ii) Los servicios en la Nube requieren considerar que el respeto por la privacidad esté predeterminado, es decir, se protejan automáticamente en los sistemas de información y en las prácticas de negocio, incluso si el titular nada dice. No olvidemos que en este caso, la externalización no requiere del consentimiento del titular, por lo que cobran aún más relevancia las acciones predeterminadas de garantía.

iii) Los sistemas tecnológicos y las prácticas de negocio en la Nube deben incorporar la seguridad de los datos personales como parte de su diseño y arquitectura.

iv) La protección de datos en un servicio de la Nube no puede ser vista como una barrera para la legítima actividad de tratamiento que realice el cliente que externaliza los datos en el proveedor. Se requiere reconocer un equilibrio entre los intereses involucrados.

v) Las medidas de seguridad deben considerar el ciclo completo del tratamiento de datos personales, es decir, no sólo la etapa de entrega de la base de datos desde el cliente al proveedor, sino en cada operación que se realice sobre ellos y, por supuesto, luego de que pierdan vigencia o caduquen, para efectos de realizar una devolución de la base o una destrucción de los datos, en forma segura.

vi) Sólo puede suscribirse un contrato *cloud computing* que sea transparente sobre la forma en que se desarrollará el tratamiento de datos, tanto porque el legislador exige explicitar en el mandato las condiciones específicas de éste, como también porque debe ser posible para el titular ejercer sus derechos y para el cliente exigir rendición de cuentas a su mandatario.

vii) Por último, el centro de la seguridad no son los datos, sino las personas a quienes concierne la información, por eso deben implementarse medidas idóneas para lograr controles robustos para los datos sensibles y facilidad de información a los titulares.

[Recibido el 5 de diciembre y aceptado el 20 de diciembre de 2011]

http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf [Consulta: 30 de noviembre 2011].

BIBLIOGRAFÍA

BERTELSEN REPETTO, Raúl, "Datos personales: propiedad privada, libre iniciativa particular y respeto a la vida privada", en *Cuadernos de Extensión Jurídica,* 5, (2001).

CAVOUKIAN, Ann, *Privacy by Design, Los 7 Principios Fundamentales,* Canadá, 2011. Disponible en: http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf [Consulta: 30 de noviembre 2011].

CLOUD HYPERMARKET, *The cloud revolution,* 2011. Disponible en: http://www.cloudhypermarket.com/whatiscloud/CloudUptake. [Consulta: 30 noviembre 2011].

CONVENIO N°108, del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.

DIRECTIVA 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

GRUPO DE TRABAJO DEL ARTÍCULO 29, DE LA UNIÓN EUROPEA, *Dictamen 4/2007 sobre el concepto de datos personales*, adoptado el 20 de junio de 2007, [en línea]. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf, [Consulta: 7 abril 2011].

ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICOS, *OCDE Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* Francia, OCDE Publications, 2002.

PUCCINELLI, Oscar, *Protección de datos de carácter personal*, Buenos Aires, Editorial Astrea, 2004.