FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES

Trabajo de Integración Final de ABOGACIA

Cloud computing en Argentina: Normativa vigente y necesidad de adecuación de la misma para la protección de los datos personales en la nube

Zanazzi Julieta LU: 1025894

Carrera: Abogacía

Tutor: Galmarini Luciano **Firma tutor:**

Fecha de presentación: 15/09/2014

Turno de cursada de Seminario de Practica Corporativa: Noche

Índice:

Abstract

El “cloud computing” es un sistema informático que ofrece la migración o la externalización de los equipos de computación y de los programas o las funciones de procesamiento de datos a un prestatario de servicios que otorga su almacenamiento a través de los servidores diseminadas sin identificación necesaria de su ubicación, por un precio determinado o determinable. Este modelo presenta innumerables ventajas técnicas y económicas para las empresas. Sin embargo, se necesita analizar que normativa legal se aplica al mismo para proteger los datos que migraran a la nube.

La protección de datos es un derecho a la intimidad personal que tienen las personas contra un tratamiento incorrecto, no autorizado o contrario a las normativas vigentes de sus datos personales por tratadores de datos. Al proteger los datos personales frente al riesgo de la recopilación y el mal uso de los mismos se ampara por ende, la privacidad de las personas

Este trabajo propone recorrer la normativa Argentina que se puede aplicar a la protección de los datos en esta plataforma. A su vez, se identificarán los riesgos que conlleva la utilización de este nuevo sistema informático, se brindarán posibles soluciones y se detallarán cuestiones a tener en cuenta a la hora de contratar un prestador de servicios en la nube.

Introducción

Hoy en día gran cantidad de empresas se ven atraídas por las ventajas técnicas y los bajos costos que ofrece el sistema de cloud computing. Sin embargo, a pesar de los beneficios que trae aparejado este sistema, cuestiones relativas a la seguridad y protección de los datos almacenados en la nube muchas veces no se contemplan. La información es el activo más importante de las organizaciones. Por ende, es necesario proteger legal y técnicamente los datos personales que se alojen en el cloud.

Al aumentar año tras año la demanda de los consumidores de servicios en la nube, es necesario investigar este fenómeno y como se protege la privacidad de las personas en el mismo.

Como hipótesis de este trabajo se busca demostrar que la normativa legal vigente en nuestro país es insuficiente para una protección adecuada de los datos personales que se alojan en la nube de internet. Para ello, uno de los objetivos del presente es el análisis de la legislación Argentina para la protección de los datos personales y cómo se puede interpretar la misma para lograr su adecuación al sistema de cloud computing. Exponer las ventajas y los riesgos que trae aparejado alojar los datos en el cloud y proponer posibles soluciones para aquellas cuestiones sin amparo legislativo, complementa el propósito del trabajo de investigación realizado.

En virtud de lo expuesto, la instancia metodología comprende en primer lugar una descripción del Cloud computing, de sus niveles de servicio y formas de despliegue. Es relevante entender como funciona este servicio para lograr comprender dónde se alojaran los datos que se deben proteger.

En una segunda etapa, se mencionaran las ventajas que ofrece *el cloud* y se abordaran los riesgos que conlleva migrar los datos personales a la nube.

En tercer lugar, se presentará la normativa vigente en la Argentina sobre la protección de datos personales, y se analizará cuales regulaciones son compatibles con el sistema del cloud computing y que cuestiones quedan sin regular o es insuficiente la regulación. Se trabajará especialmente con el concepto de la cesión de los datos, el consentimiento del titular y la

seguridad de los mismos. A su vez, se propondrá un sistema de información en capas como posible solución para obtener el consentimiento conforme lo prevé la ley.

Por último se expondrán las conclusiones obtenidas del trabajo y se trazarán las futuras líneas de investigación relacionadas con el tema

La nube de internet

En la actualidad gran cantidad de usuarios particulares y empresas son persuadidos por las ventajas técnicas y económicas que les ofrece el servicio de *cloud computing*. "Este servicio permite a empresas de todos los tamaños ahorrar tiempo y recursos en almacenamiento, servidores, productos, instalaciones, TCO (Costo total de propiedad de licencias) y actualizaciones en las diferentes soluciones (ERP, CRM, BPM, etc) utilizadas para eficientizar la gestión de un negocio"[1]

"Según el estudio *Cloud Computing – Consumer Markets: Strategies and Forecasts 2014-2018* de *Juniper Research*, la demanda de servicios en la nube por parte de los consumidores aumentará de forma muy significativa durante los próximos cinco años, y se estima que alcanzará los 3.600 millones de usuarios en 2018". [2]

Pero, ¿de qué se trata este servicio en la "nube"?. "Se podría definir *"cloud computing"* como el sistema informático que ofrece la migración o la externalización de los equipos de computación y de los programas o las funciones de procesamiento de datos a un prestatario de servicios que otorga su almacenamiento a través de los servidores diseminadas sin identificación necesaria de su ubicación, por un precio determinado o determinable" [3] En términos más sencillos, "estamos frente a un sinnúmero de servidores interconectados que ofrecen, a través de

[1] Fernández Pasos, Gonzalo. *"Integración de sistemas y cloud computing"* (online) Mercado. 7/11/ 2012. http://www.mercado.com.ar/notas/google-organic/374070/noticias-desde-google?id=374070 Consulta: 4 septiembre 2014.
[2] Martínez, Anna. *"Los servicios cloud contaran con 3.600 millones de usuarios en 2018"* (online). VozTele.com News. 3/9/2014. http://blog.voztele.com/2014/09/03/los-servicios-cloud-contaran-con-3-600-millones-de-usuarios-en-2018 Consulta: 8 septiembre 2014.
[3] Granero, Horacio R. *"Problemas legales de la Cloud Computing".* El Dial. 12/10/2010. [elDial.com-DC14B2] Consulta: 30 agosto 2014.

Internet, la posibilidad de guardar infinita cantidad de información y ejecutar todo tipo de tareas"[4].

Niveles de servicio

Dentro del *Cloud Computing* se pueden distinguir tres niveles diferentes de servicio que puede prestar el proveedor del *cloud: Infraestructure as a Service* (IaaS), *Platform as a service* (PaaS) y *Software as a Service* (SaaS)

El IaaS: "provee acceso a grupos de recursos hardware virtualizados, incluyendo máquinas, almacenamiento y redes. Con IaaS los clientes renuncian a usar sus propios equipos físicos, sino que usan los recursos virtuales que le proporciona el Proveedor de Servicios Cloud y sobre dichas infraestructuras el cliente es responsable de la instalación, mantenimiento, y ejecución de su propia pila *(stack)* de aplicaciones."[5] Prestan este servicio Amazon Web Service, GoGrid, Rackspace Cloud, entre otros.

El PaaS: "está destinado a clientes con conocimientos en desarrollos de software y aplicaciones, permitiéndoles realizar su actividad en el entorno que le ofrece el Proveedor. Ejemplo: Google App Engine, Microsoft Azzure Service, etc." [6]

El SaaS: "provee acceso a una colección de programas de aplicación. Los proveedores SaaS ofrecen a los usuarios acceso a un conjunto de aplicaciones específicas que son ejecutadas en las infraestructuras del proveedor y controladas por él. […] Es decir, el cliente no tiene acceso ni control a la Plataforma subyacente ni siquiera, en general, de las capacidades y funcionalidades de la aplicación con la única posible excepción de poder modificar aquellos parámetros de

[4] Bianchi, Adriano. *"La nube, el servicio que revoluciona Internet"*. Ámbito.com. 1/3/2010. http://www.ambito.com/noticia.asp?id=510324 Consulta: 6 septiembre 2014.

[5] *"Cloud Computing: taxonomía por niveles (o modelos) de servicios (IaaS, PaaSy SaaS)"* (online) RealCloudProject.com. 21/2/2012. http://www.realcloudproject.com/cloud-comuting-taxonomia-por-niveles-o-modelos-de-servicio-iaas-paas-y-saas. Consulta:8 septiembre 2014

[6] Toscano Silvia y Galmarini Luciano*, "Protección de datos personales en la `nube'"*, La Ley, Suplemento Actualidad, 04/10/2012, Año LXXVI Nº 187 / ISSN 0024-1636, La Ley 2012-E"

configuración de la aplicación destinados de forma específica para el usuario y su personalización"[7]

Independientemente del modelo de servicio utilizado (SaaS, PaaS, IaaS) existen tres formas de despliegue de los servicios de cloud computing[8]:

Nube Privada: La característica principal de este modelo es que el usuario no comparte infraestructura física con ningún otro cliente, agrupando los servicios y la infraestructura en una red privada. Se basa en la reserva de recursos hardware y software en exclusiva para un usuario.

Nube Pública: los clientes contratan los recursos que necesiten para sus proyectos, siendo el proveedor del servicio el responsable del mantenimiento y de la gestión de la infraestructura, lo que reduce significativamente los costos iniciales de desarrollo de estructura y acceso inmediato a sus servicios en contratación.

Nube Hibrida: El cliente gestiona exclusivamente su infraestructura, pero dispone de acceso a los recursos de la nube pública pudiendo ampliar sus recursos en cualquier momento, obteniéndolos de esta última.

Las clasificaciones expuestas son en general las más utilizadas por la doctrina especializada, sin embargo las modalidades en la nube son tantas como variantes puedan existir.

Riesgos en la nube

Las empresas son conscientes que utilizar el servicio de cloud computing mejora la eficiencia y la productividad gracias a la reducción de costos, a la movilidad y a la flexibilidad que se obtiene. El cloud les permite focalizar sus recursos humanos y técnicos en su actividad principal y delegar la gestión de las comunicaciones y/o informática, en una empresa externa que ofrece los servicios en la nube. Además tienen la posibilidad de crecer sin aumentar los costos

[7] *"Cloud Computing: taxonomía por niveles"*, Op.Cit., p.6.

[8] Gonzalez Allonca, J.C., Piccirilli, D., *Consideraciones Legales Relativas a la Privacidad en Proyectos de Cloud Computing en el Exterior de Argentina*. Revista Latinoamericana de Ingeniería de Software (online). Febrero 2014, vol. 2, n.1, p. 77-90. Consulta: 11 septiembre 2014. http://www.unla.edu.ar/sistemas/redisla/ReLAIS/relais-v2-n1-revista.pdf ISSN 2314-2642

operativos, optimizar procedimientos y acceder desde cualquier lugar a los recursos informáticos de la empresa.

A pesar de las ventajas mencionadas es una realidad que la seguridad siempre se encuentra un paso por detrás cuando nuevas tecnologías emergen. Y esta es una de las principales barreras que encuentran las empresas para implementar nuevas tecnologías.

Marcelo Pizani, Gerente de Productos de la empresa de antivirus Panda, asegura que "los principales obstáculos que encontramos a la hora de hablar de seguridad en la nube son el desconocimiento, la desinformación y el temor. En las empresas, esto sucede particularmente por los aspectos de confidencialidad". Si bien las compañías aceptan que su información está circulando constantemente en la Web, según Pizani para ellos "no es lo mismo que circule en el aire o en el medio, que volcar la confianza de sus datos a un proveedor que trabaje en la nube".[9]

El avance de Internet sobre nuestras vidas ha ido modificando nuestros hábitos, los modos de relacionarnos, y además es un medio rápido y eficaz para recolectar datos personales.

"Tanta facilidad de acceso a la red puede generar ciertos peligros respecto a la confidencialidad de los datos obrantes en la nube, ya sea por los niveles de acceso a dicha información, o de las políticas de seguridad físicas como lógicas con que cuente el prestador del servicio, lo que puede poner en riesgo la privacidad del usuario, que no quedará a cubierto con una clave, *password o passphrase*".[10]

"El temor a cloud es de alguna manera justificado ya que no existen herramientas unificadas de seguridad ni políticas consistentes que se encarguen de la administración de elementos tales como: seguridad, cumplimiento de normas, gobernabilidad y riesgos legales de los servicios cloud."[11]

La protección de los datos personales es una de las mayores preocupaciones, ya que, los datos no se almacenan en la computadora personal del usuario, sino que están alojados en la nube y

[9] Bianchi, Adriano Op. Cit p.6
[10] Toscano, Silvia. Op.Cit., p.6
[11] Lía, Mario. "*Cloud Computing se consolida*". (Online). Mercado. 26/3/ 2014. N. 1153. Consulta: 11 septiembre 2014 http://www.mercado.com.ar/notas/tecnologa-%7C/8015115/%3Cb%3Ecloud-computing%3Cb%3E-se-consolida-

se puede llegar a ellos remotamente a través de internet desde cualquier dispositivo con conexión a la red. Para el usuario de la nube (en su función de controlador de datos) es difícil, comprobar de manera eficaz el procesamiento de datos que lleva a cabo el proveedor y en consecuencia, tener la certeza de que los datos se gestionan de conformidad con la ley.

Marco legal aplicable

La ley 25.326 de protección de datos personales tiene como objetivo la protección integral de los datos, garantizando el honor, la identidad y la intimidad de las personas, y a su vez el acceso a la información que sobre las mimas se registre. Esta ley regula la actividad de las bases de datos que registran información de carácter personal y garantiza al titular de los datos la posibilidad de controlar el uso de sus datos personales

Según el artículo 2 de la ley se entiende por **datos personales**: información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

"La protección de datos es un derecho a la intimidad personal que tienen las personas contra un tratamiento incorrecto, no autorizado o contrario a las normativas vigentes de sus datos personales por tratadores de datos. Al proteger los datos personales frente al riesgo de la recopilación y el mal uso de los mismos se ampara por ende, la privacidad de las personas"[12].

La ley fue sancionada en octubre del 2000 y el decreto 1558/2001 que la reglamenta es del año posterior, en esa época el concepto de *cloud computing* aun no existía en el mundo de la tecnología.

Sin embargo, para la legislación argentina la contratación de servicios de cómputo en la nube queda comprendido como una prestación de servicios informatizados y esto implica que el tercero hace un tratamiento de los datos personales y las obligaciones de ese tratamiento se encuentran previstas en el artículo 25 de la ley: *"Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación*"

[12] González Allonca, J,C. Op.Cit. p.7

En el segundo párrafo dispone que *"Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años*"

A su vez, el artículo 25 del Decreto 1558 del año 2001, formula que:

Los contratos de prestación de servicios de tratamiento de datos personales deberán contener los niveles de seguridad previstos en la Ley Nº 25.326, esta reglamentación y las normas complementarias que dicte la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, como así también las obligaciones que surgen para los locatarios en orden a la confidencialidad y reserva que deben mantener sobre la información obtenida.

La realización de tratamientos por encargo deberá estar regulada por un contrato que vincule al encargado del tratamiento con el responsable o usuario del tratamiento y que disponga, en particular:

a) que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

b) que las obligaciones del artículo 9º de la Ley Nº 25.326 incumben también al encargado del tratamiento.

En relación a lo expuesto por los dos artículos precedentes se debe tener en cuenta que es lícito que un banco de datos contrate a un tercero para que realice el tratamiento de los datos que el mismo recolectó, pero el prestador de servicio debe cumplir con determinados requisitos:

a) Contar con un contrato de prestación de servicios de tratamiento de datos personales, en el que se determine la relación entre las partes
b) No aplicar, ni utilizar los datos con un fin distinto al que figure en el contrato.
c) La imposibilidad de ceder los datos a otras personas, ni aun para su conservación
d) Contar con un contrato de prestación de servicios de tratamiento de datos personales, en el que se determine la relación entre las partes
e) Fijar en el mismo contrato que la empresa prestadora de servicios informatizados se compromete a:
   - Cumplir con los niveles de seguridad previstos en la ley

- Con la reglamentación y las normas complementarias que dicte la Dirección Nacional de Protección de Datos Personales (DNPDP),
- Cumplir con las obligaciones que surgen en orden a la confidencialidad y reserva que deben mantener sobre la información obtenida.

Del segundo párrafo del artículo 25 del decreto 1558/2011 se pueden distinguir las partes intervinientes del servicio del cloud computing[13]:

- El responsable o usuario del tratamiento
- El ejecutor del tratamiento: el prestador de servicios en la nube
- El titular de los datos.

Con respecto al "ejecutor del tratamiento", es menester recordar que la ley 25.326 en su artículo 2 trae una serie de definiciones pero el prestador de servicios en la nube no aparece en él. Por eso es que se debe deducir y encuadrar dentro del ejecutor del tratamiento conforme a lo previsto en el párrafo segundo del artículo 25 del decreto reglamentario

Cesión

La cesión de datos implica la transferencia de la información. Sin embargo, ésta no constituye la delegación de la titularidad del dato, que siempre es de la persona a la que se refiere.

El artículo 11 de la ley de protección de datos personales enumera ciertos requisitos para que la cesión se constituya como válida y son los siguientes:

1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario **y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo**.

Es decir, que la cesión debe ser realizada para cumplir con los fines que justificó la recolección de los datos .Y para poder ceder los datos personales, objeto de tratamiento, se necesita el previo consentimiento del titular de los datos, el cual debe estar informado sobre la finalidad de

[13] Toscano, Silvia. Op.Cit. p.6

la cesión y debe poder identificar al cesionario o poseer los elementos que permitan individualizarlo.

Además se expresa en el mismo artículo que el consentimiento para la cesión es revocable y que no será exigido cuando:

a) Así lo disponga una ley;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;

d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;

e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.

2. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

Entonces, para poder ceder los datos se necesita el consentimiento del titular de los mismos. Conforme al artículo 5 de la ley 25.326, el consentimiento debe ser libre expreso e informado y deberá constar por escrito o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de:

a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;

b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;

c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;

d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;

e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Llevando la cuestión de la cesión de datos personales al contexto de la nube, podemos advertir que no es fácil controlar, como titular de los datos o como usuario del tratamiento, que el prestador de servicios en la nube cumpla con los requisitos previstos por la ley, su decreto reglamentario y las resoluciones de la DNPDP. Además toda la información que se prevé que debe poseer el titular de los datos en la mayoría de los casos no la posee. Y si nos encontramos dentro de un nivel de servicio de *cloud computing* donde el ejecutor del tratamiento pone las condiciones de seguridad y privacidad de manera previa y unilateral el titular de los datos tienen menos posibilidades de controlar, en el caso de una cesión, que se cumpla con la normativa correspondiente.

Otro punto a tener en cuenta es la forma en que el titular de los datos presta el consentimiento. Según la legislación aplicable el mismo tiene que ser libre, expreso e informado. En el ámbito del cloud en la Argentina, se considera que con solo “cliquear” aceptando los términos y condiciones de uso o las políticas de privacidad, según como lo llame cada proveedor, se está dando el consentimiento y el mismo es válido. Ya que, en nuestro país se utiliza el sistema de “opciones de exclusión” o *"opt-out"* que significa que el sitio web puede usar dicha información a no ser que el usuario específicamente indique lo contrario.

Sin embargo, la mayoría de las veces el usuario no se toma el tiempo de revisar que es lo que está aceptando o cuando lo hace pueden existir cuestiones técnicas-jurídicas que no logra comprender o no sabe de qué manera indicar que no está de acuerdo con las políticas que se presumen que el acepto. Esto nos lleva a pensar si el consentimiento, ¿realmente se presta de forma libre, expresa e informada? ¿Qué otro método se podría prever legislativamente?

Posibles soluciones

La primera solución y tal vez sea la más extremista para evitar la cesión de los datos personales consiste en especificar en el contrato de servicios la prohibición de realizar algún tipo de cesión. "Es decir, que la empresa contratada para el tratamiento informatizado de datos, no podrá realizar otra cesión de información a un tercero, ni siquiera para fines de almacenamiento."[14]

Otra opción que propongo es utilizar un **sistema de información por capas** basado en la guía sobre el uso de las cookies desarrollada por la agencia española de protección de datos.

Este sistema de información por capas consiste en mostrar la información esencial en una primera capa, cuando se accede a la página o aplicación, y completarla en una segunda capa mediante una página en la que se ofrezca información adicional.[15]

Si trasplantamos este sistema español utilizado para cookies y lo aplicamos al cloud computing **en la primera capa** se incluiría la siguiente información:

- Advertencia de que si se realiza una determinada acción, se entenderá que el usuario está prestando el consentimiento para la posible cesión de los datos
- Especificación de que información se recopila y para que se utiliza la misma
- Una breve descripción de que medidas de seguridad se adoptan para proteger tus datos

A su vez en esta primer capa además de advertirse sobre la cesión de los datos, se puede incluir información acerca de la jurisdicción a la cual se someten las partes en caso de un eventual conflicto, donde se almacenan los datos y cumpliendo con la disposición 4/2009 de la DNPDP se incluiría como información todo lo pertinente al derecho de retiro o bloqueo que posee el titular del dato.[16]

[14] Gonzalez Allonca , J.C Op. Cit. 7

[15] Agencia Española de Protección de Datos. *"Guía sobre el uso de las cookies"* (online) 2010. http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf

[16] Disposición 4/2009 DNPDP: *Artículo 1.-En las comunicaciones con fines de publicidad directa, el banco de datos emisor debe incorporar un aviso que informe al titular del dato sobre los derechos de retiro o bloqueo total o parcial, de su nombre de la base de datos, el mecanismo que se ha previsto para su ejercicio, con más la transcripción del artículo 27, inciso 3, de la Ley Nº 25.326 y el párrafo tercero del artículo 27 del Anexo I del Decreto Nº 1558/01.*

Todo lo mencionado se facilitará a través de un formato que sea visible para el usuario y que deberá mantenerse hasta que el realice la acción requerida para la obtención del consentimiento.

En la segunda capa se incluiría toda aquella información necesaria sobre el servicio de cloud computing de forma detallada y en un vocabulario apto para que las personas que no poseen los conocimientos técnicos puedan comprender.

En los casos en que el usuario no manifieste expresamente si acepta o no, pero continúe utilizando la página web o la aplicación se podría entender que éste ha dado su consentimiento, siempre que se le haya informado claramente en este sentido y se ofrezca en todo momento en algún lugar visible del sitio la información sobre el servicio que está utilizando y las formas de dar de baja el mismo sí correspondiese.

Ya que no existe normativa específica sobre los datos personales en la nube, la Dirección Nacional de Protección de Datos Personales podría emitir una disposición donde se especifiquen que información debe estar obligatoriamente en estas "capas" y así proteger de manera directa al titular de los datos personales ante el almacenamiento de los mismos en el cloud.

Seguridad

El artículo 9 de la ley de protección de datos personales expresa que**:**

1. *El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.*

2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

La autoridad de control de la ley, la DNPDP, ejerciendo su atribución de dictar normas y procedimientos técnico relativos al tratamiento y condiciones de seguridad de las bases de datos, creó dos disposiciones:

La primera es la **Disposición 11/2006** en la que se fijan *las medidas de seguridad para el tratamiento y conservación de los datos personales contenidos en archivos, registros, bancos y bases de datos públicos no estatales y privados.*

Se establecen tres niveles de seguridad: Básico, Medio y Critico, conforme la naturaleza de la información tratada. Para cada uno de los niveles se prevén distintas medidas de seguridad, establecidas teniendo en cuenta la mayor o menor necesidad de garantizar la confidencialidad e integridad de la información contenida en el banco de datos respectivo; la calidad de los datos y los riesgos a que están expuestos, así corno también el mayor o menor impacto que tendría en las personas el hecho de que la información registrada en los archivos no reúna las condiciones de integridad y confiabilidad debidas.

Niveles:[17]

- Medias de seguridad de nivel básico: le deben adoptar los archivos, registros, bases y bancos de datos que contengan datos de carácter

- Medidas de seguridad de nivel medio: además de las medidas básicas deberán adoptar las de este nivel os archivos, registros, bases y bancos de datos de las empresas privadas que desarrollen actividades de prestación de servicios públicos, así como los archivos, registros, bases y bancos de datos pertenecientes a entidades que cumplan una función pública y/o privada que, más allá de lo dispuesto por el artículo 10 de la Ley N° 25.326, deban guardar secreto de la información personal por expresa disposición legal (v.g.: secreto bancario)

- Medidas de seguridad de nivel crítico: Los archivos, registros, bases y bancos de datos que contengan datos personales, definidos como “datos sensibles además de las medidas de seguridad de nivel Básico y Medio, deberán adoptar las de nivel crítico.

[17] Disposición Nº 11/2006 DNPDP. "Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados". http://www.infoleg.gov.ar/infolegInternet/anexos/120000-124999/120120/norma.htm

La segunda disposición destacada que emitió la DNPDP es la **09/2008** donde se aprueba un modelo de documento de seguridad de datos personales.

Los archivos, registros, bases y bancos de datos personales deben disponer de un "Documento de Seguridad de Datos Personales", en el que se especifica la normativa de seguridad aplicable. Que a fin de facilitar la implementación del referido documento y la efectiva puesta en funcionamiento de medidas técnicas que garanticen la seguridad y la confidencialidad en el tratamiento de datos personales, se creó un modelo de documento de Seguridad que contenga lineamientos indispensables mínimos y cumpla con las normas dictadas en la materia.

Es menester destacar que estas regulaciones de seguridad implican estándar básico, lo que no obsta a que los organismos y empresas otorguen mayores medidas de seguridad a sus bases de datos.

A pesar de que la ley obliga al prestador el servicio a adoptar las medidas técnicas y organizativas necesarias para proteger los datos personales y las disposiciones sobre seguridad complementan lo peticionado por el artículo 9 de la ley, el usuario no debe confiarse de que esta normativa se cumple y trasladar los datos a la nube sin antes evaluar ciertos aspectos y ver si los mismos son cumplidos por el proveedor del servicio.

Se deberá tener en cuenta[18]:

- Administración de identidades y acceso *(identity and access management, IAM).*
- Prevención de pérdida de datos (*data loss prevention, DLP).*
- Seguridad Web (*Web security).*
- Seguridad de correo electrónico (e*mail security).*
- Auditoría de seguridad *(security assessments).*
- Administración de intrusos *(intrusion management).*
- Administración de eventos y seguridad de la información *(security information and event management, SIEM).*

[18] Cejudo Torres, José Juan, "*Servicios de seguridad en la nube*". (online) Magazcitum.16/6/2012. http://www.magazcitum.com.mx/?p=1784#_ednref1 Consulta: 7 septiembre 2014

- Cifrado (*encryption).*
- Continuidad del negocio y recuperación de desastres *(business continuity and disaster recovery).*
- Seguridad de la red (*network security).*

ISO/IEC 27001:

"A semejanza de otras normas ISO, ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña"[19]

Su objetivo es implantar una serie de procedimientos y controles para asegurar la gestión de la seguridad de la información.

La certificación de esta norma se logra a partir de un proceso por el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado. La guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información (ISO/IEC 27002) establece 11 dominios de control que cubren por completo la Gestión de la Seguridad de la Información.[20]

A la hora de elegir un prestador de *cloud computing* un dato a tener en cuenta es si este posee la certificación ISO/IEC 27001 y eso nos dará la pauta de que la información se gestiona de manera segura.

[19] ISO 27001 en Español (online) © 2012 http://www.iso27000.es/iso27000.html Consulta: 11 septiembre 2014

[20] Gonzalez Allonca, J.C., Piccirilli, D., *Consideraciones Legales Relativas a la Privacidad en Proyectos de Cloud Computing en el Exterior de Argentina*. Revista Latinoamericana de Ingeniería de Software [en línea]. Febrero 2014, vol. 2, n.1, p. 77-90. Consulta:11 septiembre 2014. http://www.unla.edu.ar/sistemas/redisla/ReLAIS/relais-v2-n1-revista.pdf ISSN 2314-2642

Conclusión

El avance de Internet sobre nuestras vidas ha ido modificando nuestros hábitos y los modos de relacionarnos. Lo cierto es que el usuario con solo conectarse a la red realizará todas sus tareas on-line sin necesidad de descargar nada en su computadora. Este nuevo paradigma de manejo de la información, sobre todo el hecho de trasladar nuestros datos a la nube, genera un desafío en el campo legal

La demanda de servicios en la nube por parte de los consumidores aumentará de forma muy significativa en los próximos años, ya que, como se ha expresado a lo largo del presente trabajo son indudables las numerosas ventajas técnicas y económicas que brinda este servicio. Apostar al "cloud computing" le permite a las empresas ahorrar dinero asignando los recursos de forma eficiente, enfocándose en su actividad principal delegando la gestión informática en el tercero proveedor del servicio.

Sin embargo, más allá de los beneficios a obtener, las empresas poseen dudas y un cierto resquemor a la hora de delegar en un tercero el almacenamiento, el control, la confidencialidad y seguridad de los datos.

Como se ha analizado, nuestra legislación no trae una figura que se aplique específicamente para el *"cloud computing"*, por ende se debe recurrir a los artículos 25, 9 y 11 entre otros, de la ley 25.326, las especificaciones de esos artículos que prevé el decreto reglamentario 1558/01 y a las disposiciones pertinentes de la Dirección Nacional de protección de datos personales para lograr un marco legal que permita proteger los datos alojados en la nube.

Más allá de las interpretaciones que podamos hacer de la normativa mencionada en el párrafo anterior para aplicarla a la nube, necesitamos una legislación específica para proteger los datos sometidos a un sistema de Cloud Computing.

Se necesitan por ejemplo, medidas de seguridad concretas para proteger los datos almacenado y nuevos métodos, como el propuesto de "información en capas", para que el titular de los datos preste fehacientemente el consentimiento ante una eventual cesión de los mismos. Y a su vez buscar la forma de garantizar que el usuario tenga la información necesaria para darle tranquilidad acerca de cómo están siendo tratados sus datos.

Por otro lado, ninguna disposición define las partes intervinientes en este sistema, como consecuencia se debe deducir del decreto reglamentario 1558/01 como se ha explicado oportunamente, por ende sería de gran ayuda para comprender mejor el vocabulario empleado en la normativa vigente, que en alguna disposición de la DNPDP se provean los conceptos pertinentes.

Sin perjuicio de lo manifestado, a la hora de contratar un prestador de servicios en la nube, el usuario deberá tener en cuenta: primero que tipo de servicio necesita (IaaS, SaaS o PaaS), que tipo de datos trasladará a la nube, cuáles son las medidas de seguridad que implementa el proveedor, si se rige como mínimo por la normativa vigente de nuestro país y si posee alguna certificación como la ISO/IEC 27001.

Como conclusión del presente trabajo se desprende que la normativa legal argentina sobre protección de datos personales no es suficiente para controlar y brindar una extensa protección a los datos alojados en la nube; corroborando asi la hipótesis propuesta al inicio de la investigación. Si bien, se pueden aplicar los artículos de la ley 25.326 es necesario que se dicten normas específicas para el cloud computing. De esa forma se otorgara mayor seguridad a las empresas para invertir en esta nueva tecnología y así aprovechar al máximo las ventajas que ofrece migrar los datos a la nube.

Como futuras líneas de investigación y a fin de complementar el presente trabajo de especialización se propone el estudio de la jurisdicción aplicable en la nube y la transferencia internacional de los datos a través de un prestador de servicios de cloud.

Bibliografía

I. Doctrina

- Agencia Española de Protección de Datos. *"Guía sobre el uso de las cookies"* (online) 2010.http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf

- Altmark, Daniel Ricardo, *Informática y derecho : aportes de doctrina internacional*, V.6 , Buenos Aires : Depalma, 1998 ISBN: 9789501404166

- Bianchi, Adriano. *"La nube, el servicio que revoluciona Internet"*. Ámbito.com. 1/3/2010. http://www.ambito.com/noticia.asp?id=510324

- Cavoukian, Anne. *"Privacy in the clouds A White Paper on Privacy and Digital Identity: implications for the Internet*" (online). Information and privacy commissioner,Ontariohttp://www.ipc.on.ca/images/resources/privacyintheclouds.pdf

- Cejudo Torres, José Juan, "Servicios de seguridad en la nube". 16/6/2012. http://www.magazcitum.com.mx/?p=1784#_ednref1

- "*Cloud Computing: taxonomía por niveles (o modelos) de servicios (IaaS, PaaSy SaaS)"*.RealCloudProject.com. 21/2/2012. http://www.realcloudproject.com/cloud-comuting-taxonomia-por-niveles-o-modelos-de-servicio-iaas-paas-y-saas

- Fernández Pasos, Gonzalo. *"Integración de sistemas y cloud computing"* (online) Mercado.7/11/2012.http://www.mercado.com.ar/notas/googleorganic/374070/noticias-desde-google?id=374070

- Fraga Iglesias, Alberto. "*La nube impulsara la adopción de soluciones de seguridad 2014".* (online) TICbeat. 25/8/2014 http://cloud.ticbeat.com/empresas-aceleran-adopcion-soluciones-seguridad-2014-nube-principal-catalizadora/

- Gonzalez Allonca, J.C., Piccirilli, D., "*Consideraciones Legales Relativas a la Privacidad en Proyectos de Cloud Computing en el Exterior de Argentina*. Revista Latinoamericana de Ingeniería de Software" (online). Febrero 2014, vol. 2, n.1, p. 77-90. http://www.unla.edu.ar/sistemas/redisla/ReLAIS/relais-v2-n1-revista.pdf ISSN 2314-2642

- Granero, Horacio R. "*Problemas legales de la Cloud Computing".* El Dial.com. 12/9/2010. [elDial.com-DC14B2] Consulta: 30 agosto 2014

- Lía, Mario. "*Cloud Computing se consolida".* Mercado [en línea]. 26/3/ 2014. N. 1153.http://www.mercado.com.ar/notas/tecnologa%7C/8015115/%3Cb%3Ecloud-computing%3Cb%3E-se-consolida-

- Martínez, Anna. "*Los servicios cloud contaran con 3.600 millones de usuarios en 2018*"(online).VozTele.comNews.3/9/2014.http://blog.voztele.com/2014/09/03/los-servicios-cloud-contaran-con-3-600-millones-de-usuarios-en-2018

- Toscano Silvia y Galmarini Luciano. "*Protección de datos personales en la nube".* La Ley. Suplemento Actualidad. 04/10/2012, Año LXXVI Nº 187 / ISSN 0024-1636. La Ley 2012-E

II. Normativa

- Disposición Nº 11/2006 DNPDP : "Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Banco y Bases de Datos Públicos no estatales y Privados": http://www.infoleg.gov.ar/infolegInternet/anexos/120000-124999/120120/norma.htm

- Disposición Nº 4/2009 DNPDP: http://www.protecciondedatos.com.ar/disp42009.htm

- Decreto 1558/01 DNPDP *http://infoleg.mecon.gov.ar/nfolegInternet/anexos/70000-74999/70368/norma.htm*

- ISO 27001 en Español (online) © 2012 http://www.iso27000.es/iso27000.html

- Ley 25.326 Protección de Datos Personales, http://www.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm