Marco normativo de Protección de Datos Personales de Argentina en los Servicios Cloud Computing.

Marcelo G. I. Temperini

Director de la Red Iberoamericana de Derecho Informático – elderechoinformatico.com, Estudiante de Derecho de Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral. Analista de Seguridad y Vulnerabilidades. Director de AsegurarTe – Consultora en Seguridad de la Información. temperinimarcelo@gmail.com

Abstract Español. Los servicios Cloud Computing son cada más utilizados por las empresas y organizaciones de Argentina, con un crecimiento continuo basado en las ventajas técnicas y económicas que ofrecen los mismos. Sin embargo, si en alguno de los servicios utilizados en la nube interviene algún tipo de dato personal, deberá prestarse especial atención al cumplimiento de las exigencias del régimen normativo. Un sistema legal argentino de protección de datos personales que si bien no ha sido diseñado para la dinámica de esta nueva gama de servicios, si ofrece herramientas para poder realizar dicho tratamiento de datos personales de manera lícita. El marco jurídico basará su estructura en el tratamiento automatizado de datos personales por parte de terceros (o prestación de servicios informatizados) del Art. 25 de la Ley 25.326, sumado a la reglamentación vigente del Decreto 1558-2001 y las Disposiciones de la Dirección Nacional de Protección de Datos Personales. En relación a su análisis, será el objeto de este trabajo señalar los diferentes tópicos y elementos a tener en cuenta para poder realizar la migración de los Servicios a la nube, asegurando siempre el nivel de protección adecuado que se debe brindar a los datos personales.

Abstract en Inglés: Cloud Computing services are becoming more used by companies and organizations in Argentina, with continued growth based on technical and economic advantages offered by them. However, whether any of the services used in the cloud involved some kind of personal data, should pay particular attention to compliance with the requirements of the regulatory regime. Argentine legal system to protect personal data but has not been designed for the dynamics of this new range of services if offers tools to make such personal data in a lawful manner. The legal framework structure based on automated processing of personal data by third parties (or computer services) of Article 25 of Law 25,326, in addition to current regulations of Decree 1558-2001 and the provisions of the National Personal Data Protection. In relation to its analysis, the purpose of this study point out the different topics and features taken into account to perform the migration of services to the cloud, always ensuring adequate level of protection should be extended to personal data.

Keywords: propiedad intelectual, cloud computing, licencias, Internet, servicios en la nube, contenidos, empresas proveedoras, usuarios.

Introducción.

Los Servicios Cloud Computing están cambiando la forma en que los negocios se operan y la forma en que funciona la tecnología de la información. Las Tecnologías de la Información (IT) son herramientas que cada día van creciendo en su potencial, impactando todos y cada uno de los aspectos en la forma de operar de la organización.

Esta nueva gama de Servicios consigue aportar esas ventajas, apoyándose sobre una infraestructura tecnológica dinámica que se caracteriza, entre otros factores, por un alto grado de automatización, una rápida movilización de los recursos, una elevada capacidad de adaptación para atender a una demanda variable, todo a un precio flexible en función del consumo realizado.

Este contexto de conveniencia técnica y sobre todo, de conveniencia económica, genera el ambiente propicio para la incubación de múltiples proyectos de migración de Servicios hacia la nube, tanto para las empresas privadas como para organismos públicos.

Es en este punto donde debe tenerse especial cuidado en proyectar y contemplar los diferentes aspectos legales de las migraciones, analizando si existen consecuencias riesgosas para la empresa, y en tal caso, brindar la alternativa de evaluar la conveniencia del proyecto.

Los diferentes tópicos legales que deben ser tenidos en cuenta, dependen de cada negocio o proceso a migrar, y es por ello que este tipo de contrataciones suelen ser un "traje a medida" para cada empresa u organización. Sin embargo, entre ellos, se destacan el tema de propiedad intelectual de los contenidos transferidos y la protección de los datos personales, y es éste último lo que desarrollaremos en este trabajo.

Se presenta así como objeto de la investigación, el análisis sobre la factibilidad de realizar lícitamente la migración a Servicios Cloud Computing cuando intervengan datos de tipo personal, haciendo foco en las diferentes alternativas y requisitos exigidos por la normativa argentina en protección de datos personales.

El Modelo Cloud Computing, una tendencia en crecimiento.

Este nuevo modelo de prestación de servicios permite al Usuario (en adelante, será utilizado tanto para identificar a una persona individual, empresa u organización) acceder a un catálogo de servicios (en el caso de Software como Servicio –SaaS-) estandarizados y responder a las necesidades de su negocio, de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo efectuado.

Este cambio de paradigma permite aumentar el número de servicios basados en la red, radicando allí la clave de los beneficios para los proveedores, que pueden ofrecer, de forma más rápida y eficiente, un mayor número de servicios, así como para los

usuarios, quienes tienen la posibilidad de acceder a ellos, disfrutando de la inmediatez del sistema y de un modelo de pago por consumo.

Según la Consultora Gartner[1], se calcula que las corporaciones van a destinar 112.000 millones de dólares en los próximos cinco años a segmentos como el SaaS, plataforma como servicio (PaaS) e infraestructura como servicio (IaaS). Estos expertos prevén un fuerte crecimiento en los próximos cuatro años, estimando que este sector moverá más de 148800 millones de dólares para el año 2014.

Entre los principales usuarios de estos servicios, también se observan diferencias. Actualmente, la implantación del Cloud Computing no es igual en todos los países. Así, EEUU absorbió en 2009 el 60% de los ingresos y en el ejercicio en curso mantendrá un 58%. Sólo en el año 2014, su cuota de mercado se diluirá por debajo del 50% en la medida en que otros mercados vayan acelerando la adopción de estas tecnologías.

Los Datos Personales dentro de los Servicios a migrar.

Si bien los datos personales forman parte de la mayoría de los sistemas de las empresas y organizaciones, también existen casos donde la información transmitida es de otro tipo, quedando ésta totalmente al margen de cumplir con las exigencias de las normas argentinas. El siguiente trabajo parte del supuesto de que en la migración de Servicios a la nube, intervengan algún tipo de datos personales. En estos casos, donde debe hacerse un serio análisis de la situación de dichos datos, para poder evaluar por un lado si la tecnología ofrecida por el proveedor cumple con las exigencias de la ley, y por otro, si la propia empresa u organización posee y trata dichos datos personales de acuerdo a lo establecido por la norma.

El interrogante principal que se busca desarrollar es **¿qué sucede con el tratamiento de los datos personales en el caso de que decida utilizar algún Servicio Cloud Computing?**

Cada empresa o proceso posee características particulares que deben ser evaluadas detenidamente por un profesional en la materia. Este trabajo, sólo tiene por objetivo brindar una guía académica y general sobre las diferentes situaciones que deben analizarse en relación a la protección de los datos personales en este tipo de servicios, siempre a la luz de la normativa argentina.

Primero debemos comenzar repasando algunos conceptos de la Ley de Protección de Datos Personales de Argentina, Nº 25.326 (en adelante LPDP). Según el Art. 2, será **tratamiento de datos personales:**

> ***Tratamiento de datos:*** *Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias".*

1 Gartner Inc. [en línea] <http://www.gartner.com/technology/research/cloud-computing/index.jsp>

Puede observarse que el concepto de tratamiento de datos es lo suficientemente amplio para que todo tipo de procesos sea considerado como tratamiento a fines de la Ley.

Se avanza a fin de establecer una diferencia de relevancia para los Servicios de Cloud Computing: ¿existe **cesión de datos personales** o estamos ante el caso de **tratamiento por parte de terceros**? Respondiendo este interrogante, es que se desprenden consecuencias legales importantes.

Casos de cesión de datos.

Será **cesión de datos personales** en los casos donde una Empresa A (cedente), titular de la base de datos personales, transfiera (de manera gratuita u onerosa) dicha base a una Empresa B (cesionaria), quedando esta última facultada para la utilización y tratamiento de esos datos personales, siempre **dentro de los fines** para los cuáles se recolectaron. Dicha utilización por parte de la cesionaria, **no es ni a nombre ni bajo la dirección** de la cedente, de manera que podrá realizar el tratamiento por cuenta propia, siempre respetando los límites de dicha cesión.

En estos casos, existe para el titular de los datos personales un mayor riesgo de que sus datos sean mal utilizados, y es ese el fundamento de la normativa vigente para exigir más requisitos a fines de salvaguardar a sus titulares.

Según el **art. 11** de la LPDP (la negrita pertenece al autor):

> ***ARTICULO 11. — (Cesión).***
>
> *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.*
> *2. El consentimiento para la cesión **es revocable**.*
> *3. El consentimiento no es exigido cuando:*
> *a) Así lo disponga una ley;*
> *b) En los supuestos previstos en el artículo 5° inciso 2;*
> *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.*

> *4. **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.*

Extraemos de este artículo que, en el caso de existir cesión, se debe contar con consentimiento especial del titular; debe siempre respetarse la finalidad y el cesionario queda sujeto a las mismas obligaciones del cedente, **respondiendo siempre solidariamente**. Vale destacar en este punto sobre la responsabilidad, que es un imperativo de le ley, de manera que **no podrá ser dejado de lado por las partes** a tenor de un contrato entre las mismas (práctica que se suele utilizar en los contratos).

Casos de tratamiento automatizado por parte de terceros.

Será **tratamiento por parte de terceros** en los casos donde la Empresa A (titular de la base de datos personales), transfiere a una Empresa B (encargada del tratamiento) el procesamiento de datos de carácter personal **por cuenta y conforme a las instrucciones** de la Empresa A. En estos casos el tratamiento se realiza para la prestación de un servicio con **finalidad técnica** determinada por el responsable de la base. Estas finalidades técnicas pueden ser variadas y combinadas, y es por ello que se brindarán algunos ejemplos utilizando la línea de Servicios Cloud Computing de **Google**, cada uno en relación a cada modelo de Servicio en la nube

En el primer caso, con el modelo de SaaS, donde se brinda al consumidor la capacidad de utilizar aplicaciones directamente desde la infraestructura del proveedor. Supongamos la utilización de la Empresa A de los Servicios de *Google Apps for Business*[2], más específicamente de la herramienta de Google Docs, a través de la cuál utiliza su Servicio de planilla de cálculos donde lleva registrado los datos personales de sus empleados, junto con los datos de fechas de pago de sueldos y demás aportes. En este ejemplo, la Empresa A que es titular de la base, administra de manera plena dichos datos, que son alojados y procesados por los servidores de Google, que en ningún momento posee sobre dicha información, la posibilidad de realizar algún tratamiento independiente de la dirección de la empresa contratante.

El segundo modelo es de PaaS, donde se le permite al Usuario consumidor desplegar dentro de la infraestructura del proveedor, aplicaciones privadas, incluso adquiridas, usando lenguajes de programación y herramientas del proveedor. Aquí se podría dar el caso de que la Empresa A, responsable de la base denominada "Clientes 2007-2011", en la cuál se encuentran los datos personales de todos sus clientes dentro de ese lapso de tiempo. La Empresa A, Usuaria de los servicios de *Google App Engine*[3]**,** en cuya plataforma tiene montado un software privado para el envío masivo de novedades a su base de clientes. Queda claro que la empresa proveedora (Google en este caso), en ningún momento recibe esa base de datos a modo de cesión, sino que

2 Google Apps for Business [en línea] <http://www.google.com/apps/intl/es/business/index.html>

3 Google App Engine [en línea] <http://code.google.com/intl/es/appengine/>

sólo participa de la operación como **tercero**, siendo sólo un ejecutante técnico de las instrucciones de la empresa contratante.

El tercer caso será en el modelo aún menos explotado, que es de IaaS. En este, se permite al consumidor aprovisionar recursos computacionales como almacenamiento, procesamiento, redes y otros elementos fundamentales en donde él puede desplegar y correr el software que desee, incluyendo sistemas operativos y aplicaciones. A fin de cuentas, el proveedor brinda solamente el hardware, quedando todo lo demás en manos del Usuario consumidor. Supongamos aquí que la Empresa A, contrata este Servicio, realizando la carga de un sistema Unix en uno de los servidores disponibles, ejecutando en el mismo un software programado a medida, a través del cuál la Empresa A realiza la recolección de pedidos de mercadería y que entre dichos datos, existen datos personales de sus clientes. Quizás este sea el ejemplo más extremo, donde se observa que el proveedor de Servicios, sólo se compromete a brindar al Usuario consumidor, un marco de disponibilidad de hardware para que él mismo realice toda la carga y mantenimiento de sistemas.

Vale destacar que en esta clásica clasificación de los 3 modelos, existe en realidad una superposición de servicios. Es decir, cuando hablamos de SaaS, en realidad también existe de fondo la prestación de un Servicio de PaaS y IaaS, pero solamente limitado al Servicio en particular que se contrata. De la misma manera, al trabajar en un PaaS, también existe un IaaS de fondo. Existe entre los 3 niveles, una relación de inclusión vertical según las jerarquías de servicios.

Volviendo a los ejemplos, se puede deducir en cada caso, que los datos son **tratados por cuenta y con instrucciones de la Empresa A**, de manera que el proveedor únicamente procesa y carga esos datos siguiendo la orden y dirección del responsable de la base de datos. Es decir, la prestadora de Servicios de Cloud Computing (Google en nuestro ejemplo), interviene en el tratamiento como un mero **intermediario técnico** que brinda en un caso la infraestructura, en otro una plataforma y en otros un software específico para poder ejecutarse ciertas instrucciones a esos datos.

Prestación de servicios informatizados en los Servicios de Cloud Computing.

En los Servicios en la nube existe **tratamiento de datos personales por terceros** o mejor dicho, existe prestación de servicios informatizados, que es como se lo considera según la legislación argentina, la cual citamos a continuación (la negrita pertenece al autor):

> ***ARTICULO 25. —*** *(Prestación de servicios informatizados de datos personales).*
> *1. 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****.*
> *2. 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****.*

Como se puede observar, existen claras diferencias jurídicas con respecto a la cesión de datos. Sin embargo, al texto del Art. 25, debe agregarse lo dispuesto en la **Reglamentación 1558-2001** de la Ley, en donde se establece que (la negrita pertenece al autor):

> ***ARTICULO 25.-*** *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***.

De dicha reglamentación, se obtienen nuevos elementos a tener en cuenta para poder llevar a cabo de manera legítima la migración de Servicios que contengan datos personales. Repasando todos los requisitos vistos hasta el momento, se debería contemplar la realización de un **contrato escrito de prestación de servicios de tratamiento de datos personales** en donde se considere particularmente:

- Prohibición de que la empresa proveedora utilice los datos personales para fines diferentes a los dispuestos en el contrato.
- Disponer expresamente que la empresa proveedora solamente procesará la información siguiendo instrucción y órdenes del titular contratante.
- Prohibición de que la empresa proveedora ceda los datos a terceros, ni aún para su conservación.
- Prever la supresión de los datos personales para el caso de finalización de la relación de servicios.
- La empresa proveedora se obligue a tener implementada sobre los datos personales, los niveles de seguridad exigidos por la Autoridad de Control.
- La empresa proveedora se obligue a mantener la confidencialidad y reserva de la información tratada.

Según lo trabajado hasta el momento, puede observarse que es esencial dejar bien documentada la relación entre las partes, siendo el primer requisito la existencia de un **contrato de prestación de servicios de tratamiento de datos personales**, en el cual deberá aclararse que la empresa prestadora de los Servicios se compromete a cumplir

con los niveles de seguridad previstos en la ley, la reglamentación y las normas complementarias que dicte la Dirección Nacional de Protección de Datos Personales (**DNPDP**), como así también las obligaciones que surgen en orden a la **confidencialidad y reserva** que deben mantener sobre la información obtenida.

Este tipo de compromisos sobre seguridad, confidencialidad y reserva no revisten mayores problemas para las grandes empresas que prestan esta clases de servicios. Por ejemplo, es el caso de *Google*[4], quien dentro de sus Políticas de Privacidad[5] expresa que cumple los principios de privacidad de garantía de seguridad establecidos a través del programa Safe Harbor de Estados Unidos, nivel que es suficiente para cubrir tanto las exigencias legales en materia de datos personales de la Unión Europea, así como las de Argentina (que sigue el mismo modelo europeo).

No obstante, la empresa u organización interesada en la migración de servicios a la nube, deberá asegurarse que la prestadora asuma y garantice estas obligaciones, ya que en caso de incumplimiento (por ejemplo, fuga de información) será la empresa contratante quien debe responder ante los titulares de los datos personales.

Entre las demás obligaciones que señala la legislación, destacamos la **prohibición de realizar algún tipo de cesión**. Ello significará que la prestadora de Servicios deberá realizar los procesos automatizados de manera personal, sin posibilidad de transferir la información tratada a un tercero, **ni siquiera para fines de almacenamiento.**

Mencionamos también la **obligación de suprimir los datos** una vez finalizado el tratamiento, salvo que sea un caso de prestaciones periódicas, donde en caso de ser razonable, la prestadora de Servicios podría almacenarlos hasta un plazo máximo de 2 años. Sin dudas que esta premisa fue pensada en aquellas prestaciones de servicios de tratamiento que se realizan de modo esporádico o eventual. Esto bien podría ser de utilidad en el caso de contratación de un SaaS por un período de 6 meses para una actividad específica. En los casos de migración de Servicios esenciales de las empresas, el tiempo de Servicio es **indeterminado** (en general, son contratos a largo plazo) y esta exigencia dejaría de tener relevancia al menos durante el período de vigencia de la relación, quedando suspendida hasta el momento incierto donde finalice la relación, y es allí donde la obligación de supresión de los datos tendría sentido.

Casos de transferencia internacional de datos personales.

La adecuación del contrato a lo exigido por la normativa de datos personales ha sido siempre considerando que la prestación de los Servicios se mantenga **dentro del territorio argentino**. Sin embargo, debe mencionarse que las principales prestadoras de Servicios Cloud Computing están alojadas en el exterior de nuestro país (especialmente en EEUU).

[4] Google tiene aprobado las auditorías SAS 70 Tipo II (Statement on Auditing Standards No. 70), un estándar de auditoría reconocido internacionalmente y desarrollado por el AICPA (American Institute of Certified Public Accountants).

[5] Políticas de Privacidad de Google [en línea] <http://www.google.es/intl/es/privacy/privacy-policy.html>

Queremos destacar que se ha dejado este aspecto para el final, porque metodológicamente se consideró lo más adecuado, dado que primero debía tenerse claro cuál era la situación del tratamiento de datos personales en el país, para luego poder comprender cuáles son los requisitos extras que deberán tenerse en cuenta si la empresa proveedora se encuentra en un país extranjero.

Vale recordar un debate existente en la actualidad, relacionado con el elemento que indica que un proveedor está o no en el país. Por un lado, se sostiene que basta con la presencia de servidores en el país, otros en cambio sostienen que es necesario que tanto la empresa (con su domicilio legal) como los servidores se encuentren dentro del territorio argentino. Personalmente considero que dicha discusión no reviste de mayor importancia, ya que basta con que alguno de los elementos (servidores u oficinas) se encuentre en el exterior del territorio para que sean exigibles los requisitos de transferencia internacional.

En la **LPDP**, la transferencia internacional de datos personales está regulada en el Art. 12 (la negrita pertenece al autor):

> ***ARTICULO 12. —*** *(Transferencia internacional).*
> *1. Es* ***prohibida la transferencia*** *de datos personales de cualquier tipo con países u organismos internacionales o supranacionales,* ***que no proporcionen niveles de protección adecuados****.*
> *2. La prohibición no regirá en los siguientes supuestos:*
> *a) Colaboración judicial internacional;*
> *b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior;*
> *c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;*
> *d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;*
> *e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.*

La norma argentina sigue la línea europea, en el sentido que **prohibe la transferencia de datos personales a algún país que no proporcione los niveles de protección adecuados.** Salvo las excepciones receptadas por el propio artículo, pareciera no haber salida alternativa para el caso de que el país no posea una regulación considerada "adecuada". No obstante, en la reglamentación del Decreto 1558-2001 de dicho artículo, se brindan mejores herramientas (la negrita pertenece al autor):

> ***ARTICULO 12.- La prohibición de transferir datos personales*** *hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados,* ***no rige cuando el titular de los datos hubiera consentido expresamente la cesión****.*
> *No es necesario el consentimiento en caso de transferencia de datos desde un registro público que esté legalmente constituido para facilitar*

> *información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta.*
> *Facúltase a la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES a evaluar, de oficio o a pedido de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional. Si llegara a la conclusión de que un Estado u organismo no protege adecuadamente a los datos personales, elevará al PODER EJECUTIVO NACIONAL un proyecto de decreto para emitir tal declaración. El proyecto deberá ser refrendado por los Ministros de Justicia y Derechos Humanos y de Relaciones Exteriores, Comercio Internacional y Culto.*
> ***El carácter adecuado del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos****; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración de tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales.*
> ***Se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección*** *cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación,* ***o del amparo que establezcan las cláusulas contractuales*** *que prevean la protección de datos personales.*

Atendiendo a lo visto, para lograr avanzar en materia de datos personales con transferencia internacional, se plantean las siguientes alternativas:

A) El país al cual se realizará la transferencia de datos personales posee un nivel adecuado de protección. Por ejemplo, si la empresa proveedora de servicios estuviera en España, país que posee un adecuado nivel de protección según la Autoridad de Control Argentina (DNPDP), no será necesario permiso especial alguno.

Vale aquí dedicarle algunas palabras a mencionar el **Acuerdo de Puerto Seguro (Safe Harbor)**, nacido de una clara necesidad comercial entre los EEUU y la Unión Europea, en donde los principios de protección de datos difieren tanto en su visión del sistema como en su protección. Por ello, y ante las restricciones para las transferencias internacionales de datos establecidas por la **Directiva 95/46/CE**, donde se establece que *"Los Estados miembros deben prever que la transferencia a un tercer país de datos personales* ***únicamente pueda efectuarse cuando el tercer país de que se trate garantice un nivel de protección adecuado*** *y cuando con anterioridad a la transferencia se respeten las disposiciones legales de los Estados miembros adoptadas con arreglo a las demás disposiciones de dicha Directiva"*. De esta manera, ambas potencias comenzaron a finales del siglo pasado a negociar y consensuar un sistema que permitiese dinamizar sus relaciones comerciales.

Esta negociación terminó con el Acuerdo de Puerto Seguro, aprobándose por parte de la Unión Europea[6], lograndose así que empresas de los EEUU que se adhieran al mismo (sólo éstas y no sus filiales en otros países), contarán con la ***"presunción de adecuación" al nivel de adecuación exigido por la Directiva",*** según lo establece la propia Agencia Española de Protección de Datos[7].

De esta manera, grandes potencias como Google o Amazon, están suscriptas al convenio, gozando de esta presunción para sus transferencias de datos con la Unión Europea, logrando de esta manera una mayor agilidad en las transacciones, alternativa que lamentablemente no rige para la República Argentina, pero que sí fue considerada como **país con nivel adecuado** en materia de Protección de Datos Personales según la Unión Europea y en los términos de la Directiva N° 95/46/CE[8]. La citada declaración significa que a Argentina **no se le aplican las restricciones** para la transferencia de datos personales, permitiendo el libre flujo de los datos personales desde la Unión Europea. De manera tal que si la empresa proveedora estuviera dentro de la Unión Europea, la transferencia internacional de datos sería lícita desde la Argentina (siempre reuniendo todos los demás requisitos).

B) El país al cual se realizará la transferencia de datos personales no posee un nivel adecuado de protección. En este caso, tenemos las siguientes alternativas:

1) Solicitar al titular de los datos el consentimiento para la transferencia internacional a terceros países que no brinden los niveles de protección adecuados: Esta alternativa es compleja de considerar en aquellos casos donde la base de datos sea de gran magnitud, ya que en la práctica es muchas veces complicado conseguir este consentimiento especial de todos los titulares de los datos que se alojan. En cambio, sería viable para casos de menor entidad, como por ejemplo una base de datos de 50 empleados de una empresa, donde sería factible conseguir un nuevo consentimiento para el caso particular.

2) Establecer un marco contractual adecuado que garantice el nivel de protección de los datos personales: En este caso, se buscará la obtención del marco seguro que permita la transferencia internacional de los datos, a través de un contrato especial confeccionado entre las partes.

---

[6] Decisión de la Comisión (26 de julio de 2000) con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

[7] Agencia Española de Protección de Datos [en línea] <https://www.agpd.es/portalwebAGPD/internacional/adecuacion/estados_unidos/common/pdf s/ElAcuerdodePuertoSeguroconlosEstadosUnidos.pdf>

[8] Decisión de la Comisión Europea C(2003) 1731 [en línea] <http://www.jus.gob.ar/media/33379/DecisionUE.pdf>

El marco contractual como alternativa para permitir la transferencia internacional.

Allí es donde interviene la **DNPDP**, a quien deberemos remitir el contrato para lograr conseguir la aprobación de un "permiso especial" que pueda suplir este requisito del Art. 12.

En la práctica, la DNPDP recibe un buen número de solicitud de aprobaciones de transferencias internacionales, existiendo incluso un formulario especial para ello: el **Certificado C.01**. Esta cantidad de pedidos, es también consecuencia de que según ha sostenido la DNPDP en numerosos dictámenes[9], EEUU **no posee un adecuado nivel de protección**, obligando así a que cada empresa que quiera transferir datos hacia Norteamérica (el principal país donde están radicadas las empresas proveedoras) deban cumplimentar con este contrato extra aprobado como requisito.

Según la DNPDP, este contrato debe contener como mínimo:

- *Identificación del exportador y al/los importador/es de los datos;*
- *Indicar la ubicación de la base de dato;*
- *Definir como ley aplicable al tratamiento de datos del contrato de servicios a la Ley Nº 25.326;*
- *Se precisen la naturaleza de datos personales que se transferirán;*
- *La declaración que el tratamiento de los datos se realizará en un total de acuerdo con los principios y disposiciones de la Ley Nº 25.326;*
- *Indicar la finalidad a la que serán destinados dichos datos, verificando que cumpla con los requisitos del art. 4 de la Ley Nº 25.326;*
- *Precisar las medidas de seguridad a las que se sujetará la transferencia y el tratamiento de datos personales, verificando que la misma cumpla con las pautas habituales del sector y con la normativa vigente;*
- *El compromiso del importador que los datos recibidos serán tratados en un todo y sin excepciones según las instrucciones del exportador y las disposiciones de la Ley Nº 25.326, aceptando que se le apliquen las facultades de la DNPDP y respetando los derechos de los titulares de los datos conforme Ley Nº 25.326, como ser los derechos de acceso, rectificación, actualización, confidencialidad y supresión;*
- *La declaración del importador manifestando que la legislación local aplicable no le impide cumplir con las obligaciones pactadas;*
- *La obligación de destruir, y en su caso reintegrar al exportador, los datos personales objeto de la transferencia cuando finalice el contrato;*
- *Se respetará la jurisdicción de los Tribunales argentinos por cualquier conflicto vinculado a la protección de los datos personales que afecte al titular del dato;*
- *El compromiso por parte de importador de no divulgar ni transferir los datos personales a terceros con excepción que: 1) se establezca de manera específica en el contrato o se requiera para la prestación de servicios de tratamiento, o 2) la cesión sea requerida por una ley aplicable o autoridad*

[9] Dictámenes DNPDP Nros: 248/05; 270/06; 008/08; 017/09; 028/09; entre otros.

> *competente, en la medida que no excedan lo necesario en una sociedad democrática, es decir, cuando constituyan una medida necesaria para la salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales o administrativas, o la protección del interesado o de los derechos y libertades de otras personas, en cuyo caso deberán notificar de manera inmediata y por escrito al exportador para evaluar si dicha transferencia afecta las disposiciones de protecciones de datos personales locales y en consecuencia afecte la continuidad del contrato.*

La alternativa para lograr asegurar el nivel de protección adecuado mediante el marco contractual, exige el desarrollo de un contrato especial que es una pequeña "ley a medida" para las partes. Para poder avanzar en dirección a esta alternativa, deberemos tener la posibilidad de consensuar este **contrato de cláusulas especiales** que comprometan a la empresa proveedora de Servicios a cumplir con el marco normativo argentino, cuestión que no todas las empresas proveedoras están dispuestas a aceptar.

Conclusiones.

Para **realizar lícitamente la migración** de una empresa u organización hacia los Servicios Cloud Computing donde intervengan algún tipo de datos personales, será necesario analizar, prever y proyectar una importante cantidad de requisitos jurídicos, establecidos como obligatorios por el marco normativo argentino.

Para todo proyecto de migración debe partirse de la base en donde la propia empresa u organización interesada en trabajar en la nube, tenga **total adecuación de los datos personales dentro de su propia empresa**, para desde allí comenzar a construir y recolectar los demás elementos necesarios para cada tipo de transferencia (ya sea local o internacional).

Finalmente destacamos la gran importancia de contar con un proveedor de Servicios de Cloud Computing que reúna los requisitos de seguridad de la información mínimos exigidos, y sobre todo que permita la **negociación contractual** (en oposición a los contratos por adhesión), cuestión necesaria y esencial para poder establecer cláusulas diseñadas por las partes adaptadas para el caso concreto.