INFORME:

Utilización del *Cloud Computing* por los despachos de abogados y el derecho a la protección de datos de carácter personal

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA

INFORME:

Utilización del *Cloud Computing* por los despachos de abogados y el derecho a la protección de datos de carácter personal

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CONSEJO GENERAL
DE LA ABOGACÍA
ESPAÑOLA

Índice

Utilización del *Cloud Computing* por los despachos de abogados y derecho a la protección de datos de carácter personal

1 Introducción. El concepto del *Cloud Computing* y los servicios para los despachos de Abogados

El llamado *Cloud Computing* es un modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda y a través de la red a un conjunto de recursos compartidos y configurables (como redes, servidores, capacidad de almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor de servicios.

El modelo, según *The NIST Definition of Cloud Computing*, tiene las siguientes cinco características esenciales:

1. Autoservicio bajo demanda. El usuario puede acceder a capacidades de computación "en la nube" de forma automática conforme las necesita sin necesidad de una interacción humana con su proveedor o sus proveedores de servicios *Cloud*.

2. Múltiples formas de acceder a la red. Los recursos son accesibles a través de la red y por medio de mecanismos estándar que son utilizados por una amplia variedad de dispositivos de usuario, desde teléfonos móviles a ordenadores portátiles o PDAs.

3. Compartición de recursos. Los recursos (almacenamiento, memoria, ancho de banda, capacidad de procesamiento, máquinas virtuales, etc.) de los proveedores son compartidos por múltiples usuarios, a los que se van asignando capacidades de forma dinámica según sus peticiones. Los usuarios pueden ignorar el origen y la ubicación de los recursos a los que acceden, aunque sí es posible que sean conscientes de su situación a determinado nivel, como el de CPD o el de país.

4. Elasticidad. Los recursos se asignan y liberan rápidamente, muchas veces de forma automática, lo que da al usuario la impresión de que los recursos a su alcance son ilimitados y están siempre disponibles.

5. Servicio medido. El proveedor es capaz de medir, a determinado nivel, el servicio efectivamente entregado a cada usuario, de forma que tanto proveedor como usuario tienen acceso transparente al consumo real de los recursos, lo que posibilita el pago por el uso efectivo de los servicios.

En definitiva, desde la perspectiva de los despachos de abogados como usuarios, el modelo *Cloud Computing* permite acceder a una serie de servicios, que pueden ir desde el correo electrónico hasta el almacenamiento de documentos, pasando por aplicaciones de gestión del despacho, de contabilidad, de bases de datos de jurisprudencia o legislación, o de compartición

1 de documentación e información con clientes o con otros despachos; y todo ello sin necesidad de disponer de servidores o de software en el propio despacho, con sus necesidades asociadas de mantenimiento y administración, y con las correspondientes inversiones en equipamiento y software y gastos en operación y mantenimiento de los mismos. Los datos y las aplicaciones se encuentran en algún lugar de Internet que se representa frecuentemente como una nube, de ahí el término *Cloud Computing*.

Las ventajas técnicas y económicas del modelo son inmediatas para los usuarios. No es necesario que los despachos –especialmente los más pequeños- cuenten con personal informático propio dedicado al mantenimiento de los servidores y las aplicaciones. Los servicios tecnológicos pasan a ser un gasto operativo, obviándose la necesidad de inversiones en infraestructuras de breves ciclos de vida y rápida obsolescencia. El acceso a los servicios está garantizado desde cualquier lugar del mundo en el que se disponga de una conexión a Internet, y el proveedor de servicios asegura la disponibilidad del servicio y la actualización permanente de aplicaciones y sistemas.

Sin embargo, como ya sucedió en el pasado con otras innovaciones tecnológicas, surgen dudas relativas a la seguridad e integridad de la información, especialmente la que pueda tener una naturaleza más sensible por su carácter confidencial, así como ciertas lógicas reservas a perder el control físico de los datos de carácter personal que sean objeto de tratamiento en el despacho, que dejan de estar en los servidores propiedad del mismo o en discos o dispositivos que se guardan en un lugar que cuente con las medidas de seguridad exigidas por la normativa de protección de datos. Efectivamente, los datos en el modelo de *Cloud Computing* pasan a situarse en algún lugar indeterminado, en un servidor cuya ubicación física desconoce el responsable.

Para ilustrar esta desconfianza, hasta cierto punto lógica, valga como ejemplo el hecho de que el Comité de Ética y Responsabilidad Profesional de la Asociación Americana de la Abogacía *(American Bar Association, Standing Committee on Ethics and Professional Responsibility)* no consideró el correo electrónico como medio válido y seguro para comunicarse con los clientes hasta el año 1999, en el que mediante la *"Formal Opinion No. 99-413, Protecting the Confidentiality of Unencrypted E-Mail",* consideró que el correo electrónico ofrecía la misma expectativa razonable de privacidad que el correo postal, el fax o el teléfono.

Por su parte, el llamado Grupo de Berlín, *International Working Groupon Data Protectionin Telecommunications* en su reciente *Working Paper onCloud Computing-Privacy and Data Protection issues,* denominado *"Sopot Memorandum",* adoptado en la 51 Sesión celebrada los días 23-24 Abril de 2012, en Sopot (Polonia) ha señalado la importancia del *Cloud Computing* y ha resaltado que nos encontramos ante un cambio de paradigma y una nueva situación en

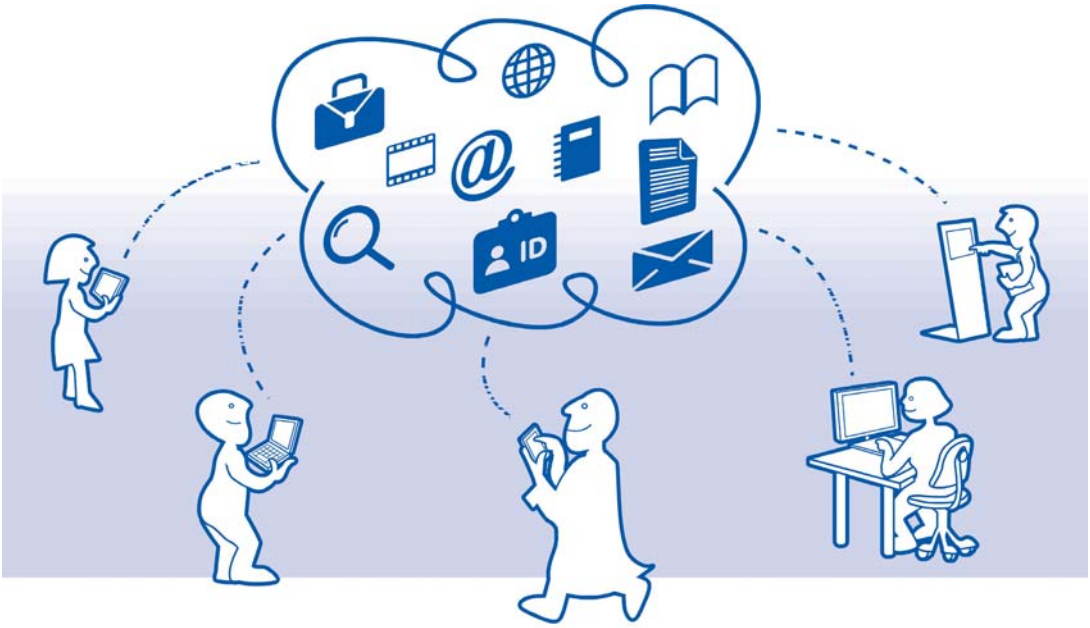
la que es necesario dar "pasos cuidadosamente medidos, especialmente en lo que respecta a la privacidad y la protección de datos".

A la vista de todo ello, el Consejo General de la Abogacía Española y la Agencia Española de Protección de Datos (AEPD) han decidido elaborar conjuntamente este Documento cuyo propósito es señalar cuáles son los aspectos esenciales que, en el marco de la legislación de Protección de Datos de Carácter Personal, deben tomar en consideración los despachos de abogados a la hora de contratar servicios *Cloud Computing* para su actividad diaria y sus relaciones con sus clientes.

Para ello, en los apartados siguientes se desarrollan los que se han considerado tres aspectos esenciales que deben tenerse en cuenta a la hora de decidir contratar servicios de *Cloud Computing* por un despacho de abogados:

- La responsabilidad del despacho sobre el tratamiento de los datos y la normativa y jurisdicción aplicable.
- La seguridad y confidencialidad de los datos.
- Aspectos esenciales del contrato de servicios que debe firmarse, tanto desde el punto de vista técnico como jurídico.

El enfoque que se ha dado a estos tres aspectos es eminentemente práctico; estableciendo pautas y recomendaciones para facilitar a los despachos la interlocución con los proveedores de servicios *Cloud Computing*.



2 Aplicación de la normativa sobre protección de datos

Con carácter previo es necesario resaltar que el cumplimento de la legislación de protección de datos es un aspecto esencial a la hora de contratar servicios *Cloud* por parte de un despacho de abogados.

Debe considerarse que las modalidades de computación y las modalidades de servicios condicionan la aplicación de los preceptos correspondientes de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y de su Reglamento, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD)[1]. En cualquier caso, la posición jurídica de los despachos de abogados que contraten servicios de *Cloud Computing* es la de responsables del tratamiento (art. 3.d) de la LOPD y art. 5.1.q) del RLOPD), pues a ellos les corresponde la decisión sobre la finalidad, el contenido y el uso del tratamiento, así como la decisión sobre optar por la computación en la nube y sobre su modalidad. Por su parte, el prestador de servicios de *Cloud Computing* tendrá la naturaleza de encargado del tratamiento (art. 3.g) de la LOPD y (art. 5.1.i) del RLOPD, pues en definitiva trata datos personales por cuenta del responsable.

En este marco, el contrato de prestación de servicios de tratamiento de datos personales por cuenta de terceros tiene una gran importancia. Por ello se dedica un apartado específico en el presente Documento.

En cualquier caso, la dinámica del *Cloud Computing* exige buscar soluciones que, siendo plenamente respetuosas con la LOPD y su Reglamento, permitan que los despachos de abogados puedan contratar tales servicios con garantías jurídicas y de seguridad en el tratamiento de los datos de carácter personal. En este sentido, y sin perjuicio del cumplimiento de las previsiones que contiene la legislación, y en particular las relativas al respeto a los principios de protección de datos y a la garantía de los derechos de los afectados (derechos de acceso, rectificación, cancelación y oposición), los artículos 20 a 22 del Reglamento, referentes al encargado del tratamiento, pueden ofrecer soluciones adaptadas a esta nueva realidad.

[1] Vid presentación del Adjunto al Director de la AEPD en la IV Sesión Anual Abierta de la Agencia de enero de 2012.

3 Territorialidad y jurisdicción aplicable

Como se ha señalado al principio, la propia naturaleza del modelo *Cloud Computing* hace posible que, en principio, los datos almacenados "en la nube" se encuentren físicamente en un servidor ubicado en cualquier punto del planeta. Esta circunstancia es muy relevante, al menos en materia de protección de datos de carácter personal, aunque también lo es desde el punto de vista de la resolución de posibles conflictos.

El cliente responsable del tratamiento cuando contrate servicios de *Cloud Computing* deberá velar porque el prestador de servicios cumpla la normativa española de protección de datos personales (art. 20.2 del RLOPD). Por tanto, las garantías exigibles son las establecidas en la LOPD y su reglamento de desarrollo. Este aspecto sobre la ley aplicable al tratamiento de datos personales no es disponible para las partes del contrato, que no podrán pactar la aplicación de una normativa distinta, ni excluir la competencia de la AEPD o de las Agencias o Autoridades autonómicas competentes.

En cualquier caso, el contrato de prestación de servicios de *Cloud* podrá incluir cláusulas de mediación. En tal sentido, el prestador de servicios podrá acordar que, si el titular de los datos invoca en su contra derechos de tercero beneficiario o reclama una indemnización por daños y perjuicios, aceptará la decisión de aquél de:

a) someter el conflicto a mediación por parte de una persona independiente o, si procede, por parte de la autoridad de control;

b) someter el conflicto a los tribunales del Estado miembro de establecimiento del abogado o despacho.

La muy probable circunstancia de que los datos no se almacenen en territorio español obliga a contemplar qué ocurre si los datos están almacenados en un tercer país. La Directiva 95/46/CE contempla en su artículo 25 la transferencia de datos personales a países terceros [2], señalando que la transferencia ha de limitarse a naciones en las que los datos cuenten con lo que se define como "un nivel de protección adecuado"[3]. En cuanto a la legislación nacional, el denominado movimiento internacional de datos está regulado en la LOPD en sus artículos 33 y 34, y en su Reglamento de desarrollo.

[2] http://europa.eu/legislation_summaries/information_society/l14012_es.htm

[3] La Agencia Española de Protección de Datos (AEPD) informa de los países con un nivel de protección adecuado en su página web: http://www.agpd.es/portalwebAGPD/canalciudadano/preguntasciudadano/transferencias_internacionales/index-ides-idphp.php

3 En estos casos es preciso tener en cuenta que no se pueden realizar transferencias internacionales de datos a países que no dispongan de un nivel adecuado de protección, salvo que se obtenga, previa la aportación de garantías adecuadas, la autorización del Director de la AEPD.

A estos efectos, hay que distinguir:

- Si la transmisión de los datos derivada de la prestación de los servicios de *Cloud* se realiza en el territorio del Espacio Económico Europeo, no tienen la consideración de transferencia internacional de datos, según el artículo 5.1.s) del RLOPD, por lo que no resulta necesaria la autorización de la AEPD, si bien se habrá de observar el resto de las garantías descritas en este documento.

- Cuando los datos se destinen a cualquiera de los países con un nivel de protección que se considera adecuado por Decisión de la Comisión Europea, la normativa de protección de datos del país en cuestión es considerada equiparable a la europea, por lo que tampoco resulta necesaria la autorización de la AEPD. Al igual que en el supuesto anterior también deberán observarse el resto de garantías enumeradas en este documento.

- Estas consideraciones son así mismo extensivas a los proveedores radicados en los EEUU que se hayan adherido voluntariamente para la prestación de estos servicios al acuerdo de "puerto seguro" *(safeharbor)*[4] , en virtud del cual se obligan a cumplir requisitos equivalentes a los europeos en materia de protección de datos. No obstante, debe reiterarse que siempre será necesario suscribir un contrato de prestación de servicios conforme a la LOPD (FAQ nº 10 de la Decisión 2000/520/CE) y que si el proveedor radicado en EEUU va a transferir los datos personales a un tercer país deberá aportar garantías por escrito para ofrecer, como mínimo, el mismo nivel de protección que se le haya requerido.

Cuando se contraten los servicios de un proveedor de *Cloud Computing* que transfiera la información a un país que no ofrezca un nivel adecuado de protección habrá de obtenerse la autorización previa del Director de la AEPD, según el procedimiento previsto en los artículos 137 a 140 del RLOPD. A este respecto hay que tener en cuenta que se considera que los contratos que se celebren de acuerdo con *"Las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países",* adoptadas por la Comisión Europea en su Decisión 2010/87/UE, ofrecen garantías adecuadas con respecto a la protección de datos de carácter personal. Otra alternativa es que el proveedor

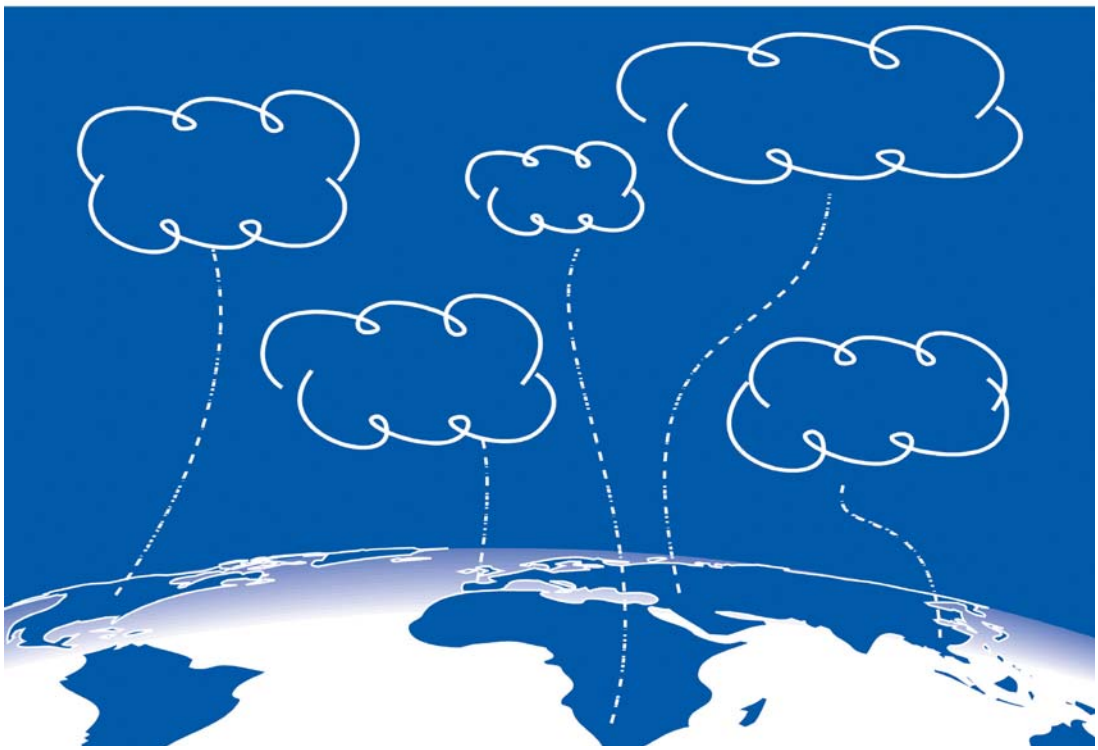
[4] La relación de entidades adheridas al sistema de "puerto seguro" está disponible en https://safeharbor.export.gov/list.aspx.

3 de *Cloud* haya obtenido una autorización previa del Director de la AEPD para realizar transferencias internacionales de datos a subencargados establecidos en terceros países basada en cláusulas contractuales en las que el despacho autorice los servicios susceptibles de subcontratación (p. ej "hosting"…) y pueda conocer en cualquier momento la identidad de las empresas subcontratadas y, si se encuentran en países que no ofrezcan garantías adecuadas, en qué países operan.

La AEPD ha elaborado unas cláusulas contractuales cuya aplicación parte de la existencia de un contrato marco entre el responsable del fichero y el encargado del tratamiento donde conste expresamente la autorización para la subcontratación por parte del encargado del tratamiento de conformidad con lo establecido en el artículo 21 RLOPD.

En dicho supuesto el responsable del tratamiento –despacho de abogados- puede contratar con el proveedor de *Cloud* que, con arreglo a dichas cláusulas, tenga autorizada la transferencia internacional de datos.

Debe recordarse que en cualquiera de los anteriores supuestos será necesario que las relaciones entre el Despacho, o responsable del fichero, y el proveedor de los servicios de *Cloud Computing*, como encargado del tratamiento, estén reguladas por contrato con los requisitos establecidos en el artículo 12 LOPD, al que se podrán incorporar las cláusulas que garanticen la protección de los interesados antes señaladas.



4 La seguridad y confidencialidad de los datos: el secreto profesional

Uno de los principios esenciales de la protección de datos es el de seguridad y un derecho irrenunciable de la profesión de abogado es el secreto profesional, la responsabilidad ética y jurídica de salvaguardar la información de los clientes. Este derecho-deber impone a los despachos de Abogados una diligencia cualificada sobre la observancia por el proveedor de servicios de todas las garantías legales relativas a los requerimientos de seguridad exigidos en relación con los datos, documentos y actuaciones amparadas por el secreto profesional.

El artículo 9.1de la LOPD dispone que "El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural". El artículo 12.2 dispone que en el contrato entre responsable y encargado se estipularán las medidas de seguridad que deberá implementar el encargado.

En materia de seguridad y confidencialidad, y desde un punto de vista técnico, los aspectos esenciales a tener en cuenta durante la selección del proveedor de servicios *Cloud* son los siguientes:

- Como cuestión previa, tanto el responsable que contrata como cliente estos servicios como el propio prestador de servicios han de actuar diligentemente solicitando y ofreciendo una información detallada sobre las medidas que vayan a garantizar la seguridad y confidencialidad de la información. A tal efecto deberán intercambiar información sobre la naturaleza de los datos para establecer un nivel de seguridad apropiado.

- El proveedor de servicios *Cloud* ha de garantizar la conservación de los datos, mediante la realización de copias de seguridad periódicas y dotando a su infraestructura de los mayores niveles de seguridad física y lógica.

- El proveedor ha de establecer mecanismos seguros de autenticación para el acceso a la información por parte de los abogados del despacho así como por parte de los clientes, en los términos que el despacho determine. Estos mecanismos han de permitir la compartición e intercambio de información sin que por supuesto sea posible que personas no autorizadas accedan a información reservada o confidencial de otros clientes o de otros abogados.

- El cifrado de los datos almacenados es una necesaria medida de seguridad. El proveedor ha de dar a conocer al despacho el nivel de seguridad ofrecido por las técnicas de cifrado de la información que aplique en sus sistemas.

4

- Asimismo, es fundamental acordar el procedimiento de recuperación y migración de los datos a la terminación de la relación entre el despacho y el proveedor; así como el mecanismo de borrado de los datos por parte del proveedor una vez que estos han sido transferidos al despacho o al nuevo proveedor designado por éste.

- Habida cuenta de que en numerosos casos los ficheros contendrán datos especialmente protegidos es necesario que el encargado del tratamiento establezca un registro de los accesos realizados a los datos.

- En el caso de que no sea posible verificar directamente las medidas de seguridad del prestador de servicios, deben contemplarse garantías alternativas que cumplan el mismo objetivo, tales como la intervención de un tercero independiente de acreditado prestigio que audite las medidas de seguridad implantadas.

- Que, en todo caso, si se producen incidencias de seguridad que afecten a los datos personales de los que es responsable el cliente del servicio de *Cloud Computing*, sean puestos en su conocimiento por el prestador del servicio junto con las medidas adoptadas para corregir los daños producidos y evitar que se reproduzcan dichos incidentes.

Para tomar una decisión informada sobre la oferta de cada proveedor en materia de seguridad y confidencialidad de la información, es del mayor interés que el despacho o bien quien le asesore en la selección de los servicios *Cloud*[5] tenga acceso a la política de seguridad del proveedor así como a las normas internacionales y certificaciones en materia de seguridad informática con las que cuenta la infraestructura del proveedor.

Lógicamente todos estos aspectos técnicos deben de trasladarse a un contrato de servicios entre el despacho de abogados y su proveedor que recoja las garantías jurídicas necesarias en caso de incumplimiento por parte del proveedor, con la finalidad última de que el despacho no sufra perjuicio alguno. Las medidas adoptadas deberán ajustarse a las previsiones contenidas en los artículos 79 y ss. del RLOPD, teniendo en cuenta que no todos los datos de carácter personal gozan del mismo nivel de protección. El art. 7 LOPD establece la existencia de datos especialmente protegidos, entre los que se encuentran por ejemplo los relativos a salud, orien-

[5] Entre las certificaciones de seguridad más conocidas aplicables a este tipo de infraestructura, pueden citarse las siguientes:
ISO 27001, de la International Standards Organization, específicamente orientada a los Sistemas de Gestión de la Seguridad de la Información.
SAS 70 (Statement on Auditing Standards, nº 70), del American Institute of Certified Public Accountants (AICPA).
Systrust y Webtrust, igualmente del American Institute of Certified Public Accountants (AICPA).
Certificación según el Federal Information Security Management Act (FISMA): NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems".

4

tación sexual, ideología o religión, para los cuales las medidas de protección que debe adoptar el encargado del tratamiento del fichero son especialmente rigurosas. Así, los art. 79 y siguientes del RD 1720/2007, por el que se aprueba el Reglamento de la LOPD, establecen tres niveles de seguridad (básico, medio y alto) que se asocian a tres categorías de datos en función del nivel de protección de los mismos. Es obligación del encargado del tratamiento articular las medidas necesarias para dotar a los datos del nivel de seguridad correspondiente; y corresponde al responsable del fichero, en este caso el despacho de abogados, exigir a su proveedor de servicios *Cloud* que articule dichas medidas. Los art. 89 y siguientes del RD 1720/2007 desarrollan cuáles son las medidas exigibles al encargado del tratamiento para cada nivel de seguridad de los datos.

Es imprescindible tener en cuenta que los despachos de abogados llevan a cabo tratamientos de datos que con cierta frecuencia requieren la adopción de medidas de nivel medio o alto (los despachos, en efecto, suelen tratar datos de los que se enumeran en los apartados 2 y 3 del artículo 81 del RLOPD).

Con el fin de poder acreditar que los procedimientos y medidas de seguridad aplicados a los tratamientos cumplen con los distintos estándares y normas legales, el usuario de servicios de *Cloud Computing* deberá de tener acceso a un conjunto de documentos que especifiquen, como mínimo, los siguientes aspectos[6]:

- Ámbito de *aplicación del conjunto documentos con especificación detallada de los recursos protegidos.*

- *Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en la normativa aplicable de protección de datos de carácter personal.*

- *Procedimientos establecidos para comunicar los resultados de las auditorías exigidas por los estándares y normas aplicados a los ficheros tratados.*

- *Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.*

- *Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan, en el caso de que los sistemas o estructuras sean proporcionados por el encargado del tratamiento.*

[6] Conforme a lo establecido en el Art 88.3 del Reglamento.

4

- *Procedimiento de notificación, gestión y respuesta ante las incidencias.*
- *Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.*
- *Las medidas de seguridad que se adoptan en el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.*
- *Departamento o persona responsable de la aplicación de los procedimientos y medidas de seguridad.*
- *Procedimiento establecido para acceder al registro de los accesos a los datos cuando sean exigibles medidas de seguridad de nivel alto.*

5 Aspectos esenciales del contrato de servicios que debe firmarse, tanto desde el punto de vista técnico como jurídico

La LOPD establece en su art. 12.2 que *"La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".* Por tanto, el contrato de prestación de servicios entre el despacho y su proveedor de servicios *Cloud* ha de incorporar las previsiones necesarias para garantizar el adecuado cumplimiento de la normativa relativa a la protección de datos. En este sentido, el encargado está obligado a seguir las instrucciones del responsable del fichero en el tratamiento de los datos.

Una forma de que el cliente indique estas instrucciones puede ser la de adoptar decisiones sobre el tipo de nube con la que se le prestarán los servicios y sobre las modalidades de servicios que contrata.

Para ello, deberá haber solicitado y obtenido previamente información suficiente sobre ambos aspectos.

De modo que la extralimitación por parte del proveedor de *Cloud* en su calidad de encargado del tratamiento tendrá las consecuencias previstas en el art. 12.4 LOPD, en virtud de las cuales el encargado del tratamiento pasa a asumir la condición de responsable del fichero.

Es importante destacar que el responsable del tratamiento, en nuestro caso el despacho de abogados, es responsable de seleccionar como encargado del tratamiento a alguien que cumpla los requisitos legalmente establecidos. Así, el artículo 20.2 RLOPD establece que "Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento". Esta responsabilidad se extiende a la subcontratación de servicios. Así, cuando el encargado del tratamiento subcontrate alguna actividad propia del tratamiento de los ficheros, dicha subcontratación habrá de recogerse en el contrato de prestación de servicios entre el responsable y el encargado, siendo necesaria una autorización del primero en los casos de subcontratación sobrevenida no prevista en el contrato (art. 21 RLOPD).

Una fórmula que puede utilizarse a tal efecto es que el cliente autorice los servicios susceptibles de subcontratación (p.ej. servicios de "hosting") y tenga permanentemente a su disposición

5

una relación actualizada de las entidades subcontratadas y de los países donde operan, (por ejemplo en una página web a la que tenga acceso o a través de otras alternativas que le permitan estar informado).

Por otra parte, existen otros aspectos relevantes que van más allá de normativa de protección de datos de carácter personal y que conviene traer a colación. Son temas que encontrarán su mejor acomodo y resolución en el propio contrato de prestación de servicios entre el proveedor y el cliente, el despacho de abogados en nuestro caso. Por la novedad de este tipo de contratos, resulta conveniente tratarlos a continuación.

En definitiva, para garantizar la seguridad jurídica del servicio *Cloud* contratado, el contrato de prestación de servicios suscrito entre el despacho y el proveedor ha de recoger, un conjunto mínimo de cláusulas, entre las que cabe destacar las siguientes:

- Régimen de los datos. Es esencial que el contrato especifique que el proveedor no puede disponer de los datos personales ni hacer uso de los mismos para ningún fin que no esté expresamente autorizado por el abogado o despacho (y cuente, en su caso, con el consentimiento del titular).

- Cumplimiento de legislación de protección de datos de carácter personal. El proveedor ha de asumir expresamente el papel de encargado del tratamiento de los ficheros de datos de carácter personal que el despacho decida trasladar "a la nube", con todas las obligaciones propias de tal figura tal y como se recogen en la legislación española y europea. Además si el proveedor almacena la información de carácter personal en sistemas ubicados fuera de la Unión Europea, ha de asumir las obligaciones que al encargado del tratamiento de los ficheros de datos de carácter personal impone la legislación española, con independencia de la jurisdicción aplicable al territorio en el que se localizan los centros de proceso de datos. En particular, si la localización no se encuentra entre las aceptadas por la AEPD, es preciso recabar autorización de la misma, y es aconsejable incluir en el contrato de servicios las cláusulas tipo propuestas por la Unión Europea.

- Seguridad en el acceso. El proveedor ha de garantizar que la información solo será accesible al despacho de abogados que contrata sus servicios, y a quienes el despacho determine con los perfiles de acceso correspondientes. En caso de que el abogado o despacho trate datos especialmente protegidos, se incluirán cláusulas que garanticen su tratamiento con las medidas de seguridad que sean exigibles.

- Integridad y conservación. El proveedor ha de disponer de los mecanismos de recuperación ante desastres, continuidad en el servicio y copia de seguridad necesarios para garantizar la integridad y conservación de la información.

5

- Disponibilidad.[7] El proveedor ha de garantizar una elevada disponibilidad del servicio, así como comprometerse a organizar las paradas programadas para mantenimiento con la suficiente antelación y dando aviso de las mismas al despacho.

- Portabilidad. El proveedor ha de obligarse, a la terminación del servicio, a entregar toda la información al despacho en el formato que se acuerde, para que éste pueda almacenarla en sus propios sistemas o bien trasladarla a los de un nuevo proveedor, en el plazo más breve posible y con total garantía de la integridad de la información.

- Consecuencias para el caso de incumplimiento del proveedor de servicios *Cloud* de las obligaciones anteriormente recogidas

- El cumplimento diligente de las garantías para la protección de datos personales que se han expuesto permitirá excluir la responsabilidad del cliente que contrate los servicios de *Cloud Computing*.

Un modelo *Cloud* es plenamente factible para un despacho de abogados, y muy aconsejable desde un punto de vista operativo y financiero. Sin embargo, es necesario que el contrato de prestación de servicios suscrito con el proveedor contemple los aspectos esenciales que se han expuesto en este documento, para garantizar que el servicio se recibe con todas las garantías técnicas y legales y con pleno respeto al derecho a la protección de datos de carácter personal.

[7] Las paradas programadas son interrupciones del servicio que los responsables de los sistemas planifican para realizar algún tipo de cambio o actualización de los sistemas (tanto software como hardware) de forma que afecten lo menos posible a la disponibilidad de éstos. El hecho de que sean programadas no implica, en principio, que tengan una duración idéntica o limitada por lo que es relevante conocer la duración máxima de éstas y el plazo de preaviso mínimo con el fin de poder recuperar la información de la nube de forma que, en caso de ser necesaria, esté disponible durante la parada en un soporte fuera de la nube.

Las paradas no programadas, por el contrario, se deben a incidentes no previstos y, por su propia naturaleza, no es posible determinar el momento de inicio o la duración de las mismas.

La disponibilidad real de los datos será la que se obtenga de restar a un plazo determinado los periodos de inaccesibilidad de los datos por ambos tipos de paradas.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CONSEJO GENERAL
DE LA ABOGACÍA
ESPAÑOLA

Para consultas y más información:

Consejo General de la Abogacía Española

www.cgae.es

Agencia Española de Protección de Datos

www.agpd.es

cloudcomputing@redabogacia.org

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA