IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «VI Congreso Internet, Derecho y Política. *Cloud Computing*: El Derecho y la Política suben a la Nube»

ARTÍCULO

Cloud computing y protección de datos

Ramón Miralles

Fecha de presentación: octubre de 2010
Fecha de aceptación: octubre de 2010
Fecha de publicación: diciembre 2010

Resumen

El *cloud computing* es una arquitectura de prestación y/o aprovisionamiento de servicios de tecnologías de la información y la comunicación, que está tomando mucho protagonismo, y que, según los analistas, en los próximos años se consolidará tanto por lo que respecta a los usuarios individuales de la red y servicios en línea, como en las empresas, que afectará a su manera de utilizar las TIC.

Con relación a los usuarios de la red el *cloud computing* tiene muchos puntos de conexión con la Web 2.0 y para las empresas está estrechamente relacionado con los procesos de *outsourcing* de los servicios TIC.

En este artículo se identifican y analizan las cuestiones más relevantes del binomio *cloud computing* y protección de datos de carácter personal.

Palabras clave

cloud computing; protección de datos, libertades, privacidad, informática en nube, encargado tratamiento, transferencias internacionales

Tema

Derecho fundamental, protección de datos, sociedad de la información

Cloud computing and data protection

Abstract

Cloud computing is an architecture for carrying out and/or providing services for information and communication technologies which is playing an increasingly prominent role. According to analysts, among companies and individual users of the Internet and online services, its application will be consolidated over the next few years.

In relation to Internet users, cloud computing has many connections with the web 2.0, and for companies it is closely linked to outsourcing of ICT services.

This article identifies and analyses the major questions regarding binomial cloud computing and private data protection.

Keywords
cloud computing, data protection, freedom, privacy, data processing requests, international transferences

Topic
Basic rights, Data protection, Information society

El *cloud computing* es una arquitectura de prestación y/o aprovisionamiento de servicios de tecnologías de la información y la comunicación que, en los últimos dos años, está adquiriendo bastante protagonismo. Según los analistas, en los próximos años se consolidará tanto entre los usuarios particulares de la red y servicios en línea, como entre las empresas; en ambos casos afectará a su manera de utilizar las TIC.

Respecto a los usuarios de la Red, la informática de nube tiene muchos puntos de conexión con la web 2.0 y, en el caso de las empresas, está estrechamente relacionada con los procesos de externalización de los servicios TIC.

Mi primer contacto profesional con el concepto *cloud computing* fue mediante un documento de mayo del 2008, concretamente un *white paper* de la oficina del Comisariado de Información y Privacidad de Ontario (Canadá), cuyo título es «Privacy in the clouds».[1]

El documento en sí mismo no aporta, en estos momentos, una reflexión relevante en cuanto a la protección de datos personales y el *cloud computing*, dado que tiene un carácter muy introductorio y se dedica fundamentalmente a la identidad digital en Internet. Por lo tanto, no aborda en profundidad ni de manera amplia la privacidad en relación con el *cloud computing*, pero a mí me sirvió para tomar contacto con este nuevo concepto.

Existe otro documento, también del IPC de Ontario, que sí aborda con más detalle la cuestión de la privacidad y el *cloud computing*. Lleva por título *Modeling Cloud Computing Architecture Without Compromising Privacy*: *A Privacy by Design Approach* y se publicó en mayo del 2010; ambos se pueden descargar en la página web del IPC.

El primero de los documentos a los que he hecho referencia sí que pone énfasis, en su introducción, al hecho de que la autodeterminación informativa es un concepto que ha ser promovido y protegido en un contexto en el que importantes cantidades de información de carácter personal (el documento habla de cantidades «ilimitadas») pasan de los individuos a las organizaciones, y de éstas a otras organizaciones. Y yo añadiría que este rasgo ilimitado no hace referencia exclusivamente a la cantidad de información, sino al tipo y a los formatos de la información.

Después volveré a referirme a la autodeterminación informativa, que como veremos está especialmente afectada por las características de procesamiento de la información del *cloud computing*.

Ahora querría continuar, en clave introductoria, con una breve referencia al origen del *cloud computing*. Desde la óptica de las telecomunicaciones, se entiende por *cloud* o nube el conjunto de dispositivos e infraestructuras de comunicaciones por los que, de manera «impredecible», pasa la información cuando se quiere transmitir de un punto a otro de Internet. Esta falta de predicción afecta tanto al número como al tipo de dispositivos; de hecho, todos los elementos que se encuentran en medio de este intercambio de informaciones se han representado, tradicionalmente, como una nube.

1. La comisaria de Información y Privacidad de Ontario (IPC, Information and Privacy Commissioner, http://www.ipc.on.ca) es Ann Cavoukian, quien ha ocupado diferentes cargos en este comisariado desde el año 1987; a lo largo de su carrera profesional, ha destacado por prestar una atención especial a los aspectos tanto tecnológicos como organizativos de la protección de datos, al considerar que la tecnología tiene un papel clave en la protección de la privacidad. Por ello, ha promovido y ha participado en un buen número de publicaciones en las que se tratan cuestiones tecnológicas relacionadas con la privacidad y la protección de datos. Por ejemplo, es bastante conocida por haber trabajado conceptos como los de *privacy by design* y *privacy enhancement technologies* (PET).

El origen de la comunicación es conocido (un usuario o proceso inicia una transacción) y el de destino también (un servidor da respuesta a la transacción), y así sucesivamente. Pero el camino que seguirá la información transportada entre los dos puntos responde a unas reglas que, si bien están fijadas por un protocolo técnico (TCP), tienen resultados impredecibles a priori; de este modo, en la práctica podemos intuir por dónde pasará la información, pero sin estar del todo seguros.

Hay que añadir otro elemento, que es que a pesar de que en esencia estos dispositivos se dedican a gestionar el tránsito de la información entre origen y destino, no se nos puede escapar que durante este tránsito la información se puede someter a tratamientos que vayan más allá de facilitar la transmisión de paquetes de información.

Quiero recordar que existe un debate abierto respecto al uso de tecnologías de inspección de paquetes (*deep packet inspection*, DPI). Es decir, la capacidad que tienen algunos equipamientos de red, que no son punto final de comunicaciones, de tratar las cabeceras de los paquetes que debe retransmitir por la Red y, convenientemente configurado, de analizar su contenido.

De hecho, la circunstancia de que los datos personales se puedan tratar exclusivamente a efectos de tránsito por la Red está prevista en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales (LOPD). En cuanto a la determinación del ámbito territorial de aplicación, el art. 2.1.a prevé que la LOPD es aplicable cuando el responsable del tratamiento, a pesar de no estar establecido en el territorio de la Unión Europea, utilice medios situados en el territorio español, excepto si estos medios se utilizan únicamente con el fin de tránsito.

Ahora bien, en el momento en el que la nube deja de ser exclusivamente un medio de transporte de la información, para pasar a tener capacidad de procesamiento de la información, se le añade el *computing*; a pesar de que en realidad la capacidad de procesamiento no recae exactamente en la nube, sino en aplicaciones, plataformas e infraestructuras disponibles en la Red y de que, en algunos aspectos, se comportan como los dispositivos de la nube a la que he hecho referencia.

El *cloud computing* implica que en el procesamiento de información concurre una serie de características cuya consecuencia directa es que el origen, y especialmente el destino, de una transacción deja de tener unos valores absolutos para pasar a tener otros relativos: la información no siempre se halla donde realmente parece y no siempre es tratada donde parece que se está procesando.

La definición de *cloud computing* que generalmente sirve de base para dotar de contenido a este concepto es la del NIST[www1] (Instituto Nacional de Estándares y Tecnologías, una agencia del US Department of Commerce, creada en 1901). La última versión de esta definición de *cloud computing* elaborada por el NIST es de julio del 2009.

Según esta definición, hay 5 características que definen el *cloud computing*:

- Autoservicio: el usuario puede utilizar más capacidades de procesamiento o almacenamiento de la información, sin pedirlo expresamente al proveedor del servicio.
- Amplio acceso a la Red: se puede acceder a ésta desde diferentes dispositivos y redes.
- Agrupación y reserva de recursos: hay un conjunto de recursos compartidos por los usuarios, de acuerdo con sus necesidades puntuales, que implica que en cada momento los recursos reservados puedan ser diferentes.
- Rapidez y elasticidad: se puede acceder a los nuevos recursos de manera inmediata y aparentemente ilimitada.
- Servicio medible y supervisado: se controla el uso y en todo momento se puede conocer, de manera transparente, el nivel de recursos utilizado.

Esta capacidad de proceso en la nube está conectada con la tendencia de externalización de los servicios TIC de las organizaciones y la reconversión de estos servicios al denominado *utility computing*.

Respecto a esta cuestión, recomiendo la lectura del artículo de Nicholas Carr[2] publicado en la *MIT Sloan Manage-*

2. Nicholas Carr es autor del *best seller* del 2008 del *Wall Street Journal, El gran cambio: cableando el mundo, desde Edison a Google*, considerado uno de los libros más influyentes en el *cloud computing*. (http://www.nicholasgcarr.com/info.shtml)

[www1] http://www.nist.gov

ment Review (Massachusetts Institute of Technology), de abril del 2005, que con el título «The End of Corporate Computing»[www2] describe los motivos que deben llevar a las organizaciones a dejar de considerar las TIC como un activo de su propiedad, para pasar a tratarlas como un servicio que compran.

En su artículo, Carr hace un paralelismo entre el proceso de transformación del uso de las TIC que deben seguir las organizaciones para ser competitivas con la transformación que se produjo a principios del siglo XX, cuando las empresas industriales empezaron a cerrar y a desmantelar las fuentes de energía utilizadas por sus industrias y que eran de su propiedad (molinos de agua, máquinas de vapor, generadores eléctricos, etc.).

Aproximadamente a partir de 1880, la producción comercial de electricidad empezó a ser posible; en 1902, en Estados Unidos había unas 50.000 plantas de generación privada de energía y sólo 3.600 estaciones podían vender energía a otras, con muchas limitaciones e inicialmente con un precio alto. Pero entre 1907 y 1920 la cuota de producción de energía eléctrica para ser comercializada pasó del 40 al 70%, y en 1930 ya alcanzaba el 80%.

Los motivos de esta rápida adopción de un nuevo modelo de suministro de energía para las industrias eran sencillos: unos costes menores y una complejidad de gestión menor, que permitía que las industrias se pudieran centrar en su negocio.

Para Nicholas Carr, en su artículo del 2005, existen tres avances tecnológicos clave en la transformación de las TIC: la virtualización, el *grid computing* y los servicios web, que, combinados con el aumento de capacidad de las redes de comunicaciones y la fibra óptica, dan como resultado un escenario idóneo para llevar a cabo esta transformación, de modo que el mayor obstáculo no será la tecnología, sino la actitud de las organizaciones a la hora de asumir este nuevo modelo de uso de las TIC en sus negocios.

Lo cierto es que el *cloud computing* ya es una realidad para los usuarios de la Red, a título individual. Los principales casos de uso del *cloud computing* implican compañías y servicios como Facebook, Amazon, Nasdaq o Google. En un informe del Pew Research Center,[3] de septiembre del 2008, se señalaba, con relación al uso del *cloud computing*, que el 69% de los usuarios de Internet de Estados Unidos almacena datos o utiliza aplicaciones basadas en servicios de *cloud computing*.

La explosión real del *cloud computing* vendrá provocada por este modelo de uso de las TIC por parte de las empresas.[4] Tal y como el propio NIST incluye en su definición, el *cloud computing* es un paradigma que todavía está en evolución.

Llegados a este punto, ya podemos empezar a hablar de algunos elementos clave a la hora de hablar de *cloud computing* y la protección de datos: la obtención de servicios TIC prestados por terceros, especializados en el procesamiento de información, y lo que en el contexto de la protección de datos conocemos como el encargado del tratamiento.

También podemos avanzar un segundo elemento de relevancia, que –aunque no siempre estará presente– si es consecuente con el paradigma del *cloud computing* y lo que éste implica como ahorro de costes, tendrá mucho peso. Este segundo elemento será la prestación de estos servicios por parte de empresas globales, ubicadas en aquellos lugares del mundo en los que la instalación de centros de proceso de datos orientados al *cloud computing* resulte más rentable. A menudo, esto implicará la aplicación de la figura del movimiento internacional de datos personales, también prevista en la normativa en materia de protección de datos de carácter personal.

Más adelante volveré a analizar con algo más de detalle estas dos cuestiones, pero ahora querría añadir algunos otros comentarios de carácter general.

3. http://pewresearch.org/. Un reciente informe de este centro de investigación (junio del 2010) recoge la opinión de los expertos de que en el 2020 la mayoría de los usuarios de Internet utilizará aplicaciones basadas en *cloud computing*, en lugar de las aplicaciones de escritorio (http://pewinternet.org/reports/2010/the-future-of-cloud-computing.aspx).
4. En este sentido, resulta de especial interés la tarea de Salesforce, con relación al uso empresarial del *cloud computing*. Ver http://www.salesforce.com/es/cloudcomputing/ y http://www.youtube.com/watch?v=VOn6tg3e1t4

[www2] http://sloanreview.mit.edu/the-magazine/articles/2005/spring/46313/the-end-of-corporate-computing/.

A pesar de que tanto la Directiva 95/46/CE, relativa a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos, como la Ley Orgánica de Protección de Datos prevén estas dos circunstancias (encargadas del tratamiento y movimiento internacional de datos), su planteamiento con relación al tratamiento de la información es «preInternet»; es decir, un escenario de bases de datos centralizadas, tanto física como lógicamente (hardware y software), y situadas en centros corporativos de procesamiento de datos instalados en los locales de la organización responsable del tratamiento.

De hecho, las propias autoridades de control europeas reconocen que, a pesar de que las previsiones de la Directiva 95/46/CE se hicieron de una manera tecnológicamente neutra, y que parece que desde el año 1995 han ido resistiendo la continua evolución de las tecnologías y las redes, hay complejidades aportadas por esta evolución que generan cierta incertidumbre en cuanto a la asignación de responsabilidades en el tratamiento de los datos de carácter personal y en cuanto al alcance de las legislaciones nacionales aplicables.

No debemos olvidar que en el contexto de la protección de datos personales resulta esencial la identificación del responsable del tratamiento, dado que esto garantiza que hay una persona que tiene asignadas una serie de obligaciones concretas derivadas del tratamiento y, por lo tanto, hay alguien a quien se le puede exigir el cumplimiento de estas obligaciones.

Muchos de los servicios en línea que han emergido como consecuencia del uso intensivo y masivo de la Red en los últimos años han llevado al límite la legislación europea en materia de protección de datos; en algún caso, incluso ha resultado insuficiente para dar respuesta a las nuevas situaciones que surgen en Internet. De aquí que el grupo de autoridades de control que crea el art. 29 de la Directiva (conocido como grupo del art. 29) haya tenido que ir analizando y dictaminando sobre determinadas cuestiones.[5] De hecho, en el programa de trabajo 2010-2011 del grupo del art. 29 se incluye explícitamente analizar el *cloud computing* con relación a la protección de datos de carácter personal.

En el ámbito internacional, y por lo tanto más allá del contexto europeo, las autoridades de control de privacidad y protección de datos también han mostrado su preocupación por estas cuestiones. Resulta de especial relevancia la propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad, respecto al tratamiento de datos de carácter personal, acogida por la 31.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (5 de noviembre del 2009, Madrid). Esta propuesta es el resultado de una resolución previa de la 30.ª conferencia, que planteaba la necesidad urgente de proteger la privacidad en un mundo sin fronteras y de lograr una propuesta conjunta para el establecimiento de unos estándares internacionales sobre privacidad y protección de datos personales.

Los diferentes modelos de servicio de *cloud computing*, ya sea como servicio de software (SaaS), de plataforma (PaaS) o de infraestructura (IaaS), impactan directamente sobre una cuestión clave en la definición del derecho a la protección de datos de carácter fundamental: la autodeterminación informativa.

A pesar de que en función del modelo de despliegue del *cloud* el impacto es mayor o menor: nube pública, privada, híbrida (dos o más nubes diferentes) o comunitario.

Esta autodeterminación informativa, tal y como la definieron las sentencias 290/2000 y 292/2000 del Tribunal Constitucional, de 30 de noviembre del 2000, implica:

5. El «Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos en el tratamiento de los datos personales en Internet para lugares web ubicados fuera de la Unión Europea», aprobado el 30 de mayo del 2002; el «Dictamen 1/2008, sobre cuestiones de protección de datos relacionados con los motores de búsqueda»; el más reciente «Dictamen 5/2009, sobre las redes sociales en línea»; o el de principios de este año, «Dictamen 1/2010, sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento"», son algunos ejemplos relevantes. En este último documento se hace una referencia directa al *cloud computing* y a las dificultades que puede implicar para esta asignación de responsabilidades en materia de protección de datos. En http://ec.europa.eu/justice_hombre/fsj/privacy/workinggroup/wpdocs/ se pueden encontrar todos los documentos aprobados por el grupo del art. 29.

- En primer lugar, que «el derecho a la autodeterminación informativa es un derecho activo de control sobre el conjunto de informaciones relativas a una persona».
- En segundo lugar, que «el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre» sus datos personales.
- Y en tercer lugar, que este poder de disposición sobre los propios datos personales no vale nada si el afectado desconoce qué datos de él tienen en su poder terceros, quién son estos terceros y con qué finalidad tienen sus datos.

Y éste es uno de los primeros inconvenientes detectados con relación al *cloud computing*: la pérdida efectiva de control sobre los datos, dado que más allá de los vínculos contractuales o de suscripción con las empresas que prestan estos servicios desaparece o «se nubla» el vínculo o la certeza sobre la ubicación física de la información y las condiciones de procesamiento y, en consecuencia, pueden quedar afectadas las garantías de confidencialidad y de seguridad de la información situada en el *cloud*.

Además, ésta no es una preocupación expresada únicamente por las autoridades de control; tal y como recoge un documento del NIST, de julio del 2009, «Effectively and Securely Using the Cloud Computing Paradigm» («Uso eficaz y seguro del *cloud computing*»), uno de los retos del *cloud computing* es la seguridad, a pesar de que el propio documento valora que «cloud security is a tractable problem».

En la misma línea, un estudio más reciente, de junio de este año, también de IDC, pero mucho más cercano porque se realizó con grandes empresas y organizaciones en Cataluña, evidencia que uno de los inhibidores de las empresas para dar el salto a la nube es la preocupación por la falta de confidencialidad de los datos (con una puntuación de 4,4 sobre 5, y a mucha distancia del resto de inhibidores).

Por último, un documento de la Cloud Security Alliance[6] (CSA), «Top Threats to Cloud Computing v1.0», de marzo del 2010, identifica las 7 principales amenazas que pueden afectar el despliegue del *cloud computing*, entre las que incluye la pérdida o fuga de datos (*data loss or leakage*).

Que la seguridad en el *cloud computing* es una cuestión de la que hay que ocuparse lo evidencian los recientes estudios, más o menos detallados, sobre ésta de distintas organizaciones. Aparte de algunos ya mencionados, podemos destacar los siguientes:

- «Privacy in the clouds: Risks to Privacy and Confidentiality from cloud computing», del World Privacy Forum[www3] (febrero del 2009)
- «Cloud computing. Information Assurance Framework» y «Cloud computing. Benefits, risks and recommendations for information security», de ENISA[www4] (ambos de noviembre del 2009)
- «Guía para la seguridad en áreas críticas de atención en *cloud computing*», de la CSA[www5] (también de noviembre del 2009)
- «Modeling cloud computing architecture without compromising privacy: a privacy by design approach», del Information and Privacy Commissioner de Ontario[www6] (mayo del 2010).

Antes de concluir esta parte introductoria, me gustaría evidenciar otros riesgos, derivados también de esta pérdida de control, que tienen que ver con el uso de los datos personales con fines de seguridad pública, dado que sin duda el *cloud computing* también puede convertirse en una oportunidad para que los cuerpos y fuerzas de seguridad puedan ejercer un mayor control sobre la población, y proteger así a la ciudadanía de actos violentos vinculados a la seguridad pública y a la seguridad de los estados.

Recomiendo consultar la web «Statewatch»[www7] (observatorio de la actividad de los estados y de las libertades

6. La Cloud Security Alliance tiene por finalidad promover el uso de las mejores prácticas en seguridad en el contexto del *cloud computing*, organización de la que, por cierto, recientemente se ha creado el capítulo español, uno de los primeros a nivel mundial. Se puede consultar en http://www.cloudsecurityalliance.org/.

[www3]http://www.worldprivacyforum.org
[www4] http://www.enisa.europa.eu
[www5] http://www.cloudsecurityalliance.org/
[www6] http://www.ipc.on.ca
[www7] http://www.statewatch.org

civiles en Europa) y la lectura del documento del Consejo de la Unión Europea, de abril del 2010, sobre el uso de un «instrumento estandarizado, multidimensional y semiestructurado de recogida de datos e información relacionada con los procesos de radicalización en la Unión Europea» (ENFOPOL 99), cuyo objeto es «evitar que las personas se conviertan en terroristas, abordando factores y causas profundas que puedan conducir a la radicalización y el reclutamiento tanto dentro como fuera de Europa».

Y es que no debemos olvidar que el derecho a la protección de datos personales tiene un carácter instrumental para el ejercicio otros derechos fundamentales y está íntimamente relacionado con las libertades públicas e individuales. Por lo tanto, se ha de tener presente que cuando hablamos de proteger los datos personales o de autodeterminación informativa estamos hablando, en definitiva, de libertad.

Respecto a los aspectos prácticos y más técnicos de la regulación en materia de protección de datos que, en relación con el *cloud computing*, hay que tener en cuenta desde una perspectiva de cumplimiento legal, ya he avanzado la primera cuestión que se debe analizar: incluso en la modalidad de despliegue privado del *cloud computing*, si la infraestructura de la nube es gestionada por un tercero, nos encontraremos con el supuesto de un «tratamiento por cuenta de terceros», es decir, con la figura de encargado de tratamiento, una situación regulada en el art. 12 de la LOPD.

Esto, sin entrar a discutir sobre las dificultades que en algunos casos se pueden dar en la determinación de quién es el responsable de un tratamiento, dado que ciertas situaciones no evidencian tanto la asignación de esta responsabilidad. En el contexto de la Directiva Europea, tiene que ver con aquella persona física o jurídica que determina las finalidades y los medios de tratamiento de los datos personales.

El dictamen 1/2010 del grupo del art. 29, al que ya he hecho referencia,[7] aborda esta cuestión con detalle y con ejemplos relacionados directamente con el *cloud computing*; en definitiva, se considera que, para la determinación del responsable del tratamiento, no sólo se hay que tener en cuenta las relaciones jurídicas, sino también las situaciones fácticas, de modo que se deben analizar las circunstancias de cada caso para asignar la responsabilidad sobre el tratamiento.

Antes de continuar con el encargado del tratamiento, hay una cuestión que querría tratar brevemente, en concreto sobre el ámbito de aplicación de la LOPD: en qué momento son de aplicación los requisitos y las condiciones del art. 12 de la LOPD, que regula la figura del encargado del tratamiento, para un tratamiento por cuenta de un tercero.

El ámbito de aplicación de la LOPD viene regulado en el art. 2, que prevé que la LOPD es de aplicación cuando:

- El tratamiento se efectúa en territorio español, en un establecimiento del responsable del tratamiento; aquí la territorialidad tiene un peso específico importante, que en el caso del *cloud computing* puede plantear serias dudas en cuanto a su verificación; como decíamos, estamos ante una óptica clásica de lo que son los centros de procesamiento de datos.
- El responsable del tratamiento no tiene un establecimiento en territorio español, pero en aplicación de las normas de derecho internacional público le es aplicable la normativa española.
- El responsable del tratamiento no está establecido en el territorio de la Unión Europea, pero utiliza medios de tratamiento situados en territorio español (con la excepción de que sólo sea con el fin de tránsito). Como resultado de la tarea interpretativa del grupo del art. 29, por ejemplo, el uso de galletas (cookies) se considera un uso de medios situados en el territorio del ordenador del usuario en el que se instalan las galletas (ver WP56, sobre la aplicación internacional de la legislación comunitaria de protección de datos).

El art. 3 del reglamento de despliegue de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD), aporta algunos elementos adicionales con relación al ámbito territorial de aplicación del reglamento, que añade tres cuestiones que conviene comentar:

7. Ver nota 5.

1) Si el responsable del tratamiento no tiene un establecimiento en territorio español, pero tiene un encargado del tratamiento ubicado en España, le es de aplicación el título VIII del reglamento, es decir, las medidas de seguridad.
2) Si el responsable del tratamiento no está establecido en el territorio de la Unión Europea, pero utiliza medios situados en territorio español, este responsable del tratamiento debe designar un representante establecido en territorio español.
3) Y por establecimiento hay que entender cualquier instalación que permita el ejercicio efectivo y real de una actividad, con independencia de la forma jurídica adoptada.

Continuando con el tratamiento por cuenta de terceros, a fin de que la figura de encargado de tratamiento entre en juego y de que, por lo tanto, se considere que no hay una comunicación de datos, debe existir necesariamente una relación jurídica que vincule al responsable y al encargado de tratamiento y que delimite, de manera precisa, cuál será su actividad con relación al tratamiento de datos personales que realiza el encargado por cuenta del responsable del tratamiento.

En situaciones en las que un tercero preste servicios de *cloud computing,* diferente por lo tanto del responsable del tratamiento, y sea de aplicación la LOPD, hay que aplicar en toda su extensión lo previsto en el capítulo III del RLOPD (arts. 20, 21 y 22).

Una de las obligaciones que establece el RLOPD en el art. 20.2 es que el responsable del tratamiento debe velar por que el encargado del tratamiento cumpla con lo que prevé el reglamento. Por lo tanto, hay que articular estos mecanismos de supervisión, que en ciertas circunstancias serán de difícil implementación, especialmente cuando el encargado del tratamiento pueda tener una posición dominante en el mercado.

Otra cuestión de interés, que regula el art. 21, es la subcontratación de servicios, que parte del principio general de que el encargado del tratamiento no puede subcontratar a un tercero ningún tratamiento que le haya sido encomendado por el responsable del tratamiento. Ahora bien, sí que lo puede hacer si obtiene autorización del responsable del tratamiento, y siempre y cuando esta subcontratación la haga en nombre y por cuenta del responsable del tratamiento.

Hay algunas condiciones que permiten exceptuar la autorización del responsable del tratamiento:

- que esté ya especificado en el contrato de servicios que regula el encargo y que se indique la empresa que se subcontratará; y si no es posible esta determinación a priori, el encargado debe comunicar al responsable qué empresa piensa subcontratar antes de proceder a su subcontratación;
- que, obviamente, el subcontratista se ajuste a las instrucciones del responsable del tratamiento, ya dadas al encargado de éste, y
- que el encargado y el subcontratista formalicen un contrato; entonces el subcontratista tendrá la consideración de encargado de tratamiento.

Una vez finalizada la prestación contractual, también será de aplicación el régimen previsto con relación a la conservación de datos por parte del encargado del tratamiento; como regla general, los datos se deben destruir o devolver al responsable, excepto que alguna previsión legal obligue al encargado del tratamiento a conservar los datos. Eso sí, los datos deben estar bloqueados, es decir, no se pueden someter a ningún tipo de tratamiento que vaya más allá de la propia conservación y de las medidas de seguridad derivadas de esta obligación de conservación.

En este punto, querría recordar que el concepto de tratamiento en el contexto de la protección de datos tiene una configuración amplia, dado que se considera tratamiento cualquier operación o procedimiento técnico que permita recoger, grabar, conservar, elaborar, modificar, consultar, utilizar, bloquear o cancelar los datos, así como las cesiones de datos que se deriven de comunicaciones, consultas, interconexiones y transferencias de datos (art. 3, letra c de la LOPD, y art. 5.1, letra t del RLOPD).

Una vez abordada la cuestión del encargado del tratamiento, ya sea porque nos presta servicios de *cloud* de aplicación (software), de plataforma o de infraestructura, la segunda cuestión de relevancia que se debe tratar está relacionada con el hecho de que se pueda llegar a producir un movimiento internacional de datos como consecuencia del uso de servicios en la «nube». Si se da este supuesto, es de aplicación lo que prevé el título V de la LOPD (art. 33 y 34) y el título VI del RLOPD (art. 65 a 70).

Como principio general, se establece que no se pueden hacer transferencias de datos personales a países que no proporcionen un nivel de protección equiparable al de la LOPD.

Esta transferencia internacional se puede realizar si, además de cumplir lo que prevé la LOPD, así lo autoriza el director de la AEPD. El procedimiento para solicitar esta autorización lo regula el RLOPD (art. 137 a 144).

No es necesaria autorización si el país en el que se establece el importador de los datos ofrece un nivel adecuado de protección; esta determinación de nivel adecuado la efectúa el director de la AEPD, mediante resolución y para un país en concreto. Tampoco es necesaria esta autorización si el nivel adecuado ha sido declarado por una decisión de la Comisión Europea; aquí también se incluye, por ejemplo, el acuerdo de puerto seguro con Estados Unidos.

Asimismo, existe toda una serie de supuestos concretos que son excepciones a la necesidad de autorización del director de la AEPD. Estas excepciones se regulan en el art. 34 de la LOPD (tratados y convenios internacionales, auxilio judicial, servicios relacionados con la salud, transferencias dinerarias, consentimiento inequívoco del afectado, necesario en relaciones contractuales, interés público, procedimiento judicial o petición desde registros públicos).

En el supuesto de que la autorización sea necesaria, hay que presentar un contrato escrito, entre importador y exportador, en el que consten las garantías de respeto necesarias para la protección de la vida privada. A estos efectos existe un conjunto de decisiones de la Comisión Europea relacionadas con los contenidos de estos tipos de contratos (art. 70.2).

Las transferencias internacionales se deben notificar para inscribirlas en el registro general de protección de datos al registrar el tratamiento que prevé la transferencia internacional. Las autorizaciones de transferencias internacionales también se inscriben, en este caso de oficio.

Para las transferencias internacionales, pueden resultar de interés los estudios realizados por algunas organizaciones sobre los diferentes niveles de exigencia en materia de protección de datos.

Así, tenemos el mapa global de la protección de datos que desde hace unos años publica Privacy International,[www8] y otro nuevo que, con una cierta orientación de marketing, ha elaborado recientemente Forrester Research,[www9] acompañado de la pregunta de si sabemos dónde están nuestros datos en la nube (*Do you know where your data is in the cloud*?).

Por último, existe un caso especial de autorización de transferencia internacional, previsto en el art. 70.4 del RLOPD, para el caso en el que se produzca en el seno de grupos multinacionales de empresas. En tal situación, es necesario que estos grupos adopten lo que se conoce como BCR (*binding corporate rules*) o normas corporativas vinculantes, en las que consten las garantías de respeto necesarias para la protección de la vida privada y el derecho fundamental a la protección de datos, así como los principios y el ejercicio de derechos previstos en la LOPD.

Estas normas o reglas deben ser vinculantes para las empresas del grupo y exigibles según el ordenamiento jurídico español, y las puede exigir tanto la AEPD como las personas afectadas.

El grupo del art. 29 también tiene publicados algunos documentos relacionados con las BCR. A efectos introductorios, resultan de interés el «Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules», el «Working Document Setting up a framework for the structure of Binding Corporate Rules» y el «Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules», todos ellos de junio del 2008.

Según datos de la AEPD, entre el año 2000 y julio del 2007 se autorizaron un total de 148 transferencias internacionales, y en el 2007 se notificaron al registro de protección de datos 8.483 movimientos internacionales de datos.

[www8] http://www.privacyinternational.org/ y el mapa en http://www.privacyinternational.org/survey/dpmap.jpg.
[www9] http://www.forrester.com/rb/research y el mapa en http://www.forrester.com/cloudprivacyheatmap.

Por último, querría añadir una cuestión esencial relacionada con la protección del derecho fundamental a la protección de datos de carácter personal, en aquellas situaciones en las que éste se pueda ver vulnerado en ambientes de *cloud computing*, en los que se pueden dar situaciones de multiterritorialidad y, por lo tanto, con dificultades para resolver de manera efectiva las posibles vulneraciones; sin duda, es un tema que deberán abordar las autoridades de control, especialmente las de la Unión Europea, en cuanto a coordinación entre autoridades, intra- y extraeuropeas.

En resumen, los aspectos más relevantes relacionados con el cumplimiento legal que hay que abordar o tener en cuenta cuando conectamos protección de datos y *cloud computing* están relacionados con:

1) La pérdida de control sobre el tratamiento de la información, tanto por parte de las personas afectadas como por parte del responsable del tratamiento, y las consecuencias que se puedan derivar de ello (seguridad, confidencialidad, ejercicio de derechos, etc.).
2) Las dificultades de encajar jurídicamente y con suficiente agilidad las situaciones de tratamiento de los datos por cuenta de terceros: el encargado del tratamiento *cloud* y las posibles subcontrataciones.
3) Las problemáticas derivadas del movimiento internacional de datos.
4) Y, por último, la resolución efectiva de los incidentes relacionados con la vulneración del derecho fundamental en la protección de datos personales en situaciones de multiterritorialidad.

Cita recomendada

MIRALLES, Ramón (2010). «*Cloud computing* y protección de datos». En: «VI Congreso Internet, Derecho y Política. *Cloud Computing*: El Derecho y la Política suben a la Nube» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 11. UOC. [Fecha de consulta: dd/mm/aa].

‹http://idp.uoc.edu/ojs/index.php/idp/article/view/n11-miralles/n11-miralles-esp›

ISSN 1699-8154

Sobre el autor

Ramón Miralles
ramon.miralles@gencat.cat

Coordinador de Auditoría y Seguridad de la Información. Autoridad Catalana de Protección de Datos.

Autoridad Catalana de Protección de Datos
C/ Llacuna, 166, 8.ª planta
08018 Barcelona, España