InDret
REVISTA PARA EL
ANÁLISIS DEL DERECHO

WWW. INDRET.COM

Computación en la nube: Big Data y protección de datos personales

Susana Navas Navarro

Catedrática de Derecho civil
Universidad Autónoma de Barcelona

BARCELONA, OCTUBRE 2015

Abstract

La cantidad y la velocidad a la que se producen los datos en el entorno digital plantean cuestiones relacionadas con su adecuado almacenamiento. Los datos masivos o Big Data son datos digitales que, en la actualidad, pueden ser guardados en la "nube". Los responsables de los datos contratan servicios de computación para su almacenamiento y, en la mayoría de casos, para su posterior tratamiento. El proveedor de estos servicios es el "encargado" del tratamiento, el cual, a su vez, puede subcontratar a terceros para que realicen determinadas operaciones en relación con aquél. Dentro de los Big Data destacan, por su especial protección, los datos personales. En este trabajo, analizamos los servicios de cloud computing, principalmente, desde la perspectiva del titular de esos datos, la persona física. Antes, de todos modos, exponemos los aspectos más técnicos del tema que nos ocupa.

The amount and speed at which data is produced in the digital environment raises issues concerning proper storage. Massive data or Big Data are digital data that, at present, can be stored in the "cloud". The controller of the data concludes a computing services contract for storage and, in most cases, further data processing. The provider of these services is the "processor" of the data processing, which, in turn, can contract third parties to carry out certain operations in connection with it. Big Data includes personal data that are subjected to special protection. In this paper, we analyze the cloud computing services, primarily from the perspective of the holder of such data, the individual. Before, however, we expose more technical aspects of the topic at hand.

Title: Cloud computing: Big Data and personal data protection

Palabras claves: computación en la nube, datos personales, transferencia internacional
Keywords: cloud computing, persona data, international transfer

Sumario

1. Del hosting al cloud computing pasando por el grid computing. Una (r)evolución informática en la sociedad de la información

En el ámbito de las telecomunicaciones se ha solido aludir a la "nube" para referirse a una forma de transmisión de la información conveniente para el usuario ya que se podía hacer de forma permanente en cualquier momento y lugar sin que la información transmitida sufriera modificación alguna. Al usuario no le preocupaba la estructura subyacente que servía de base para la transmisión de su información. Cuando nace internet la nube supone una forma de simbolizarla. En la actualidad, sin embargo, el usuario no desea sólo transmitir la información de un punto a otro, sino que quiere además su procesamiento, de suerte que la información que se envía llega a su destinatario transformada. La estructura subyacente para llevar a cabo este, así como otros, servicios es internet. La expresión "nube" indica, ahora, mucho más que la pura transmisión de la información pues se refiere al manejo de toda una serie de recursos y servicios que implican el tratamiento de la información. En definitiva, se trata de la nube como símbolo o metáfora de una nueva forma de explotar los recursos informáticos[1]. Es una forma de expresar una abstracción[2].

La computación en la nube o, en la terminología anglosajona que se suele manejar, el *cloud computing*[3], es considerada, por algunos, como una revolución informática mientras que, para otros, es el resultado normal de la evolución informática que venía aconteciendo en los últimos años[4]. De hecho, parece más lo segundo que lo primero, si bien, el éxito arrollador que está teniendo el sistema de computación en la nube más parece lo primero que lo segundo, esto es, una revolución. Quizá, desde el punto de vista informático forme parte del proceso evolutivo tecnológico. Sin embargo, desde el punto de vista de los usuarios del servicio de computación en la nube representa, en efecto, una revolución puesto que se pueden emplear recursos informáticos, que no se pueden adquirir o, si se hace, es a un elevado coste, en cualquier momento, en cualquier lugar en el que se halle (*ubicuidad*) y con un coste realmente bajo; amén de liberar el espacio físico que ocupan algunos de esos recursos informáticos (por ejemplo, las máquinas) al convertirse en virtuales[5]. Así, al usuario de los servicios de computación en la nube sólo le basta con

*La autora agradece al Sr. Iván Mateo Borge, abogado y profesor asociado de derecho civil (UAB) la lectura detenida de este escrito y a los dos evaluadores anónimos por sus sugerencias y precisiones. Los errores u omisiones que pudieran existir sólo son imputables a su autora.

[1] GARCÍA SÁNCHEZ (2012, p. 39).

[2] JAEGER *et al.*, http://pear.accc.uic.edu/ojs/index.php/fm/article/view/2456/2171. Fecha consulta: septiembre 2015.

[3] A pesar de que la voz "*cloud computing*" viene siendo, cada vez, más utilizada en la práctica, nosotros, a lo largo, de este trabajo, emplearemos preferentemente la expresión "*computación en la nube*" que es la traducción que, a la sazón, se ha realizado a nuestro idioma.

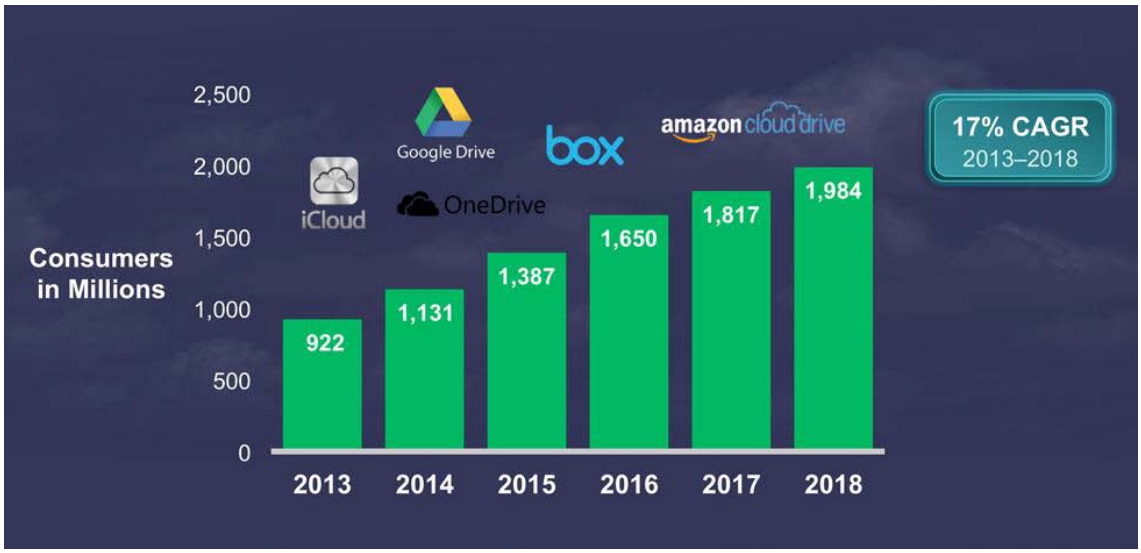
[4] SOSINSKY (2011, p. 39); MARTÍNEZ MARTÍNEZ (2012, p. 18).

[5] RODRÍGUEZ DE LAS HERAS (2010, p. 150).

poseer un equipo terminal, el que sea, para acceder a, por ejemplo, su oficina, sus documentos, su equipo informático, sus datos, etc… Este equipo terminal no tiene porqué ocupar demasiado espacio; de hecho, es suficiente con un *Smartphone* para tener acceso a todos los servicios que el proveedor ofrezca o que se contraten con él.

En el CISCO GLOBAL CLOUD INDEX 2013-2018 se advierte que hacia 2018, el 78 % de los trabajos online se harán mediante sistemas de computación en la nube. El tráfico de datos por la red de redes se triplicará de 2013 a 2018 pasando de 255 exabytes por mes en 2013 a 715 exabytes por mes en 2018. Por otro lado, si en 2015, son 1,387 millones los usuarios de servicios de computación en la nube, en 2018 se prevé un aumento pasando a 1,984 millones de usuarios. Desde 2013 hasta 2018, el aumento será del 17 % y el futuro es esperanzador para estos servicios, habida cuenta del volumen de datos que se transmiten por internet[6]. De hecho, la Comisión europea en sus trabajos sobre el mercado único digital alude a la posibilidad del uso masivo por los ciudadanos europeos de la nube en Europa y los beneficios que ello provocaría[7]; aunque no se deja de reconocer que todavía deben resolverse legalmente determinados aspectos relacionados con la protección de los datos personales que circulan -y circularán- por ella[8].

Personal Cloud Storage—Growth in Users



Source: Cisco Global Cloud Index, 2013–2018; Juniper Research

---

[6] CISCO, *Cloud Index White Paper*, 2013-2018.

[7] Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité económico y social europeo, al Comité de las regiones, *Liberar el potencial de la computación en nube en Europa*, COM(2012) 529 final. Asimismo, vid. la *Propuesta de resolución del Parlamento europeo sobre la liberación del potencial de la computación en la nube en Europa* de 24 de octubre de 2013 (www.europarl.europa.eu_sides_getDoc.pdf. Fecha de la consulta: septiembre 2015).

[8] En este sentido, véase el Dictamen del Supervisor Europeo de Protección de Datos, de 3 de septiembre de 2013, sobre la Comunicación de la Comisión citada en la nota precedente (C 253/3) que se puede consultar en www.edps.europa.eu.

Los primeros usos informáticos compartidos se centraron en el almacenamiento o alojamiento (*hosting/housing*)[9] de copias de documentos electrónicos o sitios web en servidores centrales que tenían la capacidad suficiente como para permitir que los usuarios clientes pudieran hacer uso de la misma, máxime cuando los equipos terminales poseían una capacidad limitada, de suerte que o no podían almacenar el volumen de datos que se iban generando o, aunque se almacenaran, no podían ser procesados convenientemente, salvo que se adquirieran máquinas adecuadas para ello a un elevado coste, casi inasumible para el usuario[10]. Del almacenamiento se pasa a compartir recursos en sistemas P2P, cuando varias máquinas están conectadas virtualmente entre sí y, en un proceso lógico de abstracción, se llega a la computación en malla o *grid computing* que consiste en el uso compartido, empleando internet, de diferentes ordenadores que se encuentran interconectados, aunque físicamente deslocalizados, formando, por ejemplo, un *cluster*[11]. Así, se comparten recursos heterogéneos que no se encuentran centralizados. El paso al uso compartido de la informática, de forma virtual, a la carta o bajo demanda (*cloud computing*), de forma centralizada, en los centros de datos o "granjas de servidores", iba, por ende, *de soi*; formaba parte del proceso lógico en la evolución que, de la informática, venía desarrollándose[12]. Se trata de ofrecer servicios de computación como se ofrecen servicios de electricidad, agua o gas, respecto de los cuales el usuario/consumidor paga por la cantidad que consume, nada más. Se suele aludir, en este caso, a "*utility computing*"[13] o "servicio de utilidad pública".

La computación en la nube presenta toda una serie de ventajas que permiten verla, como decíamos, como una revolución informática para el usuario[14]; pero también presenta toda una serie de inconvenientes[15]. De entre estos últimos, destaca la posible pérdida de control

[9] SÁNCHEZ LERÍA (2011, pp. 28-29), donde diferencia el *hosting* del *housing*.

[10] JAEGER *et al.* (2008, pp. 269-283).

[11] GONG *et al.* (2010, p. 276).

[12] JAEGER *et al.*, http://pear.accc.uic.edu/ojs/index.php/fm/article/view/2456/2171. Fecha consulta: septiembre 2015. La evolución en la informática hasta llegar al cloud computing puede verse en BUYYA/BROBERG/GOSCINSKI (2011, pp. 8-13).

[13] JAEGER *et al.* (2010, pp. 269-283); BUYYA/BROBERG/GOSCINSKI (2011, pp. 3-5); ROBISON (2010, p. 1195-1197).

[14] Suelen considerarse como ventajas de la computación en la nube el hecho de que implica un servicio bajo demanda, su acceso fácil a través de internet, la agrupación de recursos de los proveedores, la flexibilidad, eficiencia energética o bajo coste (GARCÍA SÁNCHEZ, 2012, p. 41; PUYOL MONTERO, 2013, pp. 22-23).

[15] Entre otros, la falta de seguridad de los datos que circulan por la red (falta de integridad, confidencialidad o disponibilidad) o las cuestiones relacionadas con la privacidad de los datos y su pérdida de control (ALAMILLO DOMINGO, 2012, pp. 63 ss; PUYOL MONTERO, 2013, pp. 32 ss; MIRALLES LÓPEZ, 2010, http://idp.uoc.edu/ojs/index.php/idp/article/view/n11-miralles/n11-miralles-esp).

respecto de datos de carácter personal para su titular[16] en la medida en que éstos pasan a circular por la "nube", en una cadena de subcontrataciones de prestadores de servicios que pueden hallarse en diferentes países, determinando una transferencia o movimiento internacional de aquéllos, cuando la contratación de servicios de computación en la nube comporte la recogida y posterior procesamiento de los datos, lo que no siempre acontecerá de este modo. La cuestión que, en este trabajo, nos planteamos es cuál sea la protección legal del titular de los datos de carácter personal, persona física, cuando éstos son tratados mediante el sistema de computación en la nube.

La computación en la nube implica un uso compartido virtual de recursos informáticos que pertenecen a una persona física o jurídica, para la cual, ese uso representa una forma de optimizarlos, es decir, de obtener un rendimiento económico pleno, de acuerdo con su destino. En definitiva, se trata de que los bienes de los que somos propietarios y que están infrautilizados, se pongan a "trabajar para nosotros", o sea, que nos generen un capital en forma de dinero. Es un nuevo modelo de negocio en el que la red de redes representa un gran ordenador[17]. De acuerdo con las previsiones del *International Data Corporation* (IDC) se esperan, para 2018, unos ingresos mundiales de aproximadamente 128 billones de dólares derivados de la explotación de servicios en la nube, lo que representa un crecimiento seis veces superior al crecimiento de todo el mercado de IT en el mundo[18].

De otra parte, no debe olvidarse que los servicios de computación en la nube son considerados "*servicios de la sociedad de la información*" al tratarse de un servicio prestado a título oneroso, vía electrónica, a distancia y a petición individual del interesado. El proveedor de los mismos es un proveedor de "*servicios de intermediación*", al facilitarse la prestación o la utilización de otros servicios de la sociedad de la información o el acceso a la información, cuya responsabilidad se regirá de acuerdo con lo establecido en los arts. 13 a 17 de la *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico*[19].

Muy críticos con las deficiencias que todavía presentan los sistemas de computación en la nube se muestran JAEGER/LIN/GRIMES (2010, pp. 269-283).

[16] El titular de los datos de carácter personal es la persona física de la cual se recogen los mismos; es el "afectado" o "interesado" al que se refiere la legislación sobre protección de datos de carácter personal (art. 3 letra e de la *Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*, BOE núm. 298, de 14 de diciembre de 1999. En adelante, LOPDCP; art. 5.1 letra a del *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*, BOE núm. 17, de 19 de enero de 2008. En adelante, RDCP).

[17] BUYYA/BROBERG/GOSCINSKI (2011, pp. 45-46).

[18] Los datos pueden consultarse en http://www.idc.com/getdoc.jsp?containerId=prUS25219014. Fecha de la consulta: septiembre de 2015.

[19] BOE núm. 166, de 12 de julio de 2002. En el anexo que contiene las definiciones se consideran "*servicios de intermediación*": la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los

2. La computación en la nube. Aspectos técnicos

Antes de entrar en las cuestiones jurídicas que puede presentar la computación en la nube, conviene detenerse en su comprensión, desde el punto de vista técnico, para así poder ser más preciso a la hora de dar soluciones legales a los posibles conflictos que se pudieran plantear. En primer lugar, por tanto, expondremos, en qué consiste (2.1.); después, referiremos los diferentes modelos que, hoy por hoy, existen (2.2.).

2.1 ¿En qué consiste?

Aunque en la introducción ya se ha apuntado en qué consiste la computación en la nube, puede precisarse todavía más. Existen más de veinte definiciones de lo que representa, si bien la más citada es la que recoge el NIST (*National Institute of Standards and Technologies*) del Departamento de comercio del gobierno federal de los Estados Unidos. Este Instituto la ha definido como "*un modelo que permite el acceso a la carta o bajo demanda a todo un conjunto de recursos informáticos como aplicaciones, infraestructura, datos u otros servicios como por ejemplo el almacenamiento de información o el procesamiento de datos recogidos con un mínimo de esfuerzo o de interacción con el proveedor del servicio*"[20].

Este modelo de nube se compone de cinco características esenciales, tres servicios principales y cuatro modelos de implementación, si bien, en la actualidad, han ido surgiendo nuevos servicios y nuevos modelos. Las características son las siguientes: autoservicio bajo demanda del cliente, accesos de banda ancha convencional sin requerimientos adicionales, los recursos se ponen a disposición simultáneamente de múltiples clientes que, aunque no saben la ubicación exacta de sus datos, sí pueden obtener información del país en el que se encuentre el centro de datos en el que los mismos se hallan ubicados, elasticidad en la provisión del servicio y mesurabilidad del mismo[21]. Aunque los usuarios no conozcan donde están ubicados sus datos, los proveedores de servicios de computación en la nube, por el contrario, si lo saben, puesto que son ellos los que centralizan la información en gigantescos centros de datos repartidos por todo el globo, también conocidos como "granjas de servidores", establecidas en grandes extensiones de terreno cercanas a puntos de acceso a electricidad e internet; si bien también se construyen en plataformas acuáticas que, en algunos casos, se instalan en aguas

---

usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet. No existe, pues, duda de que los servicios de computación en la nube son de los comprendidos en esta definición.

[20] El documento se puede consultar en www.nist.gov/itl/csd/cloud-102511.cfm. Fecha de la consulta: septiembre 2015.

[21] BUYYA/BROBERG/GOSCINSKI (2011, pp. 18-19).

internacionales[22]. Así, mientras que el usuario no puede localizar sus datos, el proveedor del servicio los tiene perfectamente controlados[23]. No debe olvidarse que, hoy por hoy, el oligopolio americano en este nuevo modelo de negocio es evidente.

Los tres modelos de servicios básicos son SaaS (*Software as a Service*), PaaS (*Platform as a Service*) y IaaS (*Infraestructure as a Service*), de los que nos ocuparemos más adelante.

Los cuatro modelos de implementación del servicio se corresponden -de ellos también daremos cuenta seguidamente- con las denominadas "*nube privada*", "*pública*", "*comunitaria*" e "*híbrida*".

Una de las primeras empresas que vieron la oportunidad de negocio compartiendo su infraestructura computacional a la carta y a bajo coste fue Amazon (*Amazon Web Services*)[24] siendo, en la actualidad, uno de los más exitosos. Tras él siguieron el Windows Azure de Microsoft, Yahoo! y Google; éste último posee una importante red mundial de centros de datos. De todos modos, hoy en día, existen otros proveedores de servicios de computación en la nube como los conocidos Salesforce.com, Dropbox o el iCloud de Apple, entre otros. En España Movistar ofrece servicios de computación en la nube a un precio realmente competitivo.

2.2 Modelos

En este lugar, diferenciaremos entre los modelos de servicios de computación en la nube (a.) y de implementación (b).

a) De servicios

Se aceptan, de forma generalizada, los tres tipos de servicios que seguidamente exponemos[25].

---

[22] Ya en 2013, Google anunciaba que estaba construyendo un centro de datos flotante en la bahía de San Francisco (http://www.elpais.com.uy/vida-actual/google-estaria-construyendo-centro-datos.html). De hecho, la movilidad de los centros de datos es ya una realidad, así pueden transportarse en containers o en camiones tipo trailers.

[23] JAEGER, *et al.*, http://pear.accc.uic.edu/ojs/index.php/fm/article/view/2456/2171. Fecha consulta: septiembre 2015.

[24] Amazon's Elastic Compute Cloud (EC2), http://aws.amazon.com/ec2. Este servicio permite al usuario emplear por tiempo el espacio virtual de los centros de datos de Amazon. Asimismo, dispone del Amazon's Simple Storage Service (S3), http://aws.amazon.com/s3. El estudio de otros proveedores de servicios de computación en la nube puede verse en BRADSHAW /MILLARD /WALDEN (2010, pp. 1-47).

[25] SOSINSKY (2011, p. 35); BUYYA /BROBERG /GOSCINSKI (2011, pp. 13-15); Agencia Española de Protección de Datos (en adelante, AEPD, 2013), p. 8.

En primer lugar, se encuentra la "*infraestructura como servicio*" (IaaS) que proporciona las máquinas virtuales, el almacenamiento virtual, la infraestructura y otros elementos de hardware al cliente de forma virtual. Esta infraestructura es administrada por el proveedor del servicio. Amazon (EC2) es un proveedor clásico de estos servicios. El usuario compartiría un ordenador de forma virtual con almacenamiento en el que instalaría su sistema operativo y las aplicaciones de este sistema desarrollando, por ejemplo, todas las aplicaciones que necesita su empresa partiendo de cero. Por su parte, Amazon posee varios sistemas operativos y aplicaciones que ofrece en régimen de arrendamiento a sus usuarios/clientes.

En segundo término, destaca la "*plataforma como servicio*" (PaaS) que proporciona máquinas virtuales, sistemas operativos, aplicaciones, servicios, trabajos de desarrollo, estructuras de control, etc… El usuario puede desarrollar sus aplicaciones en la nube o emplear las que en ésta existan para, por ejemplo construir bases de datos. Proveedores de este servicio son Google AppEngine o Windows Azure Platform.

En tercer lugar, se alude a "*software como servicio*" (SaaS) que consiste en el entorno operativo completo con aplicaciones, administración e interfaz del usuario. La aplicación se proporciona al usuario a través, normalmente, del navegador. En este caso, el proveedor del servicio ofrece al usuario un software con sus aplicaciones en formato prepago. En este modelo el usuario emplea la aplicación contratada para, por ejemplo, desarrollar la contabilidad de su empresa o para la gestión de la información de su empresa, y no responde de la instalación, de su mantenimiento o de su actualización pues ello corre a cargo del proveedor del servicio. Destacan en este servicio GoogleAps, Oracle On demand, SalesForce.com, SQL Azure.

De los tres modelos de servicios, el que se prevé claramente como el más contratado será el SaaS. En efecto, hacia 2018, se prevé que el 59 % de los servicios sean de este modelo, frente al 28 % IaaS y al 13% PaaS[26].

Estos tres modelos se conocen como SPI de computación en la nube. Junto a estos se ha hablado también de "*Storage as a Service*" (StaaS) o almacenamiento como servicio, "*Identity as a Service*" (IdaaS) o identidad como servicio, "*Compliance as a Service*" (CmaaS) o conformidad como servicio, si bien pueden surgir otros servicios en el futuro ya que la computación en la nube se encuentra, de momento, en sus inicios.

b) De implementación

Suele ser ya tradicional mencionar los cuatro modelos de implementación de la nube propuestos por el NIST. En primer lugar, encontramos la "*nube pública*" que, como su nombre indica, está disponible para el uso público proporcionando recursos a los más variados usuarios desde particulares hasta administraciones públicas pasando por

[26] CISCO, *Cloud Index White Paper*, 2013-2018.

empresas y ONGs. Cualquiera puede, en principio, contratar los servicios de computación. La "*nube privada*", en cambio, funciona para uso privado de una gran organización (por ejemplo, una administración pública o un holding de empresas), que es quien gestiona y administra sus servicios, aunque su implementación y supervisión puede ser contratada a terceros. Por su parte, la "*nube híbrida*" combina varias nubes ofreciendo servicios en el modelo de nube privada y de nube pública paralelamente. Finalmente, se encuentra la "*nube comunitaria*" en la cual los servicios son compartidos por una comunidad cerrada[27].

3. La computación en la nube y protección legal del titular de los datos de carácter personal

Una de las materias primas de las que se "alimentan" los servicios de computación en la nube es la *información*, la cual puede ser calificada, en su mayor parte, de *información de carácter personal* en la medida en que se trata de datos de carácter personal recogidos por una empresa o por la administración pública en el ejercicio de sus funciones que son usuarios de estos servicios o bien es el propio titular de los datos de carácter personal el que emplea estos servicios de computación en la nube. Según se trata de uno u otro supuesto, la figura del responsable del tratamiento de los datos de carácter personal varía. Además, el proveedor de servicios de computación en la nube suele externalizarlos contratando a terceros que, a su vez, pueden subcontratar a otros sujetos para que participen en fases concretas del tratamiento de los datos de carácter personal (3.2). Ante esta situación, es necesario plantearse diferentes aspectos relacionados con el consentimiento de la persona física titular de los datos de carácter personal, tales como si es necesario éste o no y si, en todo caso, procede el derecho a ser informado de que sus datos serán tratados mediante servicios de computación en la nube (3.4). Habida cuenta de que los servicios de computación en la nube implican transferencias de los datos a proveedores que se encuentran ubicados en países diferentes al lugar del domicilio del titular de los datos de carácter personal e incluso del responsable del tratamiento, se hace necesario referirse a la transferencia internacional de datos (3.5). De todas estas cuestiones nos ocupamos seguidamente desde la perspectiva del titular de los datos de carácter personal, esto es, la persona física de la cual los mismos se recaban. Antes, sin embargo, conviene dejar asentado qué entendemos por "*dato de carácter personal*" (3.1). El derecho aplicable será asimismo tratado (3.3).

3.1 Concepto de "dato de carácter personal"

La *Directiva 95/46/CE del Parlamento europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* (DOCE L 281 de 23 de noviembre de 1995. En adelante, "Directiva 95/46/CE"), lo define, en su Art. 2 letra a, como "*toda información sobre una persona física identificada o identificable*". Esta información puede ser relativa tanto a su identidad física, fisiológica, psíquica, económica, cultural o social. Esta definición es recogida por el Art. 3

[27] SOSINSKY (2011, p. 32); PUYOL MONTERO (2013, pp. 48-49); AEPD (2013, p. 7).

letra a de la LOPDCP y precisada en el Art. 5 letra f del RDCP en el siguiente sentido: "*cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*".

El Grupo de Trabajo del Art. 29, en su Dictamen acerca del concepto de "dato de carácter personal"[28], ha indicado que el legislador europeo contempla el concepto de "información" en sentido amplio incluyendo todo tipo de afirmaciones sobre una persona, tanto información "objetiva" (por ejemplo, datos sobre su salud) como "subjetiva" (por ejemplo, opiniones o evaluaciones acerca de su fiabilidad como parte contratante)[29]. No es necesario que esa información sea verídica o esté probada para recibir protección. En este caso, el interesado tiene el derecho de acceder a ella y refutarla. La información acerca de la persona comprende también los denominados "datos sensibles" (Art. 8 Directiva 95/46/CE, Art. 7 LOPDCP). Así, se comprende toda la información relativa a la vida personal y familiar de la persona como también cualquier información sobre actividades desarrolladas por esa persona como su actividad laboral, económica o social. Toda esta información puede estar contenida en cualquier tipo de formato o soporte. Por tanto, puede ser información alfanumérica, gráfica, fotográfica o sonora. En este sentido, la información almacenada en un ordenador utilizando un código binario es información que puede considerarse "dato de carácter personal".

Por su parte, el Art. 4 apartado segundo de la *Propuesta de Reglamento del Parlamento europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)* de 25 de enero de 2012 [COM(2012) 11 final. En adelante, "Propuesta de Reglamento general de protección de datos"] define los "*datos personales*" como "*toda información relativa a un interesado*". Se trata de un concepto "amplio" que comprende aquellas informaciones que puedan relacionarse con un individuo en el sentido que lo postuló el Dictamen del Grupo de Trabajo del Art. 29 acerca de la definición de "dato de carácter personal". De todos modos, la recogida de datos personales, que después serán objeto de tratamiento, debe ser conforme con la finalidad que se persiga con el mismo, esto es, debe cumplirse el "principio de proporcionalidad".

3.2 La figura del responsable y del encargado del tratamiento de los datos de carácter personal cuando los servicios de computación en la nube implican dicho tratamiento

Abordaremos, en primer término, la figura relativa al responsable del tratamiento (a) para, en segundo lugar, referirnos al encargado del mismo (b) en relación siempre con la contratación de servicios de computación en la nube.

[28] Dictamen del Grupo de Trabajo del Art. 29, 4/2007, sobre el concepto de datos personales adoptado el 20 de junio (WP 136).

[29] Véase, asimismo la Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, *Un enfoque global de la protección de los datos personales en la Unión Europea*, COM(2010), 609 final, pp. 5-6.

a) El responsable del tratamiento frente al titular de los datos de carácter personal

Con base en el concepto de "responsable" del tratamiento, elaborado por el Grupo de Trabajo del Art. 29, determinaremos quiénes pueden ser los posibles responsables del tratamiento de datos de carácter personal[30] cuando se contratan servicios de computación en la nube.

- Concepto de "responsable" del tratamiento

De acuerdo con el Art. 3 letra d LOPDCP se considera "responsable" del tratamiento a la "*persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*". Más preciso es el Art. 5.1 letra q del RPDCP que advierte que el hecho de que decida conjuntamente con otros acerca de la finalidad, contenido y uso del tratamiento no implica que deje de ser considerado "responsable del tratamiento"[31] (Art. 4 núm. 5 Propuesta de Reglamento general de protección de datos). La figura del "responsable" del tratamiento es esencial en la normativa protectora de los datos de carácter personal puesto que es él el que debe de tratar lícitamente los mismos, frente a él se ejercitan los derechos por parte del titular de los datos y a él se atribuye la responsabilidad por los daños que, a éste, se le puedan ocasionar como consecuencia de una acción u omisión. Además, determina qué legislación nacional resulta de aplicación a las operaciones de tratamiento de datos de carácter personal.

El Grupo de Trabajo del Art. 29, en su Dictamen 1/2010, analiza los conceptos de "responsable" y de "encargado" del tratamiento de datos de carácter personal[32] en relación con el Art. 3 letras d) y e) respectivamente de la Directiva 95/46/CE. Respecto del primero, que es el que, en este lugar, nos interesa, entiende que puede considerarse como responsable del tratamiento a aquél al que se asigna una capacidad de influencia sobre la base de las circunstancias de hecho, lo que conllevará atender a las relaciones contractuales existentes, en su caso, entre las partes[33]. Además, es el que determina el objeto, uso y finalidad del tratamiento, aunque éste delegue la determinación de los "medios" del procesamiento en terceros al tratarse de cuestiones más de índole técnica. Por tanto, es el que ostenta el poder de decisión respecto de la creación del fichero con los datos así como su tratamiento, independientemente de quién lleve a cabo materialmente dicho

[30] El tratamiento de los datos comprende, de acuerdo con la definición dada en el Art. 3 letra c LOPDCP, "*todas aquellas operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*" (Art. 5.1 letra t RPDCP).

[31] HERRÁN ORTIZ (2002, p. 207); PUYOL MONTERO (2013, pp. 90-91).

[32] Adoptado el 16 de febrero de 2010 (WP 169).

[33] MOINY (2011, pp. 290-293).

tratamiento, el cual puede actuar bajo la dependencia o instrucciones de la persona física o jurídica que ostenta el poder de decisión, esto es, del responsable[34].

- Posibles responsables del tratamiento en caso de contratar servicios de computación en la nube

La prestación de servicios de computación en nube suele ser contratada mayormente por empresas o por la administración pública[35]. Son estas personas jurídicas las que manejan un gran volumen de datos de carácter personal que necesitan, en ocasiones, de un tratamiento que comprende complejas operaciones informáticas, para las cuales no siempre se dispone de las máquinas y de los softwares adecuados. En este caso, el responsable del tratamiento es, frente a la persona física titular de los datos personales, aquél organismo público o privado que los recoge determinando los fines y, en su caso, los medios para el tratamiento[36]. En este sentido, el empresario o la administración pública se presentan como "responsables del tratamiento" resultando el "proveedor del servicio" como "encargado del tratamiento". Nosotros vamos a tratar separadamente las cuestiones relacionadas cuando el cliente del servicio de computación en la nube es un particular empresario de cuando lo es una administración u organismo público. De todos modos, con carácter previo, debemos ver si es posible que el propio usuario/consumidor de estos servicios de computación en la nube pueda llegar a ser considerado responsable del tratamiento de datos.

- El propio usuario

El particular destinatario final del servicio de computación en la nube emplea, cada vez más, este servicio para almacenar sus datos, para compartir videos o música con otros usuarios de internet destinatarios finales. Se prevé que si, en 2013, sólo un 38 % de los consumidores empleaban servicios de almacenamiento en la nube, hacia el 2018 será el 53 %[37]. Junto a este servicio se irán paulatinamente contratando otros servicios que la "nube" ofrece igualmente al destinatario final consumidor[38]. En este caso, por tanto, el usuario

[34] VIZCAÍNO CALDERÓN (2001, p. 80).

[35] De ahí que tanto el Dictamen 05/2012 sobre la computación en nube, adoptado el 1 de julio de 2012, del Grupo de Trabajo del Art. 29 (WP 196) como la *Guía para clientes que contraten servicios de Cloud Computing* de la AEPD (2013) se fijen exclusivamente en estos supuestos.

[36] HON / MILLARD / WALDEN (2011, pp. 1-31).

[37] CISCO, *Cloud Index White Paper*, 2013-2018.

[38] Acogemos el concepto de "consumidor" dado por el Art. 3 del RD Legislativo 1/2007, de 16 de noviembre redactado por el apartado uno del artículo único de la Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el RD Legislativo 1/2007, de 16 de noviembre (BOE de 28 marzo): "*son consumidores o usuarios las personas físicas que actúen con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión*.

contrata los servicios de un proveedor en relación con sus propios datos sin que haya precedido ninguna recogida de datos, ya que éstos son los propios del usuario destinatario del servicio. Así, la relación entre éste y el proveedor se regirá por lo acordado en el contrato de servicios que celebraron, en virtud del cual, el segundo se habrá comprometido, entre otros aspectos, a mantener unas determinadas medidas de seguridad de los datos del usuario del servicio.

Sin embargo, también puede darse el caso en el que el usuario destinatario final del servicio de computación en la nube haya recogido previamente los datos de terceros, por ejemplo, en el caso de redes sociales en línea, bien pudiera ser que el usuario recaba datos de otros usuarios de la misma red social y todos esos datos son posteriormente objeto de tratamiento mediante la contratación de servicios de computación en la nube. En este supuesto, el usuario debería ser considerado el responsable del tratamiento de los datos personales recogidos en la medida en que él decide la finalidad del tratamiento; mientras que el encargado del mismo sería el proveedor de servicios de computación en la nube. En este caso, no estaría amparado en la denominada "excepción doméstica" (Art. 2.2 letra a LOPDCP)[39].

> En el caso *Lindqvist*, que dio lugar a la sentencia del Tribunal de Justicia de la Unión Europea de 6 de noviembre de 2003[40], se acogió un concepto estricto de la "excepción doméstica". En el supuesto se trataba de la recogida de datos, que hacía una persona física en su sitio web, de los miembros de la parroquia con los que colaboraba. El órgano judicial consideró que se trataba de un tratamiento de datos y que la persona física debía ser considerada responsable del mismo con arreglo a la legislación de protección de datos de carácter personal sin que cupiera entender su actuación como una actividad puramente doméstica[41].

- El empresario. Contrato de outsourcing informático

La computación en la nube presenta ventajas destacables para las empresas. Entre ellas pueden destacarse la comercialización, la internacionalización, la eficiencia productiva, la capacitación del capital humano, la eficiencia financiera, la calidad o el grado de

---

Son también consumidores a efectos de esta norma las personas jurídicas y las entidades sin personalidad jurídica que actúen sin ánimo de lucro en un ámbito ajeno a una actividad comercial o empresarial".

Puesto que el consumidor destinatario final del servicio de computación en la nube es titular de datos de carácter personal, éste sólo puede ser una persona física. Luego, el concepto de consumidor, en este trabajo, aparece referido a la persona física.

[39] Dictamen del Grupo de Trabajo del Art. 29 5/2009, sobre las redes sociales en línea, adoptado el 12 de junio de 2009 (WP 163), pp. 5-7.

[40] C-101/01.

[41] Comentario a esta sentencia, DE MIGUEL ASENSIO (2004, p. 4). Acertadamente, advierte este autor que, aunque se les considere responsables del tratamiento, no tienen, en cambio, la consideración de proveedores de servicios de la sociedad de la información.

implantación de las tecnologías e innovación[42]. Los servicios de computación en la nube externalizan muchas de las tareas que debería llevar a cabo la empresa, entre ellas, el tratamiento de los datos recabados de sus propios empleados o de sus clientes sean, a su vez, consumidores destinatarios finales o no, se trate de otras empresas. En este caso, es el propio empresario cliente de servicios de computación en la nube el que ostenta poder de decisión sobre la finalidad del tratamiento de los datos y, consiguientemente, actúa como responsable del mismo y, por tanto, deberá respetar la legislación sobre protección de datos de carácter personal[43].

En el caso que nos ocupa, el empresario celebra un contrato de *outsourcing* informático[44] con otro empresario, que es el proveedor de los servicios de computación en la nube, que presenta un carácter atípico, por lo que se regirá especialmente por lo pactado entre las partes en virtud de su autonomía de la voluntad (para el derecho español, véase Art. 1255 CC) y, en lo no previsto, deberán tenerse presente las normas sobre el contrato de arrendamiento de servicios[45] y, a la postre, las normas generales sobre derecho de obligaciones y contratos. De todos modos, en la mayoría de supuestos, la contratación de estos servicios se hace de forma electrónica, a través del sitio web del proveedor del servicio, y que se trata de contratos de adhesión con condiciones generales, de suerte que la adaptación a las necesidades particulares del empresario contratante son mínimas, casi inexistentes. En todo caso, se contendrán en anexos o adendas, que establecerán las especificaciones en orden a atender las necesidades de la empresa contratante, al acuerdo o contrato marco en el que se comprenderán las estipulaciones de carácter general aplicables a otros contratos[46].

En lo concerniente a la *protección de datos*, que es el extremo que nos ocupa, el contrato que se celebre entre el proveedor del servicio y el empresario debe contener una cláusula acerca de la protección de los datos que comunica éste a aquél para su tratamiento. En particular, es relevante la ubicación de los datos, las garantías para las transferencias internacionales de datos[47], habida cuenta de que la mayoría de proveedores de servicios de computación

[42] URUEÑA *et al.* (2012, pp. 25 ss).

[43] Dictamen del Grupo de Trabajo del art. 29 5/2012, sobre la computación en nube, adoptado el 1 de julio de 2012 (WP 196, p. 9).

[44] CARRASCO LINARES / PUENTE SERRANO (2004, p. 184); DAVARA RODRÍGUEZ (2004, pp. 271-273); MARZO PORTERA/MARZO PORTERA/MARTÍNEZ FLECHOSO (2004, p. 32); PUYOL MONTERO (2013, p. 116).

[45] Cuando el responsable del tratamiento delega en un tercero la materialización del mismo, esto es, contrata con él las operaciones necesarias para llevar a cabo el tratamiento de los datos de carácter personal suele aludirse a arrendamiento de servicios (APARICIO SALOM, 2009, pp. 41 ss).

[46] GARCÍA DEL POZO VIZCAYA (2012, p. 186); OPPENHEIM (2012, pp. 95-96).

[47] El derecho aplicable en caso de contratación internacional de servicios de computación en la nube se expone más adelante (epígrafe e).

en la nube son multinacionales, las medidas de seguridad exigibles, compromiso de confidencialidad, portabilidad de los datos, garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) por parte del titular de los datos de carácter personal[48]. Asimismo, debería hacerse constar si el tratamiento de datos, o parte de las operaciones en que éste consista, se subencarga a terceros, quiénes son éstos. Especial relevancia adquiere la "cláusula de tercero beneficiario", la cual permite al titular de los datos de carácter personal exigir responsabilidad al responsable del tratamiento de sus datos por los incumplimientos que, de sus obligaciones, lleve a cabo el encargado del mismo y, en caso de existir una cadena de subcontrataciones, a éste por los incumplimientos del subencargado.

- La Administración u organismo público. Contrato de suministro o de servicios

De entrada, debe destacarse que la posibilidad de que una administración u organismo público lleve a cabo la gestión y actuación administrativa de forma electrónica viene reconocida por el Art. 33 de la Ley 11/2007, de 22 de junio, *de acceso electrónico de los ciudadanos a los servicios públicos* (BOE núm. 150, de 23 de junio. En adelante, "LAE")[49]. Una forma de gestionar electrónicamente la actividad administrativa es mediante la contratación de servicios de computación en la nube. A este respecto, desde la normativa reguladora de los contratos del sector público, esto es, el Real Decreto Legislativo 3/2011, de 14 de noviembre, *por el que se aprueba el texto refundido de la Ley de contratos del sector público*[50], el contrato celebrado con un proveedor de los servicios, que son objeto de este trabajo, sería o bien un contrato de suministro (Arts. 290 ss) o bien un contrato de servicios (Arts. 301 ss)[51].

En relación propiamente con la protección de los datos personales que los documentos electrónicos contengan, debe indicarse, en primer lugar, que la administración u organismo público será considerada la "responsable" del tratamiento de los mismos pues es ella la que tiene el poder de influencia en la determinación de la finalidad del mismo, con independencia de que los medios técnicos para ejecutarlo aparezcan concretizados por un tercero que es el que tendrá la condición de "encargado" del tratamiento[52]. El Art. 22.2 del Real Decreto 4/2010, de 8 de enero, *que regula el esquema nacional de interoperabilidad en el*

[48] AEPD (2013, pp. 15-18).

[49] Acerca de las nuevas tecnologías como herramienta para modernizar a la administración pública, véase TRONCOSO REIGADA (2010, pp. 567 ss).

[50] BOE núm. 276, de 16 de noviembre.

[51] Esta cuestión de forma más detenida puede leerse en PALOMAR OLMEDA (2012, pp. 210 ss).

[52] El riesgo de que eso afecte al ámbito de competencias de la administración, de suerte que no sea ésta la que adopte las decisiones, sino el proveedor del servicio, es puesto de relieve por VALERO TORRIJOS (2012, p. 233).

ámbito de la administración[53], establece la aplicación de la legislación de protección de datos de carácter personal cuando los documentos electrónicos administrativos contengan datos personales.

De acuerdo con el Art. 12 LOPDCP y Arts. 20 a 22 RPDCP, la contratación de estos servicios, cuando impliquen tratamiento de datos personales, debe constar por escrito u otra forma que permita acreditar su celebración y contenido. La disposición adicional vigesimosexta del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público recoge determinados extremos relacionados con la protección de datos. En primer lugar, establece que el proveedor de los servicios, en nuestro caso, de computación en la nube, tendrá la consideración de "encargado" del tratamiento. En segundo lugar, una vez ejecutada la prestación, los datos deberán ser devueltos o destruidos. En tercer lugar, que el contrato deberá constar siempre por escrito eliminando, pues, la posibilidad de que conste en otra forma que establece el Art. 12.2 LOPDCP. En cuarto lugar, el acceso del proveedor a los datos, en cuanto encargado del tratamiento, no tendrá la consideración de comunicación o cesión de datos.

En el contrato de prestación de servicios de computación en la nube deben especificarse las medidas de seguridad en relación con los datos personales y garantizar la disponibilidad, confidencialidad e integridad que pueden requerir determinados servicios electrónicos prestados por las administraciones públicas[54].

b) El encargado del tratamiento en caso de contratar servicios de computación en la nube

Cuando se contratan servicios de computación en la nube que comportan el tratamiento de datos personales, el proveedor de estos servicios adquiere, como regla general, la condición de "encargado" del tratamiento, de ahí que nos detengamos, en su concepto. Sin embargo, cuando el tratamiento de los datos comporta complejas operaciones cabe la posibilidad de que el encargado del tratamiento contrate, a su vez, con terceros algunas de dichas operaciones generándose consiguientemente una cadena de subencargados que tienen acceso a los datos de carácter personal. Como paso previo, no obstante, conviene diferenciar entre el acceso a los datos de la cesión o la comunicación de los datos.

- Acceso a los datos y cesión o comunicación de datos. Distinción

El legislador español, tras la estela del comunitario, diferencia entre "acceso" a los datos (Art. 12 LOPDCP) y "comunicación o cesión" de datos (Art. 11 LOPDCP) a terceros. En el primer caso, no es necesario el consentimiento del titular de los datos; mientras que, en el

[53] BOE núm. 25, de 29 de enero. Respecto del concepto de interoperabilidad, véase MARTÍNEZ GUTIÉRREZ (2011, pp. 671-672).

[54] AEPD (2013, pp. 20-21).

segundo caso, sí, salvo las excepciones que, en el propio Art. 11.2 LOPDCP, se mencionan. Estaremos ante un supuesto de "acceso" a los datos, por terceros, cuando la transmisión de los datos se efectúa de responsable del tratamiento a encargado; mientras que, si la transmisión acontece entre dos responsables del tratamiento, nos hallaremos ante la "cesión o comunicación" de datos[55]. En ambos casos, es posible que tanto el acceso como la comunicación o cesión impliquen una transferencia internacional de datos o no, es decir, tan sólo una transferencia doméstica.

Por otro lado, a pesar de que el legislador español ha empleado la doble expresión "cesión o comunicación", en el Art. 3 letra i LOPDCP, como "*toda revelación de datos realizada a una persona distinta del interesado*" debe entenderse que las emplea como sinónimas[56]. La revelación de datos, en este caso, se hace a una tercera persona que no es el titular de los datos, ni el responsable del fichero, ni del tratamiento, ni el encargado del mismo o personas autorizadas por éstos para tratar los datos (Art. 5.1 letra r RPDCP).

En este sentido, cuando los empleados del responsable del tratamiento tratan los datos de carácter personal no existirá cesión de datos. Tampoco cuando acceda a ellos el encargado del tratamiento vinculado contractualmente con el responsable o los subcontratados por el primero con la autorización del segundo o los empleados del encargado o subencargado. En todos estos casos, sólo existe una revelación de datos que supone *acceso* a ellos pero no *cesión o comunicación* de datos en la dirección que acabamos de ver. Cuando los datos se revelan a otras empresas del mismo grupo (filiales), en caso de multinacionales, que van a tratar los datos, pero no en calidad de encargados, sino que los van a tratar para otras finalidades (las propias) nos hallaremos ante una cesión de datos que precisará del consentimiento del titular de los datos, puesto que, a pesar de tratarse de empresas del mismo grupo, actúan como responsables del tratamiento[57]. Si, en cambio, el tratamiento que hacen éstas se atiene a la finalidad prevista por el responsable del tratamiento inicialmente, tendrán la consideración de encargados, y la revelación de datos supondrá un acceso a los mismos y no una cesión.

- Concepto de "encargado" del tratamiento. El proveedor de los servicios de computación en la nube como encargado

El responsable del tratamiento puede procesar los datos personales en su propia organización empleando a su personal o bien celebrar un contrato con un tercero al que le encarga las operaciones en que consiste el tratamiento. En este último caso, ese tercero tendrá la condición de "encargado" del tratamiento y actuará por cuenta del responsable. En la medida en que debe tratar los datos personales, tendrá acceso a los mismos. La

[55] Entiende que la LOPDCP recoge un concepto amplio de cesión, VIZCAÍNO CALDERÓN (2001, pp. 157-158).

[56] APARICIO SALOM (2009, pp. 218 ss); MESSÍA DE LA CERDA BALLESTEROS (2003, p. 41); DE MIGUEL ASENSIO (2004, p. 8).

[57] MESSÍA DE LA CERDA BALLESTEROS (2003, pp. 222 ss).

definición de "encargado" se encuentra recogida en el Art. 3 letra g LOPDCP, si bien, el Art. 5.1 letra i RPDCP es más preciso a la hora de conceptuar al "encargado", advirtiendo que la prestación del servicio de tratamiento de los datos por cuenta del responsable trae causa de una relación jurídica, entre ambos, que delimita el ámbito de actuación del "encargado" (Art. 4 núm. 6 Propuesta de Reglamento general de protección de datos).

La figura del "encargado" del tratamiento también ha sido abordada por el Grupo de Trabajo del Art. 29 en su Dictamen 1/2010, ya significado. En éste, se establece que, para poder actuar como encargado del tratamiento, tienen que darse dos condiciones: primera, que se trate de una entidad independiente del responsable y, segunda, que se traten los datos por cuenta de éste[58]. El encargado puede actuar en operaciones o actividades específicas en relación con el tratamiento o de forma más general. El elemento decisivo es su actuación por cuenta del responsable, lo que no impide que el encargado tenga autonomía para determinar qué medios técnicos son los más adecuados para mejor servir el encargo que se le ha encomendado. En la medida en que debe cumplir el encargo encomendado por el responsable tendrá acceso a los datos de carácter personal tratados.

En tratamientos complejos de datos es posible que el responsable haya contratado con diversos encargados operaciones específicas o bien que el encargado subcontrate, a su vez, a terceros para que las realicen dando lugar a una cadena de subcontrataciones o subencargados a la que en el epígrafe siguiente nos referiremos.

Debe llamarse la atención, en relación con la contratación de servicios de computación en la nube, acerca del hecho de que, el proveedor de estos servicios, si los mismos comportan el tratamiento de datos personales, lo que no siempre, tendrá lugar, será considerado "encargado" del tratamiento. Éste, a su vez, podrá subencargar determinadas operaciones a terceros[59], si así se determinó con el responsable del tratamiento cliente de los servicios de computación en la nube, lo que, por otro lado, puede implicar un movimiento o transferencia internacional de datos personales. Esto no impide que el encargado pueda resultar, a su vez, responsable del tratamiento cuando éste aparece determinado conjuntamente con el cliente. En este sentido, quedaría comprendido en la definición antes vista de responsable, si bien en la práctica quién define la finalidad del tratamiento es el cliente de los servicios de computación en la nube.

El encargado del tratamiento puede también recoger, sobre la base de los servicios que ofrece, datos de sus clientes, puede determinar su propia finalidad y puede tratarlos en relación con ésta. En este caso, el encargado del tratamiento de los datos, que actúa por cuenta del responsable, es, en cambio, responsable de su propio fichero y de su propio tratamiento. Téngase presente que, en la actualidad, estos servicios de computación en la

[58] Adoptado el 16 de febrero de 2010, WP 169, p. 31.

[59] De este modo ha sido considerado por el Grupo de Trabajo del Art. 29 en su Dictamen 05/2012, sobre la computación en nube, pp. 9-10.

nube se contratan electrónicamente, a través de sitios web, que emplean cookies u otra tecnología similar para recoger datos que, después, procesan creando perfiles y que sirven a finalidades específicas de publicidad comportamental. Respecto del tratamiento específico de estos datos será considerado, a los efectos de la legislación de protección de datos de carácter personal, responsable[60].

El Art. 12 LOPDCP (Arts. 20 a 22 RPDCP) exige que el contrato por el que un tercero acceda a los datos personales para su tratamiento conste por escrito o en otra forma que permita acreditar su celebración y contenido. Debe establecerse expresamente que el encargado del tratamiento debe sujetarse a las instrucciones dadas por el responsable y que no empleará los datos para finalidades distintas que las previstas por el responsable ni los comunicará a otras personas si no se encuentra expresamente autorizado por el responsable del tratamiento. El acceso del tercero (encargado del tratamiento) a los datos bajo estos requisitos no se considera comunicación o cesión de datos que exija, por tanto, el consentimiento del titular de los datos de carácter personal. Si, en cambio, el encargado del tratamiento usa los datos para finalidades distintas, los comunica a terceros sin estar autorizado o incumple las estipulaciones contractuales, responderá entonces, frente al titular de los datos, como responsable del tratamiento (Art. 12.4 LOPDCP). Responsabilidad que no irá exclusivamente referida a la administrativa que prevé la propia LOPDCP, sino también a la responsabilidad civil frente al titular (Art. 19.1 LOPDCP).

- La cadena de subcontrataciones

Por su parte, los subcontratistas deberán ajustarse a las instrucciones dadas por el responsable, el cual debe definir muy claramente la finalidad para la cual se tratan los datos y autorizar la contratación de terceros por parte del encargado (Art. 21.1 RPDCP), salvo que nos encontremos en el supuesto de excepción previsto en el Art. 21.2 RPDCP. Así, no se precisará de la autorización cuando se especifiquen en el contrato, celebrado entre responsable y encargado, las operaciones que pueden ser objeto de subcontratación y, si se conoce, la empresa que se va a subcontratar. Si no se conocen, antes de contratarla deberán comunicarse los datos relativos a la misma al responsable del tratamiento. Además, es necesario que el tratamiento de los datos que haga el subcontratista se ajuste a las instrucciones dadas por el responsable y que el encargado del tratamiento y la empresa subcontratista celebren el contrato de acuerdo con lo previsto en el Art. 20 RPDCP. El contrato entre encargado y subencargados debe constar por escrito o en otra forma de suerte que se pueda acreditar su celebración y contenido[61].

En el caso de que el responsable del tratamiento sea la administración u otro organismo público, también cabe la posibilidad de que el proveedor del servicio de computación en la nube, a su vez, contrate a terceros para el mejor desempeño de su prestación contractual.

[60] Sobre ello véase (NAVAS NAVARRO, 2015, *in totum*).

[61] PUYOL MONTERO (2013, pp. 99 ss).

En este caso, deberá especificarse esta eventualidad en el contrato celebrado entre la administración u organismo público y el encargado del tratamiento, esto es, el proveedor de los servicios de computación en la nube, el tratamiento se ajuste a las instrucciones dadas por el responsable del tratamiento, la administración u organismo público contratante, que el contrato celebrado entre encargado y subencargado del tratamiento cumpla con lo previsto en el Art. 12 LOPDCP (disp. ad. vigésimo sexta del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público) y conste sólo por escrito. Frente al responsable del tratamiento y frente al titular de los datos, el subencargado tendrá la consideración de "encargado" del tratamiento. Esto quiere decir, a nuestro modo de ver, que, de acuerdo con el Art. 5 LOPDCP, el titular de los datos debe ser informado no sólo de la identidad del responsable del tratamiento sino también del encargado y, en su caso, del subencargado del tratamiento.

Es frecuente, hoy en día, que tanto el encargado como los subencargados se encuentren en un país diferente al país en el que tiene su domicilio el responsable del tratamiento, lo que comporta una transferencia o movimiento internacional de datos que puede determinar que la responsabilidad, sobre todo, frente al titular de los datos de carácter personal, se diluya en la cadena de subcontrataciones. Pero, también, desde el punto de vista del responsable del tratamiento puede resultar harto difícil controlar, en estos casos, las actividades en que el tratamiento consista, si se respeta la finalidad del tratamiento que aquél ha decidido y si se comunican o no los datos personales a terceros. Por eso, la Comisión, mediante la Decisión de 5 de febrero de 2010[62], ha establecido una serie de *cláusulas contractuales tipo*, que si bien tienen que ver con la transferencia internacional a encargados y subencargados que se encuentran en terceros países, pueden servir, sin embargo, de modelo a tener en cuenta en los contratos celebrados entre responsable del tratamiento y encargado o entre éste y subencargados, aunque se encuentren en un mismo país o en diferentes países pero dentro del Espacio económico europeo (EEE) o en países con un nivel declarado adecuado como son USA[63] y Suiza[64] con los que hay firmados

[62] Decisión de la Comisión 2010/87/UE, de 5 de febrero de 2010 relativa a las cláusulas tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del parlamento europeo y del Consejo (DOUE L 39/5, 12.2.2010).

[63] Decisión de la Comisión de 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 (DOCE L 215/7 de 25 de agosto de 2000). Esta Decisión ha sido recientemente declarada inválida por la STJUE de 6 de octubre de 2015 (asunto C-362/14).

64 Decisión 2000/518/CE, de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza (DOCE L 215/7 de 25 de agosto de 2000).

sendos Acuerdos de Puerto Seguro. En estos dos últimos supuestos, no se trata de una transferencia internacional de datos de carácter personal[65].

Además, estas cláusulas contractuales tipo pueden combinarse con las "*binding corparate rules*" (en adelante, BCR) cuando el encargado del tratamiento es una multinacional y los subencargados del tratamiento son empresas que forman parte del grupo.

Como destacamos posteriormente, nos parece que estos contratos deberían contener una cláusula de tercero beneficiario a favor del titular de los datos personales, como proponen tanto la Decisión 2010/87/UE y las BCR en el caso de movimiento internacional de datos, pero referida al movimiento nacional de datos. Esta cláusula en beneficio del tercero, cuyos datos son objeto de tratamiento o subtratamiento, es especialmente relevante para fortalecer la posición de la persona física ante el responsable del tratamiento.

3.3 Derecho aplicable y protección de datos de carácter personal

El Art. 4 de la Directiva 95/46/CE (Art. 2.1 LOPDCP) regula el Derecho aplicable en materia de protección de datos de carácter personal mediante una regla general (Art. 4.1 letra a) y dos reglas especiales (Art. 4.1 letras b y c) que tienen que ver con su aplicación extraterritorial. La regla general será tratada en primer lugar (a) y, seguidamente, nos centraremos en las especiales (b)[66].

a) Regla general: establecimiento del responsable en España

El Art. 4.1 letra a de la Directiva 95/46/CE se corresponde con el Art. 2.1 letra a LOPDCP, si bien el tenor literal de esta norma no se corresponde exactamente con el de la primera. En efecto, el Art. 4.1 letra a parte del dato de que el establecimiento del responsable del tratamiento se encuentre localizado en un territorio de un Estado miembro, en cuyo caso se aplica la ley de este Estado a todo tratamiento de datos. En cambio, el precepto español, considera, analizado literalmente, que el tratamiento de los datos sea efectuado en territorio español para que sea aplicable la ley española independientemente de que el establecimiento del responsable del tratamiento se encuentre o no ubicado en territorio español. Esta asintonía entre ambos preceptos ha sido paliada por el Art. 3.1 letra a RPDCP según el cual se aplica la ley española a todo tratamiento efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español.

Puede afirmarse, pues, que el punto de vista del que parte la regla general en cuanto al derecho aplicable es el del responsable del tratamiento de los datos. Además, se aplica la

[65] Dictamen 5/2012, sobre la computación en nube, p. 11.

[66] En general, sobre la aplicación del Art. 4 de la Directiva 95/46/CE, véase MOEREL (2011, p. 92).

ley nacional de cada Estado miembro en el que éste tenga ubicado un establecimiento[67] y en éste trate datos de carácter personal. Es lo que se ha denominado aplicación "distributiva" de la ley[68].

> De interés, a este respecto, es la STJUE de 13 de mayo de 2014, conocida como *Google Spain*[69], en la que se aprecia por el alto tribunal que la vinculación que existe entre Google Inc. y su filial España Google SL permite entender cumplido el requisito que exige el Art. 4 de la Directiva 96/45/CE de que el tratamiento se lleve a cabo en el marco de las actividades de un establecimiento del responsable en territorio español. En este caso, Google cuenta con una sucursal en España, aunque esté destinada principalmente a la venta de espacios publicitarios en el sitio web.

b) Reglas especiales: aplicación extraterritorial

Dos son las reglas especiales que tienen que ver con la aplicación extraterritorial de la legislación sobre protección de datos de carácter personal: la primera, tiene en cuenta si la utilización de los medios para el tratamiento se da o no en España; la segunda, consiste en la aplicación del Derecho internacional.

- Situación geográfica de los medios usados para el tratamiento

El Art. 4.1 letra c de la Directiva 95/46/CE, el cual se corresponde con el Art. 2.1 letra c LOPDCP, contempla un supuesto en el que se aplica la ley española aunque el responsable del tratamiento tenga ubicado su establecimiento fuera del EEE. Para ello, el responsable del tratamiento debe utilizar medios para el mismo situados en territorio de un Estado miembro, en nuestro caso, en España. En este caso, el responsable debe designar un representante en España (Art. 5.1 letra d LOPDCP, Art. 3 letra c II RPDCP). Esto quiere decir que si el responsable del tratamiento está establecido en un Estado miembro del EEE que no es España, no se aplicará la ley española sino la ley del Estado en el que tenga el establecimiento[70]. El "medio" usado en el tratamiento aparece identificado por dos elementos. Según el Grupo de Trabajo del Art. 29, un primer elemento es el carácter instrumental del tratamiento que el responsable quiere hacer; un segundo elemento, que es la permanencia, es decir, que se excluye el mero tránsito del medio en un Estado miembro del EEE[71]. El propio Grupo de Trabajo del Art. 29 ha rechazado que el ordenador del

[67] Un concepto amplio de "establecimiento" es el que se desprende del "Dictamen 8/2010, sobre el Derecho aplicable", emitido el 16 de diciembre de 2010 (WP 179, pp. 12-13).

[68] SANCHO VILLA (2010, p. 43).

[69] C-131/12.

[70] Véase, "Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE", aprobado el 30 de mayo del 2002 (WP 56, p. 6).

[71] "Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria", p. 9.

usuario de internet (o, incluso, un servidor) que se encuentre localizado en un Estado miembro sea considerado medio a efectos de aplicar la ley nacional de ese Estado miembro[72]. Ahora bien, si un servidor instala, por ejemplo, cookies en el equipo terminal del usuario con el objeto de recabar información personal que será objeto de tratamiento, el Grupo de Trabajo del Art. 29 entiende que se aplicará la ley del Estado miembro donde se halle ese equipo, aunque el responsable del tratamiento tenga su establecimiento fuera del EEE[73]. A su vez, esta situación entrañaría una transferencia internacional de datos a un país fuera del EEE que sería lícita si recabara la autorización de la AEPD[74], salvo si se interpreta que el usuario ha prestado su consentimiento de acuerdo con lo explicitado en el Art. 26 letra a de la Directiva 95/46/CE[75].

- Aplicación del Derecho internacional al responsable del tratamiento

La ley española de protección de datos se aplica igualmente al responsable del tratamiento no establecido en territorio español cuando, de acuerdo con las normas de derecho internacional público, resulte de aplicación aquélla (Art. 4.1 letra b Directiva 95/46/CE, Art. 2.1 letra b LOPDCP). Se refiere el precepto a los ficheros y tratamientos que se llevan a cabo por la misión diplomática regidos por la ley nacional que acredite esa misión[76].

3.4 Información y consentimiento del titular al tratamiento de sus datos

Sobre el responsable del tratamiento compete el deber de informar al titular de los datos acerca de dicho tratamiento (a) y, en su caso, recabar el oportuno consentimiento al mismo (b).

a) Derecho a ser informado del tratamiento. Cláusula de tercero beneficiario como uso del tráfico y Códigos tipo

Tras exponer el contenido de la información, referiremos quiénes son los sujetos obligados a informar y la forma en que la información debe presentarse a fin de que el titular pueda prestar un consentimiento informado.

- Contenido de la información

---

[72] "Dictamen 8/2010, sobre el Derecho aplicable", pp. 13-14.

[73] "Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria", pp. 11-12. En la doctrina, véase DE MIGUEL ASENSIO (2015, p. 363); HON/HÖRNLE/MILLARD (2011, pp. 1-47).

[74] Véase epígrafe sobre transferencia internacional de datos.

[75] SANCHO VILLA (2010, p. 47).

[76] SANCHO VILLA (2010, pp. 49-50).

El Art. 5.1 LOPDCP establece un contenido mínimo de la información que debe de suministrar el responsable del tratamiento al titular de los datos, algunos de cuyos extremos, sin embargo, pueden omitirse si se deduce de la naturaleza de los datos que se soliciten o de las circunstancias concretas en las que éstos se demanden (Art. 5.3 LOPDCP). Por eso, nos parece que el contenido debe también comprender aquella información que imponga el principio general de buena fe y que evite el dolo (Art. 7.1 CC). Así, el titular de los datos de carácter personal debe ser informado, de modo expreso, preciso e inequívoco de la existencia de un fichero, de que sus datos personales se recogen y serán objeto de tratamiento, la finalidad del mismo y los destinatarios de sus datos, debe darse a conocer quién es el responsable del tratamiento, recordarle la posibilidad de ejercicio de sus derechos, entre otros aspectos. Dentro del grupo de destinatarios debería comprenderse al encargado del tratamiento contratado por el responsable y, en su caso, los posibles subencargados del mismo que, a su vez, haya contratado el encargado. Debe notarse que, en la mayoría de casos, sobre todo, cuando se manejan *Big Data* y el proveedor de servicios de computación en la nube es una multinacional, lo usual es la subcontratación de las diferentes operaciones en qué consiste el tratamiento de los datos. Esta información debe estar disponible para el titular de los datos, en la medida en que si encargado y subencargados no se ajustan a la finalidad perseguida con el tratamiento de los datos ocasionando daños al titular de los mismos, serán considerados como responsables del tratamiento, asumiendo la responsabilidad civil, penal y administrativa que les corresponda (Art. 12.5 LOPDCP).

En el supuesto de movimiento internacional de datos que implique el acceso a los mismos cuando el encargado es el importador de los datos y se encuentra en un tercer país, la Decisión de la Comisión 2010/87/UE establece, en virtud del Art. 26.4 de la Directiva 95/46/CE, cláusulas contractuales tipo, de las que destaca la cláusula 3 que considera al titular de los datos como "tercero beneficiario" que tiene derecho a recibir información exhaustiva tanto del exportador de los datos como del importador de los mismos, entre la que destaca, previa petición del titular de los datos, la puesta a disposición de una copia de las cláusulas contractuales contenido de la relación jurídica existente entre responsable y encargado o entre éste y el subencargado, dejando a salvo los extremos que se corresponden con aspectos confidenciales de la empresa en cuestión[77]. Por su parte, la cláusula 11 establece que los contratos entre encargado y subencargado contendrán siempre una cláusula de tercero beneficiario. A nuestro modo de ver, la cláusula de tercero beneficiario, con lo que comporta a efectos de contenido de la información, debería aplicarse también cuando no exista movimiento internacional de datos. Debería ser una práctica habitual o un uso del tráfico cuando se tratan datos de carácter personal (Arts. 1258 y 1287 CC).

En el caso en que se adopte un Código tipo por una empresa o grupo de empresas, éstos contienen necesariamente cláusulas que garanticen el ejercicio de los derechos por parte de los titulares de los datos personales así como que puedan estar informados del contenido

[77] La referencia detenida a este extremo se realiza posteriormente.

del Código al que se refiere el Art. 73 RPDCP[78]. Sin embargo, la adopción de un Código tipo es puramente voluntaria (Art. 72.1 RPDCP), para el responsable del tratamiento, lo que significa que la cláusula de tercero beneficiario queda al albur de lo que decida éste; mientras que su aplicación como "uso del tráfico" derivaría directamente de la ley y se integraría en el contenido de los contratos celebrados entre responsable y encargado o entre éste y subencargado.

En definitiva, dentro del contenido de la información que debe suministrarse al titular de los datos personales se aprecian tres niveles: el primero, un contenido "*minimísimo*" que es el que comprende tan solo la información relativa a la existencia de un fichero, del tratamiento, su finalidad y destinatarios de la información y la identidad del responsable del fichero y tratamiento (letras a y e Art. 5.1 LOPDCP); el segundo, un contenido "*mínimo*" que comprende, además de la información antecitada, la información relativa al carácter obligatorio o facultativo de las respuestas a las preguntas planteadas, a las consecuencias en caso de obtención de datos o su negativa a suministrarlos y la posibilidad de ejercitar los derechos ARCO (Art. 14 Propuesta de Reglamento de protección general de datos) y, en tercer lugar, un contenido "*óptimo*", en la medida en que es el que ofrece al titular de los datos personales la información más pertinente a los efectos de poder ejercitar sus derechos de forma eficaz y contar con los medios de prueba necesarios para ello[79], que comprendería, además, de todos los extremos acabados de mencionar, toda aquella información necesaria derivada de la buena fe (Art. 7.1 CC) y toda aquella que se avenga con la "cláusula de tercero beneficiario" que debería atribuirse al titular de la información en los contratos celebrados entre responsable del tratamiento y encargado o entre éste y subencargados, independientemente de que existiera o no movimiento internacional de datos.

- Sujetos obligados a informar

El derecho a ser informado que ostenta el titular de los datos se corresponde con la obligación de informar que tiene el responsable del tratamiento, cuya fuente es la ley, concretamente, la LOPDCP. Se trata de una obligación legal de hacer, de carácter unilateral y previa a la prestación del consentimiento por parte del titular de los datos ya que, sólo en la medida en que esté informado podrá autorizar la recogida y posterior tratamiento de sus datos. La información tiene que estar accesible en todo momento para el usuario, de suerte que la pueda consultar cuando la necesite. Asimismo debe ser informado puntualmente de todos los cambios o actualizaciones en la información que se vayan realizando por el responsable del tratamiento. Así, posibles cambios relacionados con la finalidad del tratamiento, duración del mismo o contratación de nuevos encargados o subencargados del

[78] HERRÁN ORTIZ (2002, pp. 312-313).

[79] En todo caso, en relación con el encargado o subencargado intervinientes en el proceso siempre se podrá acudir al principio de facilidad probatoria, haciendo recaer en éstos la carga de la prueba de aquellos hechos que resulten de muy difícil o de imposible prueba para el actor (Art. 217.7 LEC).

tratamiento de los datos personales del titular. En el caso de que quién recoja los datos sea una administración u organismo público, un genérico deber de informar a los ciudadanos de que la administración o el organismo público en cuestión trata sus datos mediante servicios de computación en la nube puede derivarse del deber de transparencia administrativa recogido en el Art. 3.4 y 6 LAE[80] y del Art. 5.3 de la *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno*[81]. Debe tenerse presente, de todos modos, que el deber de informar aparece recogido, como ha quedado dicho, en el Art. 5 LOPDCP, pues, una cosa es no necesitar al consentimiento al tratamiento de los datos y otra diferente que no se tenga que informar al titular de que sus datos están siendo recogidos y ya se trate de recogida directamente o indirectamente de él, si bien la administración u organismo público podría ampararse en las excepciones recogidas en el Art. 5.5 LOPDCP.

En relación con el encargado y subencargado del tratamiento, parece que tanto la LOPDCP como el RPDCP no los considera obligados a informar al titular de los datos de que los mismos son objeto de tratamiento. El único obligado a proporcionar la información es el responsable del tratamiento. Es más, el ejercicio del derecho de acceso por parte del titular de los datos es siempre frente al responsable del tratamiento (Art. 27.2 RPDCP). Será éste, por tanto, quién deba facilitarle la información que requiera el titular. Sin embargo, como hemos apuntado con anterioridad, a nuestro modo de ver, los contratos celebrados entre responsable y encargado del tratamiento o entre éste y un subencargado deberían contener, como uso habitual, una cláusula de tercero beneficiario, de suerte que el titular de los datos pueda dirigirse, en todo momento, tanto al encargado como al subencargado a fin de poder solicitarles determinada información que éstos, a buen seguro, pueden estar en mejor disponibilidad de ofrecer al titular que el propio responsable del tratamiento. Así, por ejemplo, cuando el titular de los datos quiere información acerca de los medios tecnológicos o algoritmos con los que aquélla va a ser tratada.

- Forma de la información

A tenor del Art. 5.1 LOPDCP la información debe proporcionarse de forma expresa, precisa e inequívoca, si bien no se requiere que se le presente al titular de los datos por escrito. Luego, cabe cualquier forma, si bien, en la práctica, suele proporcionarse de este modo. Por su parte, el Art. 18 RPDCP establece que el deber de informar debe cumplirse a través de un medio que permita, en un momento posterior, acreditar que éste se ha cumplido de forma efectiva. El responsable del tratamiento tiene el deber de conservar el soporte en el que conste que se ha dado cumplimiento al deber de informar por parte de éste. En el derecho de información en la recogida de los datos deberá tenerse presente si los datos son recabados directamente del titular o no, esto es, se hace de forma indirecta, en cuyo caso, el

[80] Duda de que exista efectivamente tal deber a cargo de la administración pública, VALERO TORRIJOS (2012, p. 239).

[81] BOE núm. 295, de 10 de diciembre de 2013.

titular deberá ser informado dentro de los tres meses siguientes al momento del registro de sus datos (Art. 5.4 LOPDCP).

La información que se suministra al titular de los datos debe ser precisa e inequívoca según reza el Art. 5.1 LOPDCP. La información tiene que ser clara y detallada y adecuarse a la persona a la que se dirige, por ejemplo, si es un menor de edad. Esto implica que la información debe reunir las características de visibilidad y accesibilidad. En este sentido, debe tenerse en cuenta el tipo y el tamaño de la presentación de la información siendo inteligible, de suerte que se comprenda con facilidad, debiéndose proporcionarse directamente al titular y no estar disponible, en algún lugar, del sitio web de la empresa. Debe existir una comprensión directa del texto evitando en la medida de lo posible las remisiones entre diferentes textos que puedan inducir a confusión al titular de la información personal[82].

b) Consentimiento al tratamiento

La expresión "consentimiento" empleada en la legislación protectora de los datos de carácter personal puede inducir a confusión en la medida en que se la considere como "consentimiento contractual". En efecto, el término, de hecho, se emplea en el sentido de "asentimiento" que no significa, desde un punto de vista jurídico, lo mismo que "consentimiento". Por eso, se impone, en primer lugar, la debida distinción para acto seguido referirnos a la necesidad de consentimiento al tratamiento de los datos cuando el responsable contrata servicios de computación en la nube que impliquen recogida y/o tratamiento de datos personales.

- "Consentimiento" contractual y "asentimiento". Distinción en materia de tratamiento de datos personales

Vaya por delante que, como en otro lugar hemos puesto de relieve[83], aunque la legislación protectora de los datos de carácter personal emplee la expresión "consentimiento" (Art. 7 Propuesta de Reglamento general de protección de datos), en realidad, se trata de un "asentimiento", esto es, la autorización o aprobación para que una determinada actuación, que tendrá consecuencias jurídicas, pueda producirlas. En el caso que nos ocupa, el asentimiento es una declaración de voluntad unilateral y recepticia cuya finalidad es legitimar la actuación del responsable para que se inmiscuya en la esfera privada del titular de los datos, los recoja y proceda a su tratamiento.

[82] Todas estas cuestiones, analizadas detenidamente, con diferentes ejemplos, pueden consultarse en NAVAS NAVARRO (2015, pp. 84 ss).

[83] Sobre ello véase NAVAS NAVARRO (2015, p. 108).

Por lo tanto, la prestación de ese consentimiento (*rectius*, asentimiento) no es consentimiento "contractual" o "negocial"[84] *per se* y, consiguientemente, no es constitutivo de ninguna relación jurídico-negocial con el responsable del tratamiento[85]. Otra cuestión es que, con motivo de la existencia de una relación jurídica entre titular de los datos y responsable del tratamiento, se recojan los datos del primero para ser tratados de acuerdo con una finalidad determinada por el segundo incluyéndose en el negocio jurídico que da nacimiento a la relación entre las partes, una cláusula acerca del tratamiento de los datos y se requiera la aquiescencia del titular para ello.

En la práctica, el consentimiento prestado por el titular de los datos parte contratante tiene el doble efecto de ser consentimiento contractual y asentimiento al tratamiento de sus datos que haga el responsable, a su vez, parte contratante. Esto tiene una importante implicación. A saber, que la vulneración de la legislación sobre protección de datos de carácter personal implicará para el responsable y/o encargado del tratamiento responsabilidad extracontractual y no contractual. El hecho de que se aproveche el vehículo (negocio jurídico documentado) para recabar el asentimiento al tratamiento del titular de los datos personales no supone que las consecuencias de la vulneración de la legislación mencionada, por el responsable del tratamiento, caigan bajo el manto de la responsabilidad contractual. Esta distinción es harto relevante cuando existen elementos internacionales en el supuesto de hecho y debe discernirse qué derecho es el aplicable, es decir, el Reglamento Roma I[86] o el Reglamento Roma II[87]. Y esta distinción no cambia por el hecho de que los datos que se recojan sean necesarios para el cumplimiento o ejecución del contrato o bien no estén relacionados con la relación contractual que se establezca entre las partes (Art. 15

[84] Esta alusión al consentimiento contractual también la hace el Grupo de Trabajo del Art. 29 en su "Dictamen 15/2011, sobre la definición del consentimiento", adoptado el 13 de julio del 2011 (WP 187), p. 7.

[85] En este sentido, disentimos de la distinción que hace SANCHO VILLA (2010, pp. 61 ss) que parece seguir la línea propuesta por APARICIO SALOM (2009, pp. 20 ss).

Para nosotros, los tratamientos de datos son siempre no consensuales si con esta expresión se quiere indicar la existencia de una relación jurídica entre titular de los datos y responsable del tratamiento al margen de la existencia de una relación contractual en cuyo seno se recojan una serie de datos personales de las partes contratantes. Sobre el asentimiento como "autorización" al tratamiento, véase LLÁCER MATACÁS (2012, pp. 125 ss).

[86] Como se conoce, este es el Reglamento 593/2008, sobre ley aplicable a las obligaciones contractuales de 17 de junio de 2008, el cual sustituye al Convenio sobre la ley aplicable a las obligaciones contractuales, hecho en Roma el 19 de junio de 1980 (BOE núm. 171, de 19 de julio de 1993).

[87] Reglamento 864/2007 sobre ley aplicable a las obligaciones extracontractuales (DOUE L 199, de 31.07.07). El Art. 1.2 letra g de este Reglamento excluye de su ámbito de aplicación a las "obligaciones contractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular, la difamación". Respecto de esta exclusión, lamenta DE MIGUEL ASENSIO la incapacidad del legislador comunitario de unificar este materia en concreto (2009, pp. 695-726). Para el derecho español, deberá aplicarse la norma recogida en el Art. 10.9 CC.

RPDCP). Ya se trate de un caso u otro, la necesidad de informar acerca del tratamiento y la necesidad de recabar, salvo excepciones, el consentimiento del titular de los datos al tratamiento, así como la responsabilidad, en caso de no cumplir con los requisitos que establece la legislación sobre protección de datos de forma independiente a la información precontractual, al consentimiento contractual y a la responsabilidad contractual, debe mantenerse, si no desde el punto de vista fáctico o material, puesto que se dan o se recaban a la vez, sí, y sobre todo, desde el punto de vista jurídico. Aunque, como ha quedado dicho, en puridad se trata de asentimiento y no consentimiento, nosotros seguiremos empleando esta segunda acepción pues es la que utiliza, a la sazón, el legislador.

- Necesidad de consentimiento al tratamiento. Excepciones

El Art. 6.1 LOPDCP exige el consentimiento inequívoco[88] del titular de los datos al tratamiento, salvo que la ley dispusiera otra cosa. Si el responsable del tratamiento es un empresario conviene diferenciar dos supuestos: i) los datos sobre cuyo tratamiento se contratan los servicios de computación en la nube son los datos recabados en virtud de una relación negocial, laboral o administrativa entre el empresario y el titular de los datos; ii) los datos recogidos son de titularidad de terceros con los cuales dicha relación jurídica no existe. En el primer caso, el Art. 6.2 LOPDCP exceptúa la necesidad de consentimiento del titular de los datos a su tratamiento en la medida en que este sea necesario para la celebración, el mantenimiento o cumplimiento de la relación, lo que se dará en la mayor parte de supuestos[89]. Así, si resulta que, a pesar de existir la relación jurídica entre titular de los datos y responsable del tratamiento, los datos que se recaban y el tratamiento que se pretende hacer no son necesarios para la celebración, mantenimiento o cumplimiento de la relación, será necesario el consentimiento del titular de los datos al tratamiento o, al menos, que tenga la opción de negarse al mismo (Art. 15 RPDCP)[90]. En el segundo caso, deberá recabarse el consentimiento inequívoco del titular.

En el supuesto de que quién sea el responsable del tratamiento sea una administración u organismo público, hay que tener presente igualmente la excepción prevista en el Art. 6.2 LOPDCP que preceptúa que no será necesario el consentimiento, cuando los datos se recojan para el ejercicio de las funciones propias de las administraciones públicas en el

[88] Respecto a los modos de exteriorización del consentimiento diferenciando entre el sistema *opt-in* y *opt-out* ya tuvimos ocasión de pronunciarnos, en otro lugar, al analizar el consentimiento que debe prestar el usuario a la instalación de determinado tipo de cookies (NAVAS NAVARRO, 2015, pp. 110 ss). Consideramos que tanto el derecho comunitario como el español exigen el modo de exteriorización del consentimiento *opt-in*. Éste es, a nuestro entender, el que debe aplicarse también en caso de consentimiento al tratamiento de datos personales.

[89] VIZCAÍNO CALDERÓN (2001, pp. 117-118). Por su parte, se considera, a nuestro modo de ver, erróneamente, que al prestar el consentimiento contractual se está implícitamente prestando el consentimiento al tratamiento de los datos personales por APARICIO SALOM (2009, pp. 140 ss).

[90] Acertadamente un sector doctrinal diferencia, en este supuesto, entre "datos contractuales" y "datos extracontractuales" (LLÁCER MATACÁS, 2012, pp. 72-77).

ámbito de sus competencias, independientemente de que éstas contraten servicios de computación en la nube o no para el tratamiento de todos sus datos.

La excepción a la necesidad de consentimiento es vista por un sector doctrinal como consentimiento presunto al tratamiento al quedar comprendido en el consentimiento contractual[91]. Ya hemos advertido, más arriba, que debe discernirse este último del asentimiento que es, en puridad, al que se refiere la legislación sobre protección de datos de carácter personal. En consecuencia, no existe, a nuestro entender, ningún consentimiento presunto. En todo caso, los datos recabados en el seno de una relación contractual o laboral constituyen el contenido de la carga que corresponde al acreedor (titular de los datos) de colaborar al cumplimiento de la prestación por parte del deudor (responsable del tratamiento). Pero una cosa es la necesidad de suministrar esos datos, a lo que puede compeler la relación obligatoria existente entre titular de los datos y responsable del tratamiento y otra es que esos datos deban ser objeto de tratamiento. Son dos cuestiones diferentes y lo que excepciona la ley es el asentimiento, a éste, por parte del titular de los datos. Sea lo que fuere, la no necesidad de consentimiento debe interpretarse de forma restrictiva[92].

En todo caso, hay que advertir que respecto de los datos especialmente protegidos deberá prestarse siempre el consentimiento de forma expresa y por escrito (Art. 7 LOPDCP). Estos datos no se hallan amparados por la excepción a la necesidad de consentimiento prevista en el Art. 6.2 LOPDCP[93].

3.5 Transferencia internacional de datos de carácter personal cuando se contratan servicios de computación en la nube

Cuando la contratación de servicios de computación en la nube comporta el tratamiento de datos de carácter personal, ya sea como actividad principal o accesoria, es frecuente, como ha quedado dicho, que los datos se transfieran a terceros países en los que se encuentra el encargado o alguno de los subencargados contratado por éste. En este sentido, debe, en primer lugar, referirse qué entendemos por "transferencia internacional de datos"[94] (a); después, trataremos la cuestión de la necesidad de autorización previa de la Agencia Española de Protección de Datos (en adelante, AEPD) para la transmisión internacional (b), aludiremos a las figuras del exportador e importador de datos, así como del tercero beneficiario (c) y, al final, nos centraremos en el régimen de responsabilidad (d) y en el Derecho aplicable (e).

[91] APARICIO SALOM (2009, pp. 70 ss); MESSÍA DE LA CERDA BALLESTEROS (2003, pp. 121-122).

[92] SANCHO VILLA (2010, p. 66).

[93] MESSÍA DE LA CERDA BALLESTEROS (2003, p. 281).

[94] PUYOL MONTERO (2013, pp. 141 ss).

a) Concepto de transferencia internacional de datos

La Directiva 95/46/CE recoge el régimen de las transferencias internacionales de datos a terceros países, en los Arts. 25 y 26, si bien no ofrece ninguna definición al respecto (Arts. 40 ss Propuesta de Reglamento de protección general de datos). En la misma dirección, la LOPDCP tampoco da ninguna definición, aunque su régimen jurídico se recoge en los Arts. 33 y 34, bajo la rúbrica "movimiento internacional de datos" comprendiendo no sólo la transferencia a terceros países, sino también las transferencias a otros países de la UE o a aquellos Estados con un nivel adecuado de protección, como, por ejemplo, son USA y Suiza con los cuales existe un Acuerdo de Puerto Seguro[95]. En este último caso, deberá tenerse presente si el receptor norteamericano se ha adherido a este acuerdo, en cuyo caso no necesitará autorización; en caso contrario, el exportador español deberá solicitar la autorización previa de la AEPD (Art. 33.1 LOPDCP). Las primeras transferencias, esto es, las dirigidas a terceros países están necesitadas de una autorización previa; las otras, no. Por su parte, el Art. 5.1 letra s RPDCP define la transferencia internacional de datos a un responsable o a un encargado del tratamiento, como toda aquella transmisión que se lleva a cabo fuera del territorio del EEE comprendiendo de esta guisa no sólo a los países de la UE sino también a Noruega, Islandia y a Liechtenstein.

Una transmisión de datos personales dentro del territorio del EEE no es considerada una transferencia internacional de datos. Tampoco en el caso que se dirija a un país con un nivel adecuado de protección, aunque el régimen jurídico y el control del legislador, en este caso, sea más estricto que en caso de que se dirija a un territorio del EEE. Así, habría tres niveles de protección: libre, en el caso de transmisión de datos a un territorio del EEE; estricto, cuando se trata de una transmisión dirigida a un país con un adecuado nivel de protección y, más estricto, todavía cuando se dirige a terceros países. Esta última es, en puridad, la transferencia de datos personales que se considera internacional tanto para el derecho comunitario como, obviamente, para el nacional[96].

b) Necesidad o no de autorización previa de la Agencia Española de Protección de Datos

La exportación de los datos se supedita a una autorización de la AEPD, si se trata de transmitir datos fuera del territorio del EEE (Art. 33.1 LOPDCP). Esta autorización debe ser

[95] Además, han recibido reconocimiento como país con un adecuado nivel de protección por la Comisión europea: Canadá (Decisión 2002/2/CE, de 20 de diciembre de 2001), Argentina (Decisión 2003/490/CE, de 30 de junio de 2003), Guernsey (Decisión 2003/821/CE, de 21 de noviembre de 2003), Isla de Man (Decisión 2004/411/CE, de 28 de abril de 2004), Jersey (Decisión 2008/393/CE de 8 de mayo de 2008), Islas Feroe (Decisión 2010/146/UE, de 5 de marzo de 2010), Andorra (Decisión 2010/625/UE de 19 de octubre de 2010), Israel (Decisión 2011/61/UE, de 31 de enero de 2011), Uruguay (Decisión 2012/484/UE, de 21 de agosto de 2012) y Nueva Zelanda (Decisión 2013/65/UE, de 19 de diciembre de 2012).

[96] SANCHO VILLA (2010, pp. 24-25); ÁLVAREZ RIGAUDIAS (2012, pp. 112-114); GUASCH PORTAS/SOLER FUENSANTA (2014, pp. 253-255).

solicitada por el responsable exportador y el procedimiento para su solicitud se encuentra recogido en los Arts 137 a 140 RPDCP.

El Art. 33.1 LOPDCP exige, para transmitir datos a terceros países, una autorización previa de la AEPD, la cual será otorgada en dos supuestos: uno, cuando el nivel de protección del país receptor sea evaluado positivamente por la AEPD tomando en cuenta las circunstancias que concurren en la transmisión misma, esto es, la identificación del emisor, del destinatario, del país tercero, de la finalidad de la transferencia, de la duración, de los riesgos implicados, de la evaluación de la protección que del país tercero ofrece respecto de esos riesgos e informes que la Comisión haya emitido (Art. 33.2 LOPDCP); dos, exige la aportación de garantías adecuadas por parte del exportador de datos a un tercer país (Art. 33.1 LOPDCP, Art. 70.2 RPDCP). En este segundo caso, las garantías adecuadas se corresponden con cláusulas contractuales, en virtud de las cuales, el exportador y el importador se comprometen a tratar los datos personales según un determinado nivel de protección que es el que hayan establecido en las mismas. Estas cláusulas contractuales cubren cuatro finalidades diferentes: facilitadora, supletoria de flexibilidad y de garantía[97]. En relación con esta última función, es relevante destacar que los derechos y deberes de las partes pueden verse condicionados por la introducción de una cláusula a favor del tercero beneficiario. Según el Art. 26.4 Directiva 95/46/CE, la Comisión puede adoptar -y ha adoptado-, como hemos reiterado, varias decisiones sobre cláusulas contractuales tipo para las transferencias de datos a terceros estados proponiendo modelos que ahorran costes de transacción a las partes implicadas y facilitando la autorización de la autoridad pública nacional correspondiente[98]. En concreto, cuando se trata de transferencias de responsable a responsable, esto es, de una cesión de datos, las partes tienen a su disposición el modelo adoptado por la Decisión 2011/497/CE[99] que fue modificada en 2004 por la Decisión 2004/15/CE[100]. Cuando se trata de responsable a encargado o de éste a un subencargado, es decir, a un importador, por lo tanto, se trata de acceso a datos y no de cesión, las partes a su disposición la ya citada tienen la Decisión de la Comisión 2010/87/UE[101].

Cuando se trata de grupos multinacionales que tienen empresas en diferentes estados, las cláusulas contractuales adoptan la forma de BCR (Art. 70.4 RPDCP), las cuales regulan la exportación de datos desde cada una de las sedes europeas hacia las sedes del grupo en terceros países, asegurando un nivel de protección adecuado con arreglo a la norma

97 SANCHO VILLA (2010, p. 125).

98 SANCHO VILLA (2010, p. 128).

99 DOUE L 181, de 4 de julio de 2001.

100 DOUE L 385, de 29 de diciembre de 2004.

101 Véase el "Dictamen del Grupo de Trabajo del Art. 29, sobre transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", adoptado el 24 de julio de 1998 (WP 12).

comunitaria, esto es, la Directiva 95/46/CE. Estas BCR deben ser aprobadas por las autoridades nacionales de protección de datos de los países exportadores de datos. Por eso, se ha establecido, mediante la Recomendación 1/2007, de 10 de enero, un procedimiento standard para solicitar la aprobación de estas BCR, la cual tiene en cuenta la propuesta que, en su momento hizo, la Cámara de Comercio internacional[102].

De todos modos, el Art. 34 LOPDCP contiene un listado de excepciones a la necesidad de autorización previa para poder transferir datos a terceros países (Art. 66.2 RPDCP). La primera excepción tiene que ver con la aplicación de Tratados o Convenios internacionales (Art. 34 letra a LOPDCP). La segunda excepción tiene que ver con la prestación del consentimiento a la transmisión internacional de datos: se da cuando concurra el consentimiento inequívoco del titular de los datos (Art. 34 letra e LOPDCP) o cuando la transferencia es necesaria para la celebración y ejecución de un contrato o precontrato entre el titular de los datos y el responsable del tratamiento o entre éste y un tercero interesado (Art. 34 letras f a g LOPDCP). Otra de las excepciones va ligada a intereses vitales del sujeto o sanitarias (Art. 34 letra c LOPDCP), cuando la transferencia sea necesaria para la prevención o para diagnósticos médicos, de asistencia sanitaria o tratamiento médico o gestión de servicios sanitarios. Las transferencias de dinero se rigen por su normativa específica (Art. 34 letra d LOPDCP), por lo que se excluyen de esta autorización necesaria. Las transmisiones que se basan en un interés jurídico-público (Art. 34 letra h LOPDCP) también quedan exceptuadas de dicha autorización.

c) Sujetos implicados en la transferencia

En punto a los sujetos, trataremos el concepto de "exportador" y de "importador" que no necesariamente se corresponden con el de "responsable" y "encargado" del tratamiento, aunque puedan coincidir, después, nos referiremos al tercer beneficiario, cual es, como se sabe, el titular de los datos de carácter personal, al que se refiere, de modo explícito, la Decisión 2010/87/UE ya que nos centraremos en el acceso a los datos personales por el encargado o por los subencargados, pues, es el supuesto de contratación de servicios de computación en la nube al ser considerado el prestador de éstos como encargado.

- Exportador e importador de datos

Aunque los conceptos sobre los cuales pivota el ámbito subjetivo de la LOPDCP sean los de responsable y encargado del tratamiento de los datos, en relación con la transferencia internacional de datos, el legislador introduce otros dos conceptos, cuales son el de "exportador" e "importador" de datos, que no tienen por qué coincidir con los otros dos anteriores.

A tenor del Art. 5.1 letra j RPDCP, "exportador" es aquella *persona física o jurídica que promueve la transferencia de los datos a un tercer país*; mientras que el Art. 5.1 letra ñ RPDCP

[102] SANCHO VILLA (2010, p. 127).

advierte que "importador" es la *persona física o jurídica que los recibe en un tercer país*, ya sea éste responsable o encargado del tratamiento. Esta clasificación está en función de quién envía y quién recibe los datos en un movimiento internacional de los mismos, nada más; sin pretender sustituir los conceptos de responsable y encargado del tratamiento[103]. Así, un exportador de datos puede ser un encargado del tratamiento, como bien puede suceder cuando se subcontratan servicios de computación en la nube, en los que el encargado al subcontratar los servicios hace una transferencia internacional de datos.

- El titular de los datos de carácter personal como "tercero beneficiario"

La cláusula del tercero beneficiario permite al titular de los datos de carácter personal exigir el cumplimiento de determinadas obligaciones tanto al responsable exportador como al encargado importador tal y como advierte la Decisión 2010/87/UE. En el mismo sentido aparece referida en las BCR.

- Las cláusulas contractuales tipo. La Decisión 2010/87/UE

Las obligaciones del *responsable exportador*[104] gozan del beneficio de la cláusula del tercero beneficiario, a excepción de la cláusula 4 letra a de la Decisión 2010/87/UE, que se refiere a la cláusula general de cumplimiento de las obligaciones previas a la transferencia de acuerdo con la ley de origen[105]. Se suele diferenciar entre obligaciones materiales y de garantía del exportador. Respecto de las primeras, el responsable exportador responde de la actividad desarrollada por el encargado y también de la que desempeñe un subencargado en caso de que se le hubiera contratado. El responsable exportador se compromete a determinar los extremos del tratamiento que debe realizar el encargado, a velar por su idoneidad y a responder por el incumplimiento en que incurriera el encargado. Las tres obligaciones gozan del beneficio de la cláusula de tercero beneficiario, es decir, el tercero titular de los datos puede exigir el cumplimiento de estas obligaciones (cláusula 4 Decisión 2010/87/UE). En el caso de que intervenga un subencargado, el exportador responde frente al titular de los datos de que el tratamiento se desarrolle sólo en su nombre y conforme al nivel de protección previsto en el contrato. Así, el titular de los datos puede dirigirse contra el exportador si el subencargado no garantiza el nivel de protección previsto en el contrato o no actúa en su nombre.

---

[103] SANCHO VILLA (2010, p. 27); ÁLVAREZ RIGAUDIAS (2012, p. 116).

[104] En punto al contenido de las obligaciones exigibles por el tercero beneficiario respecto del responsable exportador o del encargado importador, seguimos el acertado esquema bosquejado por SANCHO VILLA (2010, pp. 170 ss). Véase asimismo el considerando núm. 19 de la Decisión 2010/87/UE, a tenor del cual, "*las cláusulas contractuales tipo deben ser exigibles no solamente por las organizaciones que sean parte en el contrato, sino también por los interesados, en particular cuando estos sufran un daño como consecuencia del incumplimiento del contrato*".

[105] Véase el elenco de obligaciones del responsable que recoge el Art. 22 de la Propuesta de Reglamento de protección general de datos.

En relación con las obligaciones de garantía del responsable exportador, el tercero puede dirigirse contra el exportador si incumple la obligación de comunicar a la autoridad de control su intención de proseguir con la transmisión de datos, a pesar de la eventual incidencia de una regulación local del país del establecimiento del encargado notificada por éste y que impida cumplir con sus obligaciones. Asimismo, se puede dirigir contra el exportador, si incumple la obligación de entrega de una copia de las cláusulas al tercero que lo demande con mención de las medidas de seguridad adoptadas[106] y también de suministrarle una copia del contrato de subcontratación a los terceros que lo soliciten eliminando la información que sea confidencial de la empresa o no sea de interés para el tercero titular de los datos personales (cláusula 4 Decisión 2010/87/UE).

Si aludimos, en este momento, a las obligaciones del *encargado importador*, tenemos que todas ellas caen bajo la cláusula de tercero beneficiario salvo la obligación de auditoría (art. 26 Propuesta de Reglamento de protección general de datos). Asimismo debe diferenciarse entre obligaciones materiales y obligaciones de garantía. En lo concerniente a las primeras, el tercer beneficiario puede exigir el cumplimiento de las obligaciones de ejecución del contrato sólo en nombre del exportador de los datos y de acuerdo con sus instrucciones (cláusula 5 Decisión 2010/87/UE), el cumplimiento de sus obligaciones de conocimiento de los eventuales riesgos de incumplimiento que se deriven de la aplicación de la legislación local del país de su establecimiento y que le imponga obligaciones incompatibles con el contrato, incluye también la obligación de notificación al exportador derivada de cambios legislativos que tengan el efecto incompatible advertido. El tercero beneficiario puede exigir el cumplimiento de sus obligaciones como encargado de implementación de las medidas de seguridad y en lo relativo a la subcontratación, el encargado tiene la obligación de haber informado y obtenido previamente del exportador su consentimiento por escrito para la subcontratación. El importador responde frente al tercero beneficiario de que los servicios de subcontratación se harán en nombre del exportador obligándose a que el subencargado asegure el mismo nivel de protección ofrecido en las cláusulas (cláusula 5 Decisión 2010/87/UE).

En punto a las obligaciones de garantía del importador encargado, el tercero beneficiario puede exigir el cumplimiento de toda una serie de obligaciones. Así, la obligación de notificar al exportador las solicitudes de divulgación de datos realizadas por autoridades públicas competentes, todo acceso fortuito o no autorizado y las solicitudes no atendidas de los terceros, la obligación de atención de las consultas del exportador respecto de los datos transmitidos, así como, su obligación de atenerse a la opinión de las autoridades de control, obligación de suministrar copias del contrato de acceso o del contrato celebrado para la subcontratación de los datos a petición del interesado, sin la información comercial y sin que sea necesario incorporar copia sobre las medidas de seguridad, a estos efectos, basta una descripción somera. Asimismo, tiene la obligación de enviar al exportador de los

[106] En general sobre las medidas de seguridad adoptadas en el cloud computing, véase PUYOL MONTERO (2013, pp. 219 ss).

datos en el EEE una copia de todo acuerdo que concluya con un subencargado con arreglo a las cláusulas (cláusula 5 Decisión 2010/87/UE).

Por otro lado, a tenor de la cláusula 11.1 de la Decisión 2010/87/UE, el subencargado asume en el contrato con el importador las mismas obligaciones exigidas a este último. Esto quiere decir que este contrato contendrá también la cláusula de tercero beneficiario, si bien sólo podrá dirigirse contra el subencargado subsidiariamente cuando no pueda hacerlo contra el exportador o el importador (cláusula 11.2 Decisión 2010/87/UE). La cláusula 6 de la Decisión 2010/87/UE contiene las reglas del sistema de responsabilidad al que están sometidos exportador, importador y subencargado del tratamiento. De ellas daremos cuenta posteriormente. Cuando se trate de un responsable y de un encargado dentro del territorio del EEE, el régimen de responsabilidad se deducirá de la ley del responsable en el EEE.

Por su parte, la AEPD elaboró en 2012 un conjunto de cláusulas contractuales aplicables a los contratos de subcontratación de servicios entre encargados establecidos en España y subencargados radicados en terceros países[107]. Estas cláusulas tienen en cuenta el considerando núm. 23 de la Decisión 2010/87/UE, el cual, concede a las autoridades nacionales la opción de dar mayor flexibilidad en la subcontratación que lleven a cabo los encargados nacionales en relación con subencargados ubicados en terceros países. Las cláusulas contractuales tipo de la AEPD son similares a las comunitarias, aunque no idénticas. Se incluyen toda una serie de obligaciones del exportador de datos que son adicionales a las establecidas en la Decisión 2010/87/UE[108]: son las contenidas en las letras i) a n) de la cláusula 4.2.

- Las "binding corporate rules"

Los Arts. 70 ss del RPDCP establecen el régimen aplicable a las transferencias internacionales de datos dentro de las diferentes empresas que forman parte de un grupo multinacional. Concretamente, se refieren a la posibilidad de regular estos movimientos mediante las BCR pensadas básicamente para el responsable exportador. La Propuesta de Reglamento de protección general de datos las define como: "*políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro de la Unión para las transferencias o un conjunto de transferencias de datos personales a un responsable o encargado del tratamiento en uno o más países terceros, dentro de un grupo de empresas*". La transferencia sobre la base de las mismas se recoge en el Art. 43 de la misma Propuesta de reglamento.

[107] Este documento se puede consultar en www.aepd.es. Fecha consulta: septiembre 2015.

[108] GUASCH PORTAS / SOLER FUENSANTA (2014, p. 263).

El Grupo de Trabajo del Art. 29, en su Documento de 19 de abril de 2013[109], diseñó BCR para los encargados importadores de datos. Éstas deben considerarse como garantías adecuadas que el encargado del tratamiento ofrece al responsable (Art. 137 RPDCP). Su contenido se encuentra recogido en el Documento del Grupo de Trabajo del Art. 29, núm. 195[110]. Básicamente, se dispone que el subtratamiento de los datos podrá ser realizado por otro miembro del grupo del encargado del tratamiento cuando se haya informado previamente al responsable del tratamiento y se haya recibido su consentimiento por escrito. El acuerdo entre el encargado y el subencargado recibe el nombre de "*acuerdo de nivel de servicios*".

Los acuerdos deberán incluir una cláusula de tercero beneficiario a fin de que los titulares de los datos personales puedan exigir el cumplimiento de las obligaciones al responsable, encargado y subencargado del tratamiento.

Las obligaciones recogidas en las BCR que se ejecutarán mediante la cláusula de derechos de terceros beneficiarios son las siguientes[111]: obligación del encargado del tratamiento de respetar las BCR, las instrucciones del responsable del tratamiento relacionadas con el tratamiento de datos y las medidas de seguridad y de confidencialidad previstas en el acuerdo de servicios; creación de derechos de terceros beneficiarios para los interesados; responsabilidad del encargado del tratamiento de abonar las indemnizaciones y reparar las infracciones de las BCR; la carga de la prueba recae sobre el encargado del tratamiento, no sobre los interesados; fácil acceso a las BCR para los interesados; existencia de un proceso de gestión de quejas para las BCR; obligación de cooperar con las autoridades de protección de datos y con el encargado del tratamiento; principios de protección de la vida privada; lista de entidades encargadas del tratamiento sujetas a las BCR; transparencia para los casos en los que la legislación nacional no permite al encargado del tratamiento cumplir las BCR.

d) Régimen de responsabilidad

La Decisión 2010/87/UE introduce, en relación con el régimen de responsabilidad, una regla principal y dos reglas que tienen carácter subsidiario.

La regla principal se establece en la cláusula 6.1, en cuya virtud, se pueden diferenciar dos supuestos: a) en caso de incumplimiento del encargado y subencargado, en cuyo caso, el titular de los datos personales debe dirigirse contra el responsable en el EEE por el daño sufrido, el cual podrá dirigirse contra el encargado o el subencargado para reembolsarse

[109] "Documento explicativo sobre las normas corporativas vinculantes para los encargados del tratamiento" (WP 204).

[110] "Working Document 02/2012, setting up a table with the elements and principles to be found in processor binding corporate rules", adoptado el 6 de junio de 2012 (WP 195).

[111] Estas obligaciones se encuentran recogidas en el "Working Document 02/2012, setting up a table with the elements and principles to be found in processor binding corporate rules" referido en la nota anterior.

del perjuicio sufrido; b) en caso de incumplimiento del responsable del tratamiento se dirigirá contra éste directamente.

La regla subsidiaria primera se recoge en la cláusula 6.2 y se aplica cuando el exportador ha desaparecido de facto, ha cesado de existir jurídicamente o es insolvente, y, por tanto, el titular de los datos no puede dirigirse contra éste, podrá dirigirse contra el importador o el subencargado. El encargado no podrá alegar que quién incumplió sus obligaciones fue el subencargado y no él. Frente al titular de los datos, en la medida en que éste no pueda dirigirse contra el exportador, podrá dirigirse contra el importador (cláusula 6.2 II). Así, el encargado responde de los incumplimientos del subencargado pero no de los del responsable exportador.

La regla subsidiaria segunda aparece en la cláusula 6.3, en cuya virtud, si el titular de los datos no puede dirigirse contra el exportador o el importador por los incumplimientos del subencargado, por haber éstos desaparecido de facto, cesado de existir jurídicamente o ser insolventes ambos, el subencargado responderá frente al titular de sus propias obligaciones.

En general, debe recordarse que el régimen de responsabilidad cubre el incumplimiento de aquellas obligaciones que contienen la cláusula de tercero beneficiario; no de aquellas obligaciones que no la contengan[112].

e) Derecho aplicable

El tratamiento de los datos implica la celebración de un contrato entre el responsable y el encargado o entre éste y el subencargado. Por ello, la ley aplicable es la que establecen las reglas generales recogidas en los Arts. 3 y 4 del Reglamento de Roma I. En principio, la ley aplicable será la libremente elegida por las partes (Art. 3 Reglamento de Roma I), si bien, el sistema de autorizaciones de las transferencias está diseñado sobre la base de que las mismas sean más fácilmente obtenibles si se acoge la ley del exportador (Art. 33.1 LOPDCP, cláusula 9 Decisión 2010/87/UE). Esta solución, además, es congruente con el Art. 4 de la Directiva 95/46/CE que opta por la aplicación de la ley del lugar de residencia del responsable del fichero[113].

En defecto de elección, el Art. 4.1 letra b del Reglamento de Roma I determina que se aplique la ley estatal de la residencia habitual del prestador del servicio, es decir, del encargado o del subencargado según el caso[114]. Sin embargo, en materia de protección de

[112] SANCHO VILLA (2010, pp. 176-177).

[113] En cambio, el Art. 2.1 LOPDCP opta por la ley del lugar del tratamiento de los datos de carácter personal.

[114] En lo concerniente a los aspectos más específicos de Derecho Internacional Privado, véase SANCHO VILLA (2010, pp. 178 ss); ORTEGA GIMÉNEZ (2012, pp. 275 ss); FERNÁNDEZ ROZAS *et al.* (2013, p. 329); CASTELLANOS RUIZ (2009, pp. 126 ss).

datos, el Art. 4.1 de la Directiva 95/46/CE parte de la figura del responsable para determinar la ley aplicable a la protección de datos. Luego, ley aplicable al contrato de servicios de computación y ley aplicable a la protección de datos no siempre coincidirían. Sea lo que fuere, lo cierto es que el Grupo de Trabajo del Art. 29 considera que el responsable del tratamiento debe asumir una mayor responsabilidad por el tratamiento que el encargado. A éste le compete cumplir con las medidas de seguridad[115]. De ahí que un sector doctrinal considere que el responsable asume con carácter general los riesgos inherentes a la internacionalización de la prestación de estos servicios frente a los afectados titulares de los datos de carácter personal. Esto supone que si el responsable está ubicado en un Estado miembro del EEE y el encargado no, debe entenderse que el régimen de protección viene determinado por la ley aplicable al responsable del tratamiento y no al encargado (Cdo. núm. 18 de la Directiva 95/46/CE)[116].

4. Conclusión. Privacy by Design

Para los usuarios de los servicios de computación en la nube, esto es, para responsables o encargados del tratamiento, la computación en la nube representa una oportunidad para implementar lo que se ha dado en llamar *Privacy by design* (en adelante, PbD)[117]. La tecnología debería ser neutra, de suerte que no se dificultara el ejercicio de los derechos por parte de los sujetos concernidos. Si bien, inicialmente, la PbD, mediante el uso adecuado de la tecnología (*Privacy Enhancing Technologies* – PETs), pretende que el titular de los datos de carácter personal, o sea, el individuo o el ciudadano tenga un mayor control sobre sus datos, el tratamiento que se da a los mismos y las medidas de seguridad que se adoptan, previendo o evitando el acceso inconsentido a los mismos o a transmisiones de datos, cancelación automática de datos (o su rectificación), cuando ya no se correspondan con la finalidad perseguida por el tratamiento establecida por el responsable del mismo[118], también puede resultar una herramienta muy útil para éste cuando el tratamiento de los datos es encomendado a un tercero, el encargado, el cual, a su vez, puede subcontratar a otros para que realicen todo o parte de las operaciones en que el tratamiento de los datos consiste. Así, se minimizará el tratamiento de los datos, se reforzará la seguridad del mismo evitándose usos no autorizados de los datos por terceros, además de fortalecer la posición del titular de los datos de carácter personal, o sea, del afectado o interesado. En este sentido, es necesario que los fabricantes de las máquinas, de las aplicaciones, y demás herramientas tecnológicas creen mecanismos y las diseñen técnicamente de forma que

---

[115] "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la Unión Europea" aprobado el 24 de julio de 1998 (WP 12, pp. 15-16).

[116] SANCHO VILLA (2010, pp. 186-187).

[117] CAVOUKIN, www.privacybydesign.ca. Fecha de la consulta: septiembre 2015.

[118] LLÁCER MATACÁS (2011, pp. 88-92).

permitan que se adapten al nivel de privacidad exigido por el usuario, sea un particular, un empresario o la administración u organismo público[119].

La Comisión europea no ha sido ajena a esta cuestión, por lo que mediante la Comunicación al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad, de 2 de mayo de 2007[120], ha planteado la necesidad de diseñar tecnologías de protección que define como "*un sistema coherente de medidas de TIC que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin menoscabo de la funcionalidad del sistema de información*". Siguiendo esta línea, el Art. 23 de la Propuesta de Reglamento de protección general de datos determina la necesidad de proteger los datos personales desde el diseño y la técnica. Luego, la colaboración entre legislador e ingenieros informáticos se hace especialmente necesaria.

La posición del titular de los datos personales se fortalecería mucho más, a estos efectos, si se introdujera en los contratos entre responsable y encargado o entre éste y los subencargados una cláusula de tercero beneficiario, en los términos que hemos indicado en líneas superiores, puesto que esta tecnología diseñada formaría parte de las medidas de seguridad, de las obligaciones de garantía exigibles, por éste, a aquéllos.

5. Tabla de sentencias

Tribunal de Justicia Unión Europea

Tribunal y Fecha	*Referencia*	*Partes*
Gran Sala, 6.10.2015	C-362/14	Maximillian Schrens v Data Protection Commissioner, Digital Rights Ireland, Ltd.
Gran Sala, 13.05.2014	C-131/12	Google Spain SL, Google Inc. v AEPD, Mario Costeja González
Gran Sala, 6.11.2003	C-101/01	Lindqvist v Swedish Government, Netherlands Government, United Kingdom Government, Commission of the European Communities

[119] La relación entre privacidad diseñada y administración electrónica puede verse en TRONCOSO REIGADA (2011, pp. 196-199); ROIG BATALLA (2010, pp. 739 ss).

[120] COM(2007) 228 final.

6. Bibliografía

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2013), *Guía para clientes que contraten servicios de Cloud Computing*, (www.aepd.es).

Ignacio ALAMILLO DOMINGO (2012), "El control de localización de los datos e informaciones en el cloud" en Ricardo MARTÍNEZ MARTÍNEZ (ed.), *Derecho y Cloud Computing*, Thomson Reuters, Cizur Menor, pp. 63 ss.

Cecilia ÁLVAREZ RIGAUDIAS (2012), "Condiciones para las transferencias internacionales de datos personales en servicios de cloud" en Ricardo MARTÍNEZ MARTÍNEZ (ed.), *Derecho y Cloud Computing*, Thomson Reuters, Cizur Menor.

Juan APARICIO SALOM (2009), *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 3ª edic., Aranzadi, Thomson Reuters, Cizur Menor.

Simon BRADSHAW / Christopher MILLARD / Ian WALDEN (2010), "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services", Queen Mary University of London, School of Law, *Legal Studies Research Paper,* núm. 63/2010, pp. 1-47. Se puede consultar en: www.cloudlegal.ccls.qmul.ac.uk/Research/index.html. Fecha de la consulta: septiembre 2015.

Rajkumar BUYYA/James BROBERG/Andrzej GOSCINSKI (2011), *Cloud Computing. Principles and Paradigms*, Wiley, New Jersey.

Juan CARRASCO LINARES / N. PUENTE SERRANO (2004), "Las relaciones entre empresas" en Ana MARZO PORTERA / Fernando María RAMOS SUÁREZ, *La protección de datos en la gestión de empresas*, Aranzadi, Cizur Menor.

Esperanza CASTELLANOS RUIZ (2009), *El Reglamento «Roma I» sobre la ley aplicable a los contratos internacionales y su aplicación por los tribunales españoles*, Comares, Granada.

Anne CAVOUKIN, "Privacy by Design. The 7 Foundational Principles", www.privacybydesign.ca. Fecha de la consulta: septiembre 2015.

CISCO, *Cloud Index White Paper*, 2013-2018.

Miguel Ángel DAVARA RODRÍGUEZ (2004), *Manual de Derecho informático*, Thomson-Aranzadi, Cizur Menor.

Pedro DE MIGUEL ASENSIO (2004), "Avances en la interpretación de la norma comunitarias sobre protección de datos personales", *La Ley Unión Europea*, núm. 5964, de 27 de febrero de

2004, pp. 1-8.
- "El régimen comunitario relativo a la ley aplicable a las obligaciones extracontractuales" (2009), *Revista española de seguros*, núm. 140, pp. 695-726.
- *Derecho privado de internet* (2015), 5ª edic., Thomson Reuters, Civitas.

José Carlos FERNÁNDEZ ROZAS / Rafael ARENAS GARCÍA / Pedro DE MIGUEL ASENSIO (2013), *Derecho de los negocios internacionales*, 4ª edic., Iustel, Madrid.

Rafael GARCÍA DEL POZO VIZCAYA (2012), "La contratación empresarial de servicios de cloud computing" en Ricardo MARTÍNEZ MARTÍNEZ (ed.), *Derecho y Cloud Computing*, Thomson Reuters, Cizur Menor.

Manuel GARCÍA SÁNCHEZ (2012), "Retos de la computación en nube", en Ricardo MARTÍNEZ MARTÍNEZ (ed.), *Derecho y Cloud Computing*, Thomson Reuters, Cizur Menor.

C. GONG / J. LIU / Q. ZHANG / H. CHEN / Z. GONG (2010), "The Characteristics of Cloud Computing", *39th International Conference on Parallel Processing Workshops*, pp. 275-279 (DOI 10.1109/ICPPW.2010.45).

GRUPO DE TRABAJO DEL ART. 29, "Dictamen sobre transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", adoptado el 24 de julio de 1998 (WP 12).
- "Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE", aprobado el 30 de mayo del 2002 (WP 56).
- "Dictamen, 4/2007, sobre el concepto de datos personales" adoptado el 20 de junio (WP 136).
- "Dictamen 5/2009, sobre las redes sociales en línea", adoptado el 12 de junio (WP 163).
- "Dictamen 1/2010, sobre los conceptos de "responsable del tratamiento" y de "encargado del tratamiento", adoptado el 16 de febrero (WP 169).
- "Dictamen 8/2010, sobre el Derecho aplicable", adoptado el 16 de diciembre (WP 179).
- "Dictamen 15/2011, sobre la definición del consentimiento", adoptado el 13 de julio (WP 187).
- "Dictamen 05/2012 sobre la computación en nube", adoptado el 1 de julio (WP 196).
- "Working Document 02/2012, setting up a table with the elements and principles to be found in processor binding corporate rules", adoptado el 6 de junio (WP 195).
- "Documento explicativo sobre las normas corporativas vinculantes para los encargados del tratamiento", adoptado el 19 de abril de 2013 (WP 204).

Víctor GUASCH PORTAS / José Ramón SOLER FUENSANTA (2014), "Cloud Computing, cláusulas contractuales y reglas corporativas vinculantes", *Revista de Derecho UNED*, núm. 14, pp. 253-255.

Ana Isabel HERRÁN ORTIZ (2002), *El derecho a la intimidad en la nueva Ley orgánica de protección de datos personales*, Dykinson, Barcelona.

W. Kuan HON / Christopher MILLARD / Ian WALDEN (2011), "Who is Responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Part 2", Queen Mary University of London, School of Law, *Legal Studies Research Paper* núm. 77, pp. 1-31. Se puede consultar en: www.cloudlegal.ccls.qmul.ac.uk/Research/index.html. Fecha de la consulta: septiembre 2015.

W. Kuan HON / Julia HÖRNLE / Christopher MILLARD (2011), "Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law?, The Cloud of Unknowing, Part. 3, Queen Mary University of London, School of Law, *Legal Studies Research Paper*, núm. 84. Se puede consultar en www.cloudlegal.ccls.qmul.ac.uk/Research/index.html. Fecha de la consulta: septiembre 2015.

P. T. JAEGER / J. LIN / J. M. GRIMES / S. N. SIMMONS, "Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing", *First Monday* 14 (5). Se puede consultar en: http://pear.accc.uic.edu/ojs/index.php/fm/article/view/2456/2171. Fecha consulta: septiembre 2015.

P. T. JAEGER / J. LIN / J. M. GRIMES (2008), "Cloud Computing and Information Policy: Computing in a Policy Cloud?", *Journal of Information Technology & Politics*, 5:3, pp. 269-283 (DOI:10.1080/19331680802425479).

María Rosa LLÁCER MATACÁS (2012), *La autorización al tratamiento de información personal en la contratación de bienes y servicios*, Dykinson, Madrid.

- "La autodeterminación informativa en la sociedad de la vigilancia: *Ubiquitous Computing*" en María Rosa LLÁCER MATACÁS (2011), *Protección de datos personales en la sociedad de la información y la vigilancia*, La Ley, Madrid.

Rubén MARTÍNEZ GUTIÉRREZ (2011), "Cooperación y coordinación entre Administraciones públicas para el impulso de la Administración electrónica. La interoperabilidad" en José Luis PIÑAR MAÑAS (dir.), *Administración electrónica y ciudadanos*, Thomson Reuters, Cizur Menor, 2011.

Ricardo MARTÍNEZ MARTÍNEZ (2012), "El Derecho y el Cloud Computing" en Ricardo MARTÍNEZ MARTÍNEZ (ed.), *Derecho y Cloud Computing*, Thomson Reuters, Cizur Menor.

Ana MARZO PORTERA / Iciar MARZO PORTERA / Gonzalo MARTÍNEZ FLECHOSO (2004), *Los contratos informáticos y electrónicos*, edic. Experiencia, Barcelona.

Jesús Alberto MESSÍA DE LA CERDA BALLESTEROS (2003), *La cesión o comunicación de datos de carácter personal*, Thomson, Civitas, Cizur Menor.

Ramón MIRALLES LÓPEZ (2010), "Cloud Computing y protección de datos", IDP, *Revista de Internet, Derecho y Política*, núm. 11, UOC http://idp.uoc.edu/ojs/index.php/idp/article/view/n11-miralles/n11-miralles-esp.

Looke MOEREL (2011), "Back to basics: when does EU data protection law apply?" 1(2) *International Data Privacy Law*, p. 92.

Jean-Philippe MOINY (2011), "Facebook y la Directiva 95/46: Algunas reflexiones" en María Rosa LLÁCER MATACÁS, *Protección de datos personales en la sociedad de la información y la vigilancia*, La Ley, Madrid.

Alberto PALOMAR OLMEDA (2012), "Incidencia del cloud computing en el ámbito de la contratación pública" en Ricardo MARTÍNEZ MARTÍNEZ (ed.), *Derecho y Cloud Computing*, Thomson Reuters, Cizur Menor.

Javier PUYOL MONTERO (2013), *Algunas consideraciones sobre el Cloud Computing*, AEPD, BOE, Madrid.

Susana NAVAS NAVARRO (2015), *La personalidad virtual del usuario de internet. Tratamiento de la información personal recogida mediante cookies y tecnología análoga*, Tirant Lo Blanch, Valencia.

Christian OPPENHEIM (2012), *The No-Nonsense Guide to Legal Issues in Web 2.0 and Cloud Computing*, Londres, Facet Publishing.

Alfonso ORTEGA GIMÉNEZ (2012), "Cloud Computing, protección de datos y Derecho internacional privado (Resolución de controversias y determinación de la ley aplicable)" en Ricardo MARTÍNEZ MARTÍNEZ (ed.), *Derecho y Cloud Computing*, Thomson Reuters, Cizur Menor.

William Jeremy ROBISON (2010), "Free at What Cost?: Cloud Computing Privacy Under the Store Communication Act", *The Georgetown Law Journal*, vol. 98, pp. 1195-1239. Se puede consultar en http://ssrn.com/abstract=1596975. Fecha de la consulta: septiembre 2015.

Antonio RODRÍGUEZ DE LAS HERAS (2010), "El concepto de espacio digital y sus propiedades" en Alicia REAL PÉREZ (coord.), *Códigos de conducta y actividad económica: una perspectiva jurídica*, Marcial Pons, Barcelona/Madrid.

Antoni ROIG BATALLA (2010), "Intimidad y Administración electrónica" en Lorenzo COTINO HUESO/Julián VALERO TORRIJOS (coord.), *Administración electrónica*, Tirant Lo Blanch, Valencia.

Reyes SÁNCHEZ LERÍA (2011), *El contrato de hospedaje de página web*, Tirant Lo Blanch, Valencia.

Diana SANCHO VILLA (2010), *Negocios internacionales de Tratamiento de datos personales*, Thomson Reuters, Civitas, Cizur Menor.

Barrie SOSINSKY (2011), *¿Qué es la nube? El futuro de los sistemas de información*, Anaya, Madrid.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, Dictamen de 3 de septiembre de 2013, sobre la Comunicación de la Comisión citada en la nota precedente (C 253/3) que se puede consultar en www.edps.europa.eu.

Antonio TRONCOSO REIGADA (2011), "La administración electrónica y la protección de datos personales" en José Luis PIÑAR MAÑAS (dir.), *Administración electrónica y ciudadanos*, Thomson Reuters, Cizur Menor.

- *La protección de datos personales. En busca del equilibrio* (2010), Tirant Lo Blanch, Valencia.

Alberto URUEÑA / Anni FERRARI / David BLANCO / Elena VALDECASA (2012), *Cloud Computing. Retos y oportunidades*, ONTSI, Ministerio de industria, energía y turismo.

Julián VALERO TORRIJOS (2012), "La administración pública en la nube. Análisis de las implicaciones jurídicas desde la normativa sobre administración electrónica" en Ricardo MARTÍNEZ MARTÍNEZ (ed.), *Derecho y Cloud Computing*, Thomson Reuters, Cizur Menor, 2012.

Miguel VIZCAÍNO CALDERÓN (2001), *Comentarios a la Ley orgánica de protección de datos de carácter personal*, Civitas, Cizur Menor.