Revista de Derecho UNED, núm. 10, 2012

ALGUNOS RETOS DE LA PROTECCIÓN DE DATOS EN LA SOCIEDAD DEL CONOCIMIENTO. ESPECIAL DETENIMIENTO EN LA COMPUTACIÓN EN NUBE *(CLOUD COMPUTING)*

Celia Fernández Aller

Profesora titular de universidad interina. Escuela universitaria de informática. Universidad politécnica de Madrid

Resumen: Los continuos avances tecnológicos están trayendo consigo nuevas formas de almacenar, tratar y comunicar datos personales. Es necesario repensar el derecho fundamental a la protección de datos, y arbitrar mecanismos para adaptarlo a las nuevas formas de tratamiento. A nivel europeo se está trabajando en una nueva propuesta de regulación que consideramos, en general, muy apropiada para afrontar los nuevos retos en esta materia. Para ejemplificar todo esto, en el presente estudio se plantea de forma detallada el caso de la computación en nube, sus principales características y algunas preocupaciones acerca de los riesgos potenciales que su utilización trae consigo.

Abstract: Rapid technological developments are bringing new ways to store, process and communicate personal data. We need to rethink the fundamental right to data protection and adapt it to new forms of treatment. There is a new «european» proposal for a regulation on the protection of individuals with regard to the processing of personal data, well suited to meet the new challenges.

This study offers one example of this: the cloud computing, its main characteristics and some concerns about the potential risks that its use entails.

Palabras clave: Computación en nube, protección de datos, marco legal

Key words: Cloud Computing, Data protection, Legal Framework

I. INTRODUCCIÓN Y CONTEXTO

El contexto actual ha multiplicado las posibilidades de atentar contra la privacidad: las tecnologías, que en ocasiones pueden ayudar a proteger el derecho a la autodeterminación informativa o protección de datos[1], la mayoría de las veces suponen una ocasión para almacenar, comunicar o hacer un seguimiento de la información referida a personas que atenta seriamente contra su derecho a «ser dejado en paz»[2].

Permanecer ajeno a estas intromisiones y vulneraciones de la privacidad no es sencillo en una sociedad como la nuestra, basada en el

[1] Es el caso de las *Privacy Enhancing Technologies*, o tecnologías como la encriptación, anonimización o herramientas de gestión de la identidad, que aunque están pendientes de un mayor desarrollo y adolecen de ciertas debilidades en su implementación, suponen un intento de poner la tecnología al servicio de la privacidad. Así mismo, hay que citar los principios del *Privacy by Design*, muy impulsados por la autoridad canadiense e inglesa, incluyendo los *Estudios de Impacto de Privacidad*, o los *Sellos de Privacidad*.

[2] El borrador de Regulación europea para la protección de los individuos en lo que respecta al procesamiento de datos personales y a la libertad de movimiento de esos datos (versión de 29/11/2011), en su considerando 5 recuerda en este sentido que «los rápidos desarrollos tecnológicos y la globalización han traído consigo nuevos retos para la protección de datos personales. La cantidad de datos personales que se comparten y se recogen se ha incrementado espectacularmente. La tecnología permite a empresas privadas y autoridades públicas hacer uso de los datos personales a gran escala para perseguir sus actividades. Cada vez más, los individuos hacen disponibles a nivel público y global sus datos personales. La tecnología ha transformado la economía y la vida social y requiere que se facilite el tráfico de datos entre los países de la Unión Europea y hacia terceros países y organizaciones internacionales, al tiempo que se garantice un alto nivel de protección de los datos personales».

conocimiento. Y por otro lado, este derecho a la protección de datos no es absoluto, y muchas veces choca frontalmente con la necesidad de garantizar la libertad de expresión, de propiedad intelectual o de empresa[3]. De esta forma, el problema es realmente complejo.

El objetivo de este estudio es analizar cuáles son los retos que la protección de datos presenta en este momento, teniendo en cuenta los casi quince años de aplicación de la Directiva europea de protección de datos (95/46/EC), y en un momento en que se debate en profundidad la pertinencia de una nueva regulación a nivel europeo[4].

---

[3] Para resolver los conflictos entre derechos, el Tribunal Constitucional español ha utilizado la *regla de la proporcionalidad de los sacrificios*. Desde STC 37/1989 se conoce con el nombre de regla de la proporcionalidad de los sacrificios el conjunto de requisitos necesarios para llevar a cabo la limitación de un derecho fundamental. La restricción de un derecho fundamental o una libertad pública es considerada por el Tribunal Constitucional como «un acto tan grave» que «necesita encontrar una especial causalización y el hecho o el conjunto de hechos que lo justifican deben explicarse con el fin de que los destinatarios conozcan las razones por las cuales su derecho se sacrificó y los intereses a los que se sacrificó. De este modo, la motivación es no sólo una elemental cortesía, sino un riguroso requisito del acto de sacrificio de los derechos». En un principio, la doctrina constitucional sobre la regla de la proporcionalidad de los sacrificios incluía fundamentalmente un elemento: la *motivación exhaustiva*: «Según una muy reiterada doctrina constitucional, la regla de la proporcionalidad de los sacrificios (Sentencia 26/1981, fundamento jurídico 5º) es de observancia obligada al proceder a la limitación de un derecho fundamental (Sentencia 13/1985, fundamento jurídico 2º), y bien se comprende que el respeto de esta regla impone la motivación de la resolución judicial que excepcione o restrinja el derecho (Sentencia 62/1982, fundamento jurídico 2º), pues sólo tal fundamentación permitirá que se aprecie, en primer lugar, por el afectado y que se pueda controlar, después, la razón que justificó, a juicio del órgano judicial, el sacrificio del derecho fundamental».

Ahora bien, la doctrina constitucional posterior ha ido enriqueciendo el elenco de requisitos para que una limitación o injerencia en el ámbito protegido por un derecho fundamental puede considerarse legítima. Así, la STC 207/1996 (RTC 1996, 207) –que puede considerarse como un leading case en el tema que tratamos– exige explícitamente el cumplimiento de otras exigencias: «Conviene recordar los requisitos que conforman nuestra doctrina sobre la proporcionalidad, los cuales pueden resumirse en los siguientes: que *la medida limitativa del derecho fundamental esté prevista por la Ley, que sea adoptada mediante resolución judicial especialmente motivada, y que sea idónea, necesaria y proporcionada en relación con un fin constitucionalmente legítimo*» STC 207/1996, FJ 4 y STC 207/1996, FJ 4. (HERRERO-TEJEDOR ALGAR, F., «Escáneres personales e intimidad». *Revista Aranzadi Doctrinal* num. 2/2010. Estudio. Pamplona, 2010).

[4] Existe un Borrador de Regulación Europea de Protección de Datos de fecha 29/11/2011, *Regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*.

II. ¿EN QUÉ CONSISTE LA PROTECCIÓN DE DATOS Y CÓMO SE PROTEGE?

El derecho a la protección de datos personales es el derecho fundamental que tiene la persona a *controlar el uso que se hace de la información que personalmente le concierne*, sea de carácter íntimo o no, para evitar o rechazar usos que puedan perjudicarle. Este derecho se desprende, en nuestro ordenamiento jurídico, del artículo 18.4 de la Constitución, tal y como reiteradamente ha recordado nuestro tribunal constitucional[5]. En concreto, la STC 254/1993[6] señala que «la Constitución de 1978 ha incorporado el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos. El derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados… son absolutamente necesarias para que los intereses protegidos por el artículo 18 de la Constitución, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos». Y posteriormente, la sentencia 292/2000 reconoce el *carácter de fundamental del derecho a la protección de datos*: «el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes… se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular».

---

[5] Sobre el concepto de protección de datos personales, *vid.* LUCAS MURILLO DE LA CUEVA, «La construcción del derecho a la autodeterminación informativa», *Revista de Estudios Políticos,* nº 4, 1999; «La protección de datos personales ante el uso de la informática en el Derecho Español». *Estudios de Jurisprudencia COLEX.* Nº 4, en-feb 1993, pág. 7. MERCEDES SERRANO PÉREZ, *Introducción a la protección de datos*. Ed. Dykinson, 2006. TRONCOSO, A., *La protección de datos. En busca del equilibrio*. Ed. Tirant Lo Blanch, 2011. Datos de la persona, sobre la persona, comunicaciones y anonimato. SMEDINGHOFF. *On Line Law*, 1996, pág. 269

[6] *Vid.* comentario exhaustivo de esta sentencia en VILLAVERDE MENÉNDEZ, I., «Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993». *Revista Española de Derecho Constitucional.* Año 14, num. 41, may-agosto 1994, pág. 187.

El *derecho a la protección de datos no es absoluto*. Así lo justifica FERNÁNDEZ ESTEBAN[7]: «La posibilidad de mantener un control integral sobre los propios datos contribuye de manera determinante a definir la posición del individuo en la sociedad. No es casual que uno de los derechos consagrados en el art. 18 sea el derecho al honor…¿Qué es lo que debe percibir la sociedad? ¿la imagen que cada no quiere dar de sí mismo? ¿la reconstrucción que otro puede ofrecer a partir de sus datos? En otras palabras, la atribución a un individuo del control sobre sus datos, ¿puede llevar a afirmar un derecho exclusivo de autorrepresentación? A estas preguntas cabe responder que el derecho a la autodeterminación informativa o libertad informática en palabras del TC, no puede traducirse en un poder absoluto del individuo en las modalidades de composición y de representación de aquellas informaciones que son legítimamente disponibles a terceros».

Los derechos fundamentales pueden verse limitados ante bienes, e incluso, intereses constitucionalmente relevantes, «siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (STC 57/1994, de 28 de febrero, FJ 6; STC 18/1999, de 22 de febrero, FJ 2)»[8].

En la reciente STC 173/2011, de 7 de noviembre, el Tribunal Constitucional recuerda en su FJ 4º el *carácter amplio del derecho a la protección de datos*: «el Tribunal Europeo de Derechos Humanos ha venido asumiendo una interpretación extensiva del concepto «vida privada» del art. 8 del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales. Así, su Sentencia de 16 de febrero de 2000, dictada en el caso Amann contra Suiza, considera que «el término "vida privada" no se debe interpretar de forma restrictiva», de forma que éste «engloba el derecho del individuo de crear y desarrollar relaciones con sus semejantes», sin que «ninguna razón de principio permita excluir las actividades profesionales o comerciales».

El Tribunal Constitucional alemán, en sentencia de 27 de febrero de 2008 (1 BvR 370/07; 1 BvR 595/07), creó un derecho constitucional

[7] FERNÁNDEZ ESTEBAN, M. L., *Nuevas Tecnologías, Internet y derechos fundamentales*. Mc Graw Hill, Madrid, 1998, pág.135.

[8] GOIG MARTÍNEZ, J. M., NÚÑEZ MARTÍNEZ, A., NÚÑEZ RIVERO, C., *El sistema constitucional de derechos y libertades según la jurisprudencia del Tribunal Constitucional*. Ed. Universitas Internacional, Madrid, 2006, pág. 247.

a la confidencialidad e integridad de los sistemas de tecnologías de la información. Los sistemas que son capaces de crear, procesar y almacenar datos personales sensibles requieren especial protección. El ámbito de protección del derecho fundamental a la confidencialidad e integridad del sistema de tecnologías de la información se aplica a sistemas que, solos o técnicamente interconectados, pueden contener datos personales de la persona concernida hasta tal punto y en tal diversidad que el acceso al sistema facilita la vigilancia e intromisión en partes muy significativas de la persona, e incluso facilita un perfil de su personalidad. Esos sistemas son, por ejemplo, ordenadores personales, teléfonos móviles o calendarios electrónicos.

En esta misma línea se pronuncian algunos autores en España. Tal y como entiende J. L. RODRÍGUEZ LAINZ, el concepto de privacidad es una esfera superior que abarca los ámbitos de la intimidad, el secreto de las comunicaciones y la protección de datos de carácter personal. Comenta este autor que, con ocasión de la STC 173/2011 de 7 de noviembre, el tribunal Constitucional estableció que un terminal informático puede entenderse como si de un domicilio electrónico se tratase; de hecho, puede considerarse como objeto digno de protección por razón de la potencialidad de afectación a profundas esferas de la intimidad cuyo acceso o desvelo supone. Esta idea está plasmada en el anteproyecto de Ley de Enjuiciamiento Criminal de julio de 2011, y también en varias sentencias del Tribunal Europeo de Derechos Humanos, en concreto la de fecha 16 de octubre de 2007 (caso *Wieser y Bicos Beiligungen Gmbh v.Austria,* asunto núm. 74336/01).

El TC español interpreta, basándose en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, que el contenido de la memoria de un PC es un objeto digno de una especial protección jurídica, habida cuenta de la potencialidad de afectación de las más ignotas esferas de la intimidad. Además, utiliza el concepto de perfil del individuo, «para constatar cómo un tratamiento conjunto de todo ese cúmulo de informaciones, en buena parte aparentemente insignificantes, podría permitirnos desarrollar un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona»[9].

Es necesario repensar este concepto amplio de privacidad, espe-

[9] RODRÍGUEZ LAINZ, J. L., «Hacia un nuevo entendimiento de la protección integral de los dispositivos privados de almacenamiento electrónico de datos relativos a las comunicaciones (comentario a la STC 173/2011, de 7 de noviembre», *OTROSI,* núm. 9, 2012, pág. 35.

cialmente en los problemas de protección de datos que traen consigo algunas tecnologías que están implantándose de manera creciente y, a veces, subrepticia, como es el caso de las etiquetas de identificación por radiofrecuencia[10] (*RFID*), el tratamiento de datos personales por parte de las redes sociales y los buscadores, la computación en nube (*Cloud Computing),* etc.

III. ¿POR QUÉ LAS NORMAS ACTUALES NECESITAN UNA REDEFINICIÓN?

Los conceptos básicos de la Directiva 95/46/CE fueron desarrollados en los años setenta, cuando el procesamiento de información estaba caracterizado por los grandes ordenadores (ordenadores centrales). Hoy la informática es ubicua, global y en red[11].

Las máquinas de las tecnologías de la información están miniaturizándose y equipándose con tarjetas de red, wifi y otras. Los servicios web 2.0 y de *cloud computing* están desfigurando las distinciones clásicas entre responsable, encargado del tratamiento y afectado o titular de los datos personales.

La Directiva 95/46/EC de protección de datos personales de las personas físicas ha servido de marco de referencia hasta el momento, entre otras cosas, por la neutralidad tecnológica del marco legal. Sus principios continúan siendo aplicables. Sin embargo, es necesario aportar, desde el campo legislativo, algunas aclaraciones referidas a problemas que surgen con la aplicación específica de algunas nuevas tecnologías, y reforzar algunos conceptos, como el de «privacidad en el diseño», «estudios de impacto de privacidad» o «sellos de privacidad», que si no se hacen obligatorios para las industrias, difícilmente van a conseguirse en la práctica.

En este contexto de grandes cambios tecnológicos, los principales retos[12] que se han identificado en relación a la protección de datos son los siguientes:

---

[10] *Vid.* Fernández Aller, M. C., «La tecnología RFID y sus implicaciones jurídicas». *Datospersonales.org*. Revista de la Agencia de Protección de Datos de la Comunidad de Madrid, ISSN 1988-1797, Nº. 38, 2009.

[11] *Vid.* «La privacidad en el diseño como nuevo principio», en Grupo de trabajo del artículo 29. *The Future of Privacy*. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Adopted on 01 December 2009, pág. 12.

[12] NEIL ROBINSON, HANS GRAUX, MAARTEN BOTTERMAN, LORENZO VALERI, *Review of the European Data Protection Directive.* RAND Europe. 2009, pág. 18. Disponible on line: <www.rand.org> [Consulta: 10 de enero de 2012].

— La definición misma de privacidad: cuándo se afecta a la privacidad de las personas a través de un tratamiento de datos personales y cuándo no. ¿Cómo de fuerte debiera ser el vínculo entre las regulaciones de protección de datos y la protección de la privacidad?

— Estudio de riesgos: ¿podemos prever cómo es de peligrosa una provisión de datos personales a una empresa o institución?

— Los derechos de los individuos en relación con el beneficio de la sociedad: ¿bajo qué circunstancias puede la privacidad de una persona sacrificarse en favor de las necesidades de la sociedad, teniendo en cuenta la importancia de la protección de la privacidad para el desarrollo de las sociedades democráticas en su conjunto?

— Transparencia: hay datos personales en cualquier lugar, sobre todo en el contexto online, sin embargo, los desarrollos tecnológicos como la inteligencia ambiental o el cloud computing podrían llegar a ser difícilmente controlables. ¿Cómo podemos estar seguros de cómo y dónde se usan nuestros datos?

— Ejercicio de elección: muchos servicios no se facilitan sin antes aportar nuestros datos personales. ¿Qué sucedería si estos servicios son importantes, pero no queremos dar nuestros datos? ¿Hasta dónde llega nuestra capacidad de elección?

— Rendición de cuentas y responsabilidad: ¿quién es en último término responsable y a dónde y a quién nos dirigimos para buscar y exigir compensación?

IV. EL CASO PARTICULAR DE LA COMPUTACIÓN EN NUBE (CLOUD COMPUTING)

III.1. Conceptos previos

Cloud computing se ha definido como un modelo para hacer posible el acceso a red adecuado y bajo demanda a un conjunto de recursos de computación configurables y compartidos (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios…) cuyo aprovisionamiento y liberación puede realizarse con rapidez y con un mínimo esfuerzo de gestión e interacción por parte del proveedor del *cloud*.

El origen del término está en el gráfico de uso común para representar Internet como si fuera una nube (*cloud*). Los recursos de computación (hardware y software) de estos modelos están disponibles a través de Internet[13]. Esta tecnología está siendo utilizada por un número cada vez mayor de empresas y particulares por las ventajas que supone.

Las cinco *características*[14] que definen el *cloud computing* son:

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

Existen *diferentes tipos de nubes*:

— Nubes públicas: Se trata de aquellas que son administradas por el proveedor del servicio. La gran ventaja es que no requieren de una inversión inicial para comenzar a utilizarlas y no suponen un gasto de mantenimiento para el cliente. Estas nubes son compartidas con otros clientes dentro de los *data centers*[15] del proveedor.

— Nubes privadas: Las nubes privadas, a diferencia de las públicas, son administradas por el cliente para obtener un mayor

[13] COMISIÓN EUROPEA. DIRECCIÓN GENERAL DE JUSTICIA, LIBERTAD Y SEGURIDAD. *Comparative study of different approaches to new privacy challenges, in particular in the light of technological developments*. 2010, pág. 3. INTECO, *Riesgos y Amenazas en Cloud Computing,* 2011, pág. 6. Disponible on line: www.inteco.es [Consulta: 2 de febrero de 2012].

[14] MIRALLES, R., «Cloud Computing y protección de datos». *Revista D Internet, Derecho y Política.* Nº 11, 2010, pág. 16.

[15] Data center es aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

control. Debido a esto, supone una inversión inicial en la infraestructura ya que esta será alojada en las instalaciones del cliente.

— Nubes comunitarias se dan cuando dos o más organizaciones forman una alianza para implementar una infraestructura *cloud* orientada a objetivos similares y con un marco de seguridad y privacidad común.

— Nubes híbridas: Esta opción es intermedia entre la pública y la privada. La idea principal de las mismas es que el cliente podrá mantener el control de aquellas aplicaciones principales y delegar la administración en las que considere secundarias.

Dependiendo de la necesidad que queramos cubrir, existen *distintos niveles de servicios* dentro del cloud computing:

Infrastructure as a Service (IaaS): Este tipo de servicio ofrece la infraestructura necesaria para poder subir nuestro entorno y además ejecutar el software propietario en ella. Los dos pilares fundamentales son la computación y el almacenamiento como servicio, es decir, el alquiler de espacio de alojamiento o cloud hosting.

Platform as a Service (PaaS): Cuando hablamos de la plataforma dentro de la nube nos ofrecen el entorno donde podemos desplegar directamente nuestras aplicaciones, es decir, alquiler de plataformas para desarrolladores.

Software as a Service (SaaS): Es el servicio transformado en aplicación final proporcionado por el proveedor, listo para ser usado por los clientes. En este tipo de servicio se nos asegura el mantenimiento, el soporte y la disponibilidad del programa de ordenador.

Las modalidades de computación y las modalidades de servicios condicionan la aplicación de la LOPD.

El cliente en la computación en nube es el responsable del fichero. Tal y como ha señalado ya la Agencia de Protección de Datos[16], es él quien decide utilizar el servicio, la modalidad de computación en nube, y la modalidad de servicios. El proveedor se considera entonces encargado del tratamiento.

El cliente, como responsable de un fichero de datos personales, utiliza estos servicios de *cloud computing* y pone a disposición del proveedor –encargado– muchos datos personales.

[16] En la 4ª Sesión Anual abierta celebrada en Madrid el 27 de enero de 2012.

La ley aplicable a estos casos, en los que una empresa española contrata servicios de computación en nube, será la ley nacional del responsable (artículo 2.1 a de la Ley Orgánica de Protección de Datos –LOPD–).

III.2. Retos de esta tecnología en lo relativo a protección de datos

III.2.A. Retos generales

Interesa especialmente seguir profundizando en los principales retos que presenta esta tecnología desde el punto de vista de la protección de datos: Aunque la computación en nube aporta en cierto sentido mayor disponibilidad y seguridad de los datos –las empresas de cloud computing ofrecen, en su mayoría, procedimientos de backup, restore o planes de contingencia para casos de pérdidas de información o fallos que muchas empresas no tienen– esta tecnología presenta muchos *riesgos relacionados con la privacidad del individuo*. En general, existe un nivel de confianza bajo en la seguridad de los datos, por el hecho de que datos de la empresa no estén localizados dentro de las paredes de la empresa, sino en servidores ajenos. Además, existe una cierta sensación de cautividad del cliente, ya que al no disponer de los datos en sus propias unidades de almacenamiento, el cliente se encuentra a merced del proveedor de servicios y su proveedor de internet.

Debido a la importancia de este reto de la privacidad para la computación en nube, conviene recordar los principios pactados en Madrid, en la Declaración de la Sociedad Civil de 3 de noviembre de 2009. Aunque se refieren a la privacidad en general, resultan especialmente sugerentes en el análisis de la computación en nube:

(1) Ratificar el apoyo a un marco global de prácticas justas sobre la información que establezca obligaciones a los que recogen y procesan información personal, y conceda derechos a aquéllos cuya información personal se recoge;

(7) Exhortar a los países para asegurarse que los individuos sean inmediatamente notificados cuando su información personal sea revelada de forma inapropiada o usada para finalidades distintas para la que fue recogida o recabada;

(10) Hacer un llamado para el establecimiento de un nuevo marco

internacional para la protección de la privacidad, con la plena participación de la sociedad civil, basado en el imperio de la ley, el respeto a los derechos humanos y el apoyo a las instituciones democráticas.

III.2.B. Reconfiguración de los sujetos que intervienen en el tratamiento de datos personales: responsable, encargado y titular de datos

En el caso de una prestación de servicios las normas españolas de protección de datos distinguen dos personas: el encargado y el responsable del fichero. Será muy importante, en el caso de la computación en nube, delimitar bien cada uno de los sujetos, con sus derechos y obligaciones.

El cliente debe prestar especial atención a la hora de contratar un servicio de *cloud computing*, puesto que asume la responsabilidad sobre la información personal contenida en los ficheros, como responsable. La empresa proveedora del servicio de *cloud computing* será la encargada del tratamiento.

Como en cualquier encargo, habrá de respetarse la garantía contractual del artículo 12 de la LOPD. El contrato, que deberá constar por escrito o en alguna forma que permita acreditar su celebración y contenido, debe contener:

— Que el encargado únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.

— Las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

— Que el encargado del tratamiento no utilizará los datos con fines distintos a los que figuren en el contrato.

— Que el encargado del tratamiento no cederá los datos a otras personas, ni siquiera para su conservación.

— Que una vez cumplida la prestación, los datos será destruidos o devueltos al responsable, al igual que cualquier soporte o documentos en que consten los datos objeto de tratamiento.

El cumplimiento de estos requisitos puede encontrarse con problemas en la práctica de la computación de nube. En este caso, es muy frecuente que el encargado o prestador del servicio transfiera los datos a terceros ubicados en terceros países. De esta forma, cuando sea necesaria la destrucción o devolución de datos, habrá que des-

truirlos de los ficheros del encargado, y también de todos aquéllos que hayan recibido datos del encargado en sucesivas subcontrataciones o transferencias de datos.

Como sucede en otras prestaciones de servicios, cabrán subcontrataciones. Entrarán en juego, en este caso, los criterios tradicionales de la subcontratación del artículo 21.2 del RD 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante RPD):

— Especificación de los servicios a subcontratar, y si fuese posible, la empresa subcontratista

— Que el tratamiento se ajuste a las instrucciones del responsable.

— Autorización del responsable/cliente sobre los subencargados

— Contrato entre encargados y subencargados

El subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el art. 20.3 del RPD. Si el encargado utilizase los datos incumpliendo el contrato, será considerado responsable a los efectos de responsabilidad por infracciones.

La diligencia exigible al encargado se manifestará en la necesidad de facilitar:

— Información detallada sobre la tipología de nube, servicios, participantes, etc.

— Información sobre las medidas de seguridad (, niveles de seguridad, auditoría, encriptación, incidencias de seguridad, etc). El análisis que se haga ha de ser funcional, no estrictamente formal.

— Información sobre portabilidad al término del contrato.

Las instrucciones que debe dar el responsable en estos casos de encargo serán las siguientes:

— Selección del tipo de computación en nube y de los servicios a contratar

— Decisión sobre los tratamientos que no se contratan al prestador de servicios (por la naturaleza de la información, por la posible pérdida de control, etc…)

— Decisión sobre la información solicitada y/o ofrecida por el CCP (proveedor de servicios de computación en nube).

Cabe, así mismo, que el responsable dé una autorización previa sobre empresas subencargadas con:

— Especificación funcional de los servicios susceptibles de subcontratación

— Especificación de los niveles de calidad exigibles

— Relación actualizada de entidades subencargadas (que puede estar accesible en un sitio web con indicación de los países en que opera)

Como conclusión, puede decirse que en la computación en nube se da un cambio de paradigma, en el sentido de que hay más autonomía, se utilizan los contratos de adhesión, y se seleccionarán, en un proceso dinámico, los subencargados (que prestarán, como hemos visto, servicios al prestador de servicios de *cloud computing);* será muy importante que el encargado reúna las garantías del artículo 20.2 del Reglamento, tanto en lo referente a la obtención de información sobre las garantías (art. 12 LOPD) como en la tarea de ejercer diligentemente su posición.

En cuanto a los contratos de adhesión, los prestadores de servicios de *cloud computing* ponen a disposición de sus clientes dichos contratos con condiciones generales de contratación, en los que únicamente se hace necesario para su perfeccionamiento las firmas de las partes contratantes y en los que se incluye una cláusula de protección de datos personales, cláusula con la que se puede dar cumplimiento a la exigencia recogida en el artículo 12.2 LOPD. De esta forma, los prestadores de servicios de computación en nube pueden tener formularios en línea en los que, eligiendo una casilla con el ratón, se acepten los términos de este contrato.

En *materia sancionadora*, el encargado responderá de las infracciones en las que hubiere incurrido personalmente, y se equipara en materia de responsabilidad a la figura del responsable. A este respecto, resultan especialmente interesantes las sentencias de la Audiencia Nacional de 10 de noviembre de 2000, y de 14 de abril de 2000.

Una cuestión que supone preocupación desde el punto de vista de la protección de datos es la *inexistencia de la obligación de informar a los interesados* de este encargo de tratamiento de datos. Los interesados sí tienen obligación de conocer, sin embargo, las comunicaciones o cesiones de datos, debido a que suponen la existencia de un nuevo responsable del fichero (el cesionario). Creemos que esta falta de in-

formación, en el caso del *cloud computing,* no en otros encargos, puede traer consigo indefensión del interesado. Es posible que la empresa encargada transfiera datos personales a un tercero para la subcontratación de servicios; en ese caso, el titular de los datos perderá, en nuestra opinión, el control sobre ellos. Precisamente sostenemos, desde el comienzo de este texto, que la protección de datos consiste en el derecho a controlar el uso de los datos personales. Sin control, sin conocimiento de lo que sucede con los datos personales, no hay derecho de autodeterminación informativa.

III.2.C. Transferencia internacional de datos

Otra cuestión que plantea cierta inseguridad jurídica es el lugar físico de almacenamiento de los datos del cliente. Una característica de estos servicios es precisamente la ubicuidad de los recursos informáticos, lo que implica el acceso desde cualquier lugar, y el almacenamiento y tratamiento en cualquier lugar.

Normalmente, se dará un completo desconocimiento del lugar en el que realmente van a estar alojados los datos personales tratados por el encargado de tratamiento, ya que en muchos supuestos el prestador de estos servicios tiene ubicados sus servidores en otros países y en otros casos subcontrata el servicio a otros prestadores, perdiéndose así en ambos casos el control sobre la información almacenada. *El tratamiento de datos* mediante el uso de servicios en nube *implicará,* con mucha frecuencia y por la propia naturaleza de este modo de prestación, la existencia de *transferencias internacionales* con origen en territorio español.

Las transferencias internacionales de datos se definen en nuestra legislación como «*tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo*» para «*la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español*» –art. 5.1.s) RPD.

La normativa española de protección de datos prevé que puedan realizarse transferencias internacionales a países que ofrezcan un nivel adecuado de protección.

Para facilitar estas transferencias, la Agencia de Protección de Datos ha detallado los países que tienen un nivel de protección adecuado al exigido por la LOPD. Estos países son los Estados Miembros de la Unión Europea, Islandia, Liechtenstein, Noruega, Suiza, Argentina, Guernsey, Jersey, Isla de Man, Canadá y las entidades esta-

dounidenses adheridas a los principios de «Puerto Seguro» o «Safe Harbor». Estos principios son un acuerdo al que se acogen entidades estadounidenses por el cual se comprometen a aplicar nuestros principios jurídicos de la protección de datos.

En este sentido, el artículo 33.1 de la LOPD dispone que «*no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas*».

Por tanto, cuando el país destinatario no ofrezca ese nivel adecuado, las transferencias podrán autorizarse si:

— Concurre alguna de las excepciones legalmente previstas (consentimiento del interesado, transferencia necesaria para la ejecución de un contrato, etc.)

— El responsable ofrece garantías adecuadas. El responsable podrá aportar esas garantías mediante la presentación de un contrato (especialmente si el mismo incluye las cláusulas tipo aprobadas por la Comisión Europea[17]) o, en los casos en que las transferencias se produzcan en el seno de grupos multinacionales, de normas corporativas vinculantes (BCR) que hayan sido adoptadas por esos grupos.

Estos mecanismos están básicamente diseñados para transferencias que siguen un esquema clásico, en el que se conoce el país o países a los que se van a exportar los datos y la entidad o entidades que los van a recibir. Las últimas cláusulas contractuales tipo aprobadas por la Comisión Europea y las BCR son un intento de responder a la indeterminación que sobre algunos de estos elementos ha propiciado la evolución de los flujos internacionales de datos, ofreciendo instrumentos que permiten gestionar transferencias a una pluralidad de destinatarios siempre que se encuentren en un mismo grupo y estén ligados por unas reglas comunes de protección de datos y subcon-

[17] Decisión de la Comisión Europea de 5 de febrero de 2010, 2010/87/UE, relativa a las cláusulas contractuales 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.

trataciones no previstas en el momento en que se autorizó la primera transferencia.

El modelo de cloud computing, por su propia naturaleza, implica en muchos casos el desconocimiento del país preciso en que los datos van a ser tratados y de las entidades (subcontratadas) que van a intervenir en ese tratamiento. Más importante aún, la flexibilidad del modelo supone que países y entidades pueden variar constantemente de forma no predecible en el momento en que se produce la contratación del servicio y debe decidirse la utilización del instrumento jurídico más adecuado al tipo de transferencia que se va a producir.

La responsabilidad jurídica que establecen nuestras normas para el caso de incumplimientos de estas normas sobre transferencias internacionales de datos están previstas en el artículo 44.4 d) de la LOPD: «*Será infracción muy grave*[18]*: La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria*».

Existen cautelas que habrá que considerar en el caso de las transferencias internacionales de datos, y que evitarán tratamientos no respetuosos con la normativa de protección de datos:

— En el caso de que las *transferencias tengan como destino un país con un nivel adecuado de protección:*

  a) Será necesario redactar un contrato de prestación de servicios (art.12 LOPD, arts. 20-22 RLOPD entre el responsable y el encargado que recoja las garantías de protección de datos;

  b) En caso de subcontratación, habrá de llevarse a cabo un encadenamiento de garantías de protección de datos y una solicitud de autorización y/o conocimiento de la subcontratación por parte del responsable. Además, habrá de obtenerse información sobre los posibles destinatarios de transferencias ulteriores, o disponer de acceso a dicha información. El prestador de servicios de computación en nube puede mantener actualizada y disponible la relación de los mismos.

[18] Artículo modificado por la Ley de Economía Sostenible de 5 de marzo de 2011. Las sanciones previstas para esta infracción oscilan entre 300.001 y 600.000 €.

— En el caso de que las *transferencias no tengan como destino un país con nivel adecuado de protección:*

a) Habrá que solicitar autorización del Director de la Agencia y aplicar las cláusulas contractuales de la Decisión 2010/87/UE – cláusulas contractuales tipo de responsable. En concreto, la cláusula 11 permite la subcontratación del encargado – importador, establece el encadenamiento de garantías de protección de datos y la autorización y conocimiento de la subcontratación por parte del responsable; además, será necesaria la existencia de información de los subencargados disponible para la AEPD.

b) Otra posibilidad es la solicitud de autorización a la Agencia y además, el seguimiento de reglas corporativas vinculantes – Binding Corporate Rules (BCRs), cuya tramitación debe ser conforme al procedimiento previsto en el RPD (3 meses). Estas normas están basadas en varios documentos del grupo de trabajo del artículo 29, WP 153, WP154, WP155, WP108, WP107, WP74, que agrupa a Autoridades Europeas de Protección de Datos. Se trataría de transferencias internacionales de datos entre empresas del grupo, y cuyos responsables son las mismas empresas. El ámbito de aplicación sería sólo la nube privada del grupo.

III.2.D Seguridad

La seguridad es una de las herramientas o instrumentos de que disponemos para asegurar el respeto a la protección de datos. La seguridad abarca varios ámbitos –disponibilidad, autenticación, integridad y confidencialidad– siendo el último de ellos el más relacionado con la libertad informática.

Tal y como expone CORRIPIO GIL-DELGADO, R.[19], «en Internet existen necesidades específicas de seguridad que generan obligaciones particulares de los agentes involucrados en el tratamiento de datos personales. Estas necesidades particulares deben conducir a un reforzamiento de las medidas de seguridad atendiendo al grado de

[19] CORRIPIO GIL-DELGADO, M. R., *Regulación jurídica de los tratamientos de datos personales realizados en el sector privado en internet»*. Agencia Española de Protección de Datos. Premio Protección de datos Personales, IV Edición, 2000, pág. 129.

vulnerabilidad del medio tecnológico empleado en dicho tratamiento, y que se traduce en el nacimiento de derechos específicos –para el titular de los datos– tales como la obligación de ser informado de la falta de seguridad de la red, entre otros».

La seguridad es el reto y la preocupación más importante en torno al *cloud computing,* tal y como reconocen los estudios más recientes[20].

La normativa europea debería armonizarse en esta materia, puesto que el RPD vigente en España, establece una serie de medidas de seguridad, en función de los niveles de seguridad del fichero, con unas sanciones previstas para el caso de incumplimiento, que no coinciden con otros países europeos. ¿Qué medidas habrían de aplicarse a determinado supuesto en el que una empresa de otro país de la Unión Europea presta servicios de *cloud computing* a un cliente español? Al convertirse el cliente en responsable de los ficheros que está utilizando la empresa, ¿podría seguir aplicando el reglamento vigente en España?

El RPD recuerda que las medidas de seguridad tienen que aplicarse a cualquier fichero o tratamiento de datos de carácter personal, con independencia: a) De *quién realice* el tratamiento (Encargado del tratamiento, diferentes modos de prestación del servicio (art. 82 RPD, prestación de servicios sin acceso a datos personales, cláusula informativa en el contrato (art. 83 RPD); b) *Desde dónde se realice* (acceso a datos a través de redes de comunicaciones, sean o no públicas (art. 85), régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento, dispositivos portátiles (art. 86); c) *Cómo se realice* (ficheros temporales o copias de trabajo de documentos (art. 87).

Muchos de estos supuestos pueden coincidir con los tratamientos que se llevan a cabo en *cloud computing,* como el acceso a datos a través de redes de telecomunicaciones. Y a estos casos hay que aplicar un régimen de medidas de seguridad[21].

Las medidas de seguridad previstas son, resumidamente, la ela-

[20] IDC Entreprise Panel, 2008, señalaba que un 74,6% de los encuestados manifestaban preocupaciones en torno a la seguridad. *Vid*. Así mismo, *Modelling Cloud Computing. Architecture Without Compromising Privacy: A Privacy by Design Approach*. NEC Company, Ltd.. and Information and Privacy Commissioner,Ontario, 2010. Es también muy interesante a estos efectos el estudio de INTECO, *Riesgos y Amenazas en Cloud Computing,* 2011. Disponible on line: www.inteco.es [Consulta: 2 de febrero de 2012].

[21] FERNÁNDEZ ALLER, C., *Análisis y gestión de riesgos en los sistemas de información, cl.* Fundación UPM, 2010.

boración de un documento de seguridad, actualizado, que consta de un contenido mínimo fijado reglamentariamente; además, han de detallarse las funciones y obligaciones del personal, contar con un registro de incidencias, medidas de control de acceso, gestión de soportes y documentación, sistemas de identificación y autenticación, copias de respaldo y recuperación, cautelas en la transmisión de datos a través de redes de telecomunicación. En función de cuál sea el nivel de seguridad exigido (básico, medio o alto), las medidas serán más o menos exigentes.

Si una clínica que trata información sensible de sus pacientes, por ejemplo, contrata un servicio de computación en nube, ha de cifrar o utilizar un procedimiento equivalente siempre que transmita sus datos a terceros, e igualmente, el proveedor (puesto que el encargado también debe respetar las medidas de seguridad). Si el proveedor subcontrata a un tercero, la medida de seguridad exigible sigue siendo la misma. Es innegable que existen dificultades para controlar que estas medidas se están llevando a cabo.

En este sentido, la nueva regulación de protección de datos en trámite en Europa recoge previsiones de seguridad en los artículos 3, 19, 23, 27, 28 y 29, en los que se hace alusión al concepto de brecha de seguridad, y a las obligaciones que en esta materia tienen tanto el responsable como el encargado.

La seguridad es uno de los aspectos clave en la computación en nube. Se aprecia gran preocupación por el hecho de que estas infraestructuras pueden gestionar los datos en múltiples países, lo que puede generar conflictos en cuanto al marco legal de seguridad en el que son tratados. Además, al manejarse gran cantidad de datos, pueden ser objeto de fugas de información –intencionadas o fortuitas– con más facilidad que otro tipo de modelos de almacenamiento.

V. CONCLUSIONES

La protección de datos, como derecho fundamental, se encuentra hoy día con importantes desafíos, provenientes de una tecnología que avanza y se incorpora a la realidad con más rapidez que las respuestas jurídicas. Un ejemplo de ello es la computación en nube, que se va implantando progresivamente en la sociedad en sus diversas formas, y que trae consigo nuevos problemas de aplicación de la libertad informática, tanto si es un particular como si es el sector público el que contrata los servicios de *cloud computing*. Será necesario

redefinir el papel del responsable y el encargado, resolver problemas vinculados con las transferencias internacionales, y reforzar las medidas de seguridad. En este sentido, la legislación que se encuentra en preparación en el ámbito de la Unión Europea puede contribuir a facilitar la adopción de esta tecnología, relativamente creciente, por parte de los diferentes actores.